The Novel Methods on Survivability for Next-Generation Internet

Keping Long

Professor and director
Email: lkp@uestc.edu.cn

Research Center for Optical Internet & Mobile Information Networks (COIMIN)
University of Electronic Science & Technology of China (UESTC)
Outline

• Background for Internet Survivability

• Conventional activities to enhance Internet survivability

• New directions and our works
  – Semi-ecosystem framework
  – Internet artificial Immune
  – Fault/intrusion tolerance based on social trust model
  – Soft-sensing

• Conclusions
Outline

• Background for Internet Survivability

• Conventional activities to enhance Internet survivability

• New directions and our works
  – Semi-ecosystem framework
  – Internet artificial Immune
  – Fault/intrusion tolerance based on social trust model
  – Soft-sensing

• Conclusions
Background
- We are more depended on Internet

- All electronic devices are to be plugged to the Internet in future
- The world will more depend on the Internet
- Economics
- Education and academic research
- Entertainments
- etc…
Background

- Internet is a complex system facing survivability challenges

The Internet is actually a complex system linked by lots of fibers, radios, cables..., just like the spider web.

- The Internet is fragile due to the variety of failures and attacks
  - Fiber cut, cable cut, link down, machine failures
  - Hacker, network virus and worms

- Techniques enhancing the survivability of Internet against failures and attacks, are urgent
Background
- Internet is a complex system facing many challenges

More and more bigger! More and more complex!
We have to find new methods to make the Internet:
• Robust with high survivability
• Pervasive trust
• Effective management
• Optimized resource usage
• ...

- Internet is a complex system facing many challenges

Background

Lower trust
Hard to manage
Lower survivability
Inefficiency usage of Resource
Background
- The concept of network survivability

• The concept of survivability for the information network is a historical topic, and variety of issues are involved:
  
  – What does survivability mean?

  – How is survivability being measured?

  – How is survivability computed and provided?

  – etc…
Background

- The definitions of network survivability

Techniques needed to evaluate each. Among the many measures of survivability that can be considered are as follows:

1) The ability of any node to communicate with any other node.
2) The existence of communication paths between specified pairs of nodes.
3) The number of nodes in the largest communicating section of the network after attack.
4) The length of the shortest surviving path between each pair of nodes or between specified pairs of nodes.
5) The average fraction of specified pairs of nodes able to communicate after attack.
6) The average or maximum time required to transmit a high priority message from source to destination.

Background

- The definitions of network survivability

- The ability of a network to maintain or restore an acceptable level of performance during network failures by applying various restoration techniques
  - Source: USA, ANSI T1A1.2 work group

- To define survivability as the capability of a system to fulfill its mission, in a timely manner, in the presence of attacks, failures, or accidents
Background

-The definitions of network survivability

Westmark from University of Central Florida conducted a interesting survey on 3760 matched publications within ACM, IEEE, and SEI libraries (http://www.sei.cmu.edu) in 2004

- The rich elements of survivability in current literatures
  • Availability, dependence, connectivity, correctness, dependability, fault tolerance, recoverability, reliability, restorability, safety, security, etc.

- No one article listed all elements, no two articles were consistent in the definition, and no formal complete definition could be cited.

Source: V R Westmark, “A Definition for Information System Survivability,” HICSS'04
Background
- The definitions of network survivability

- No clear definitions are given up to now, knowledge can be achieved:

  - **Survivability of Internet is a complex conception, in which a variety of survivability models such as security, reliability, and fault tolerance are combined**
Outline

• Background for Internet Survivability

• Conventional activities to enhance Internet survivability

• New directions and our works
  – Semi-ecosystem framework
  – Internet artificial Immune
  – Fault/intrusion tolerance based on social trust model
  – Soft-sensing

• Conclusions
Conventional efforts on the survivability of optical Internet

- Practically implemented by APS for SDH/SONET Ring
  - 50ms guarantee

- Academic proposals/algorithms on survivability at optical layer
  - Previous protection, Restoration after failures occurring
  - Dedicated 1+1/1:1, shared N:1 protection, Preserved circles (p-circle)....

- Recent topics in GMPLS controlled optical Internet
  - Multi-layer restoration by bottom-up/up-down via signaling
  - Dual homing, routing diversity, fast rerouting via path computation element
  - ...
  - Source: B. Linick, OFC/NFOEC 2008, paper NWD1;
Conventional efforts on intrusion and attack tolerance of Internet

- Today’s Internet suffers great damages of malice attacks from computer viruses, malwares, etc.
  - Worms, Trojan horses …
  - Hackers…

- Conventional anti-virus methods using signature scanning, check summing, real time scanning etc., can not defense increasingly sophisticated polymorphic and metamorphic viruses.

- More advanced and adaptive solutions are required.
Outline

• Background for Internet Survivability

• Conventional activities to enhance Internet survivability

• New directions and our works
  – Semi-ecosystem framework
  – Internet artificial Immune
  – Fault/intrusion tolerance based on social trust model
  – Soft-sensing

• Conclusions
• Current Internet is fragile, rigid, and notoriously difficult to configure and maintain.

• Many ecosystems (biological or social) are excellent on robustness, adaptive and self-organization, despite being highly decentralized.

• Can we draw inspirations from ecosystems to build robust, survivable Internet?
• Self-organization capable network requires:
  – short-term adaptive to the environment as well as long term evolution of the new self-healing functions without any manual intervention

• Its goals: to develop the new self-healing and reconfiguration methods using semi-ecosystem framework, Internet artificial Immune, etc.
• An example of the biological system: the rerouting of ant colony
  – How to preserve/increase the resilience of food-track routing.

Operations in the normal case
Biologic- and ecosystem-inspired Internet survivability
— example

• the rerouting of ant colony
  – How to preserve/increase the resilience of food-track routing

The “ant colony optimization” mechanisms can be used to achieve robust route for Internet
  • Introduce fact of pheromone into routing table
  • Choose next hop by estimating the quality of the associated pheromone

Keping Long, COIMIN, UESTC
http://www.coimin.uestc.edu.cn/
Survivability models using semi-ecosystems

- Motivated by the ant colony, etc., Internet can be modeled as digital semi-ecosystems or complex adaptive systems
  - Demonstrates some features of emergent collective, systemic behaviors, etc., to evolve its functionality.
  - Performs its functionality seamlessly even in case of a sudden dysfunction (e.g. collapse or attack).
Example
-- Similarities between ecosystem and Internet

- **Ecosystem**
  - A complex ecosystem network is formed among species and individuals, via food chain or energy chain.
  - Self-healing mechanisms to keep system stable

- **Internet**
  - Hosts and routers etc. are connected and webbed by cables or logical links via traffic delivering, which forms complex information networks.
  - Robust ingenuities to recover from failures/attacks are also required.
Similarities between ecosystem and Internet

-- Example

Internet vs. ecosystem
Related research works

• Some existing research activities
  – Cyber-engineering Research program funded by US NFS
    • To regard the future Internet as a networked embedded control system
  – European project IRRIIS (Integrated Risk Reduction of Information-based Infrastructure Systems)
    • Aims at increasing the dependability and resilience of Large Complex Critical Infrastructures (LCCIs) by introducing appropriate Middleware Improved Technology (MIT) based on Information and Communication Technology (ICT)
Related research works

– Highly DEpendable IP-based NETworks and Services (HIDENETS) Denmark project

  • to develop and analyze end-to-end resilience solutions for distributed applications and mobility-aware services in ubiquitous communication scenarios

– ReSIST (Resilience for Survivability in IST,) is a Network of Excellence (NoE)

  • integrating leading researchers active in the multidisciplinary domains of dependability, security, and human factors.
Related research works

– Digital Ecosystems Consortium

  • To develop a complex conceptual framework for Enterprise Networking for describing the interactions between firms, technology, and knowledge inspired by biological ecosystems

– European IST FP5 BISON project (Biology-Inspired techniques for Self-Organization in dynamic Networks) and FP6 BIONETS project

  • To enhance information network via borrowing ecosystem theory
Our works

- Funded by 973 (National Basic Research Program of China), National Science Fund for Distinguished Young Scholars of China, 863 (National High Technology Research and Development Program of China) are as following:

  - *The survivability semi-ecosystem*

  - *Internet artificial immune*
Our works
- survivability semi-ecosystem

• Semi-ecosystem framework

• Self healing mechanism of ecosystem from the point view of complex network

• Propose the natural protection zone in Internet.
  – e.g, special protection for panda on earthquake or other disasters
Outline

• Background for Internet Survivability

• Conventional activities to enhance Internet survivability

• New directions and our works
  – Semi-ecosystem framework
  – Internet artificial Immune
  – Fault/intrusion tolerance based on social trust model
  – Soft-sensing

• Conclusions
Due to the analogous role between bio-immune system and network security system, the artificial immune system has been inspired to input solutions to the network attack tolerance since early 1990s.

- Negative Selection based algorithms by pattern matching of large quantity of generated detectors to abnormal patterns
- Considerable computing resources are required to execute the extensive pattern matching.
- Digital immune system using decoy program to collect and detect unknown viruses
Internet artificial immune
——State of the art

– Multi-level computer immune architecture to release computation burden (R.E. Marmelstein, IEEE ICMSMC 1998)
  • Not easy to be implemented due to complexity and multi-level feature

  • Lack of self-adaptability

– Cooperative intrusion detection immune system following P2P principles (K. Luther et al, ICC 2007)
  • Dynamic collaboration between individual artificial immune system agents
  • Single point of failure avoidance
There are three layers in Bio-immunology of human body to defense attacks:

- Layer 1, Skin and fur…

- Layer 3, provided by co-operation among various immune cell, including B-cell, T-cell….

Excellent robustness achieved by large number of immune cells.
Information and knowledge of local process forms Log files and then are transferred to network manage system or server etc.

abnormal Failures sensed via self or noself anomalies identification

Solutions are made on the transferred log files etc, and delivered to involved network parts

Innate immune vs. network anti-attack system
Outline

• Background for Internet Survivability

• Conventional activities to enhance Internet survivability

• New directions and our works
  – Semi-ecosystem framework
  – Internet artificial Immune
  – Fault/intrusion tolerance based on social trust model
  – Soft-sensing

• Conclusions
Motivation

• The failure/attacks migration requires:

  – The abilities to quickly evaluate system vulnerability and start protection against potential threats/abnormal events.
  
  – Goals: recovery mechanisms is needed to anticipate in the security of critical infrastructures.
Our Works- modeling

- The migration Markov model for IP survivability
  - Key point: M→GD/R

H: Health      GD: Gracede degradation
S: Susceptible R: Recovery
C: Collapse    F: Failure
M: Migration

$$H \rightarrow S \rightarrow C \rightarrow M \rightarrow R \rightarrow F$$

1-p_c 1-p_{gr} 1-p_a
1-p_s  p_s  p_c  p_a  1-p_g\cdot p_f
1-p_g \cdot p_f  p_g  p_h  1-p_a
Fault/Intrusion Tolerance

- Conventional methods

*The existing methods: fault/intrusion tolerance are separating*

**Fault Tolerance Only**
- Self-healing
- Recovery

**Intrusion Tolerance Only**
- Cryptograph
- Intrusion detection

Keping Long, COIMIN, UESTC
http://www.coimin.uestc.edu.cn/
Fault/Intrusion Tolerance- Our Works

- More efficient method?
  - Motivation: Social networks vs. Internet
- In social networks, individuals utilize the trust relationships to decide whether contract with each other or not, and realize both fault-and intrusion-tolerance

<table>
<thead>
<tr>
<th>Social networks</th>
<th>IP networks</th>
</tr>
</thead>
<tbody>
<tr>
<td>individual</td>
<td>node</td>
</tr>
<tr>
<td>association or community</td>
<td>subnet or autonomous system</td>
</tr>
<tr>
<td>contact</td>
<td>communicate</td>
</tr>
<tr>
<td>individual faults</td>
<td>node faults</td>
</tr>
<tr>
<td>individual intruded</td>
<td>node intruded</td>
</tr>
<tr>
<td>transfer</td>
<td>relay</td>
</tr>
<tr>
<td>direct known</td>
<td>direct trust</td>
</tr>
<tr>
<td>indirect known</td>
<td>indirect trust</td>
</tr>
<tr>
<td>hierarchy and grade in social networks</td>
<td>hierarchy and grade in IP networks</td>
</tr>
</tbody>
</table>
Fault/Intrusion Tolerance - Our Works

- Trust-based Fault/Intrusion tolerance Scheme

Keping Long, COIMIN, UESTC
http://www.coimin.uestc.edu.cn/
Outline

• Background for Internet Survivability

• Conventional activities to enhance Internet survivability

• New directions and our works
  – Semi-ecosystem framework
  – Internet artificial Immune
  – Fault/intrusion tolerance based on social trust model
  – Soft-sensing

• Conclusions
• In Internet, some parameters, e.g., the location of failures, cannot be directly obtained.

• Soft-sensors, or virtual sensors can be used to estimate or infer some performance parameters from the indirect measurements.
The Internet shares common features with process industries
- Some parameters can be directly measured or sensed while others cannot.
- Linear or nonlinear relations exist among parameters.

We introduce soft sensing into Internet survivability designs
- Soft sensor modeling via multi-discipline crossing
- Failure/attack detection and locating
- Failure predication
- ...
• Network Tomography
  • To obtain network topology, internal link properties
Soft-sensing
-Our works

- IP positioning based on virtual coordinates using soft-sensing method
  • To locating failure/anomaly nodes
  • To predicate failure/anomaly events

Keping Long, COIMIN, UESTC
http://www.coimin.uestc.edu.cn/
• Background for Internet Survivability

• Conventional activities to enhance Internet survivability

• New directions and our works
  – Semi-ecosystem framework
  – Internet artificial Immune
  – Fault/intrusion tolerance based on social trust model
  – Soft-sensing

• Conclusions
Concluding Remarks

• The Internet is more than a complex webbed information system and confronts with various survivability challenges.
• Conventional methods and concepts on Internet survivability designs are extended to accommodate more complex requirements.
• New methods based on multi-discipline crossing may provide more flexible solutions:
  – Solutions based on Internet artificial immunology and semi-ecosystem;
  – Solutions based on social relationship trust;
  – Solutions under the umbrella of soft sensing;
  – ….
Thanks
Welcome all of you to COIN2009 in Chengdu (Panda’s hometown), China