Cyber Security Challenges & Co-operative Solutions: An Indian Perspective

Rajeev Shorey
(Ph.D, Fellow Indian National Academy of Engineering)

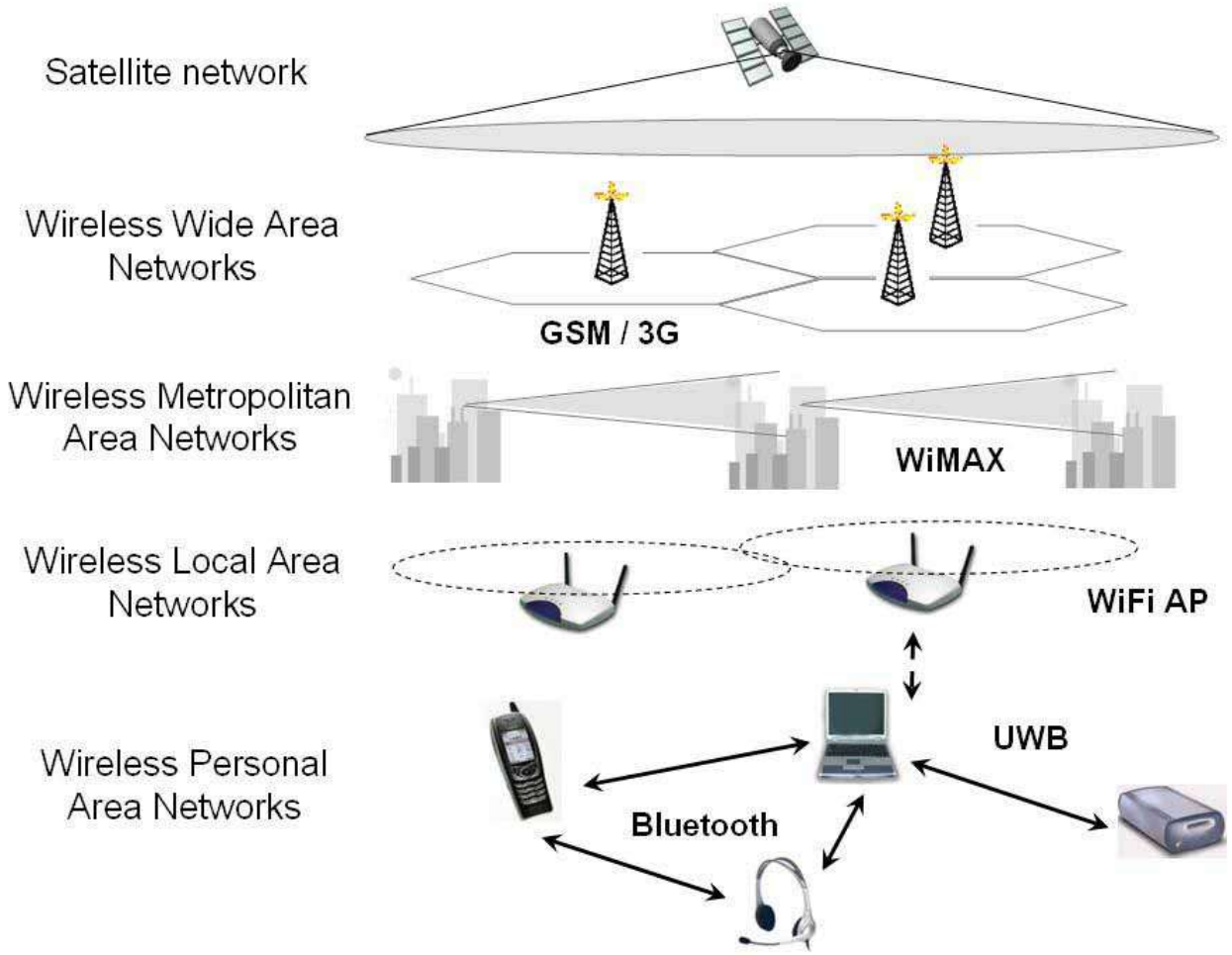
NIIT University, India
www.niituniversity.in
(Formerly GM Research Labs, Bangalore, India)

First International Workshop "Scientific Analysis and Policy Support for Cyber Security" (SA&PS4CS'10)
11 September 2010
St. Petersburg, Russia

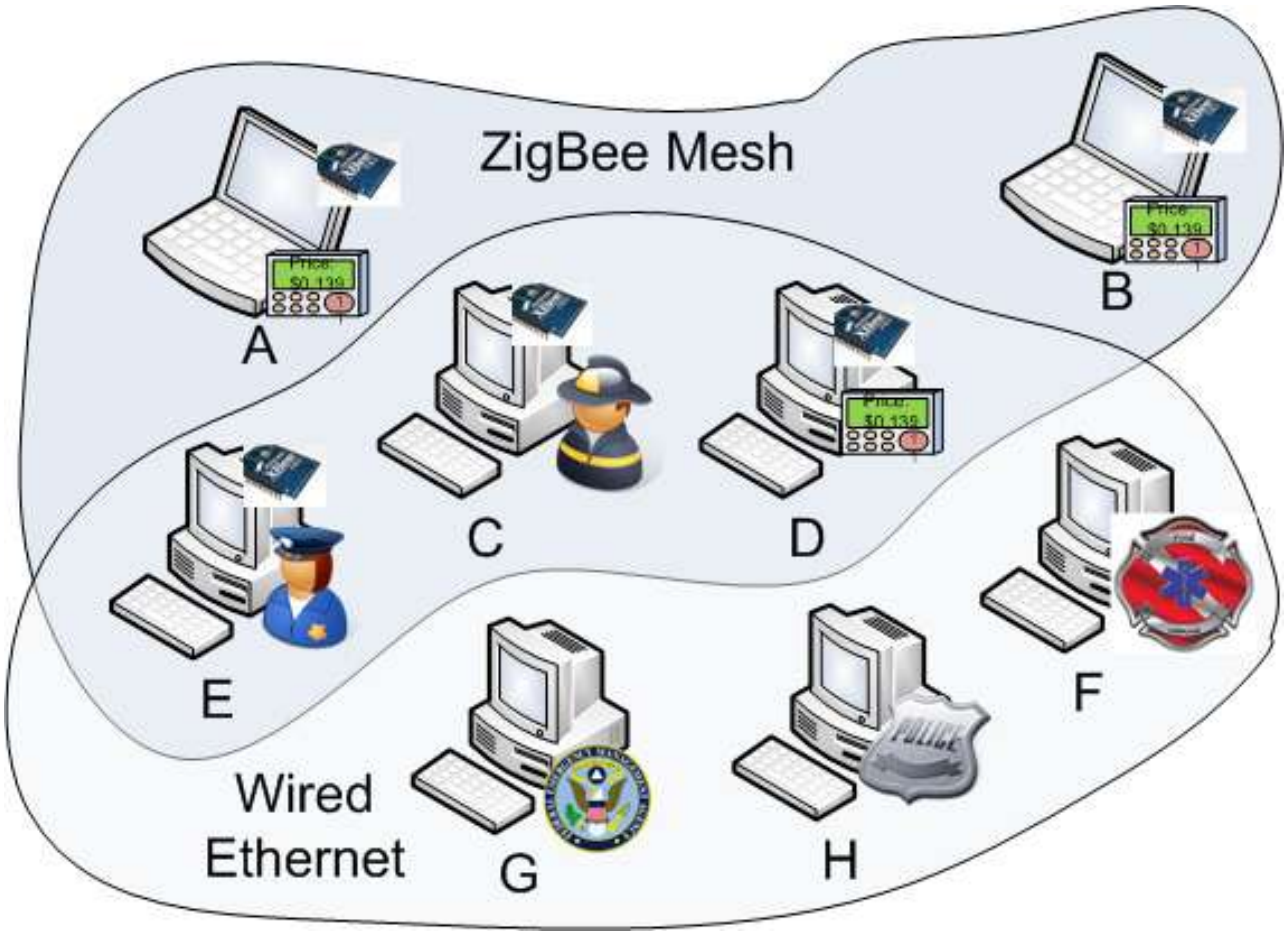
Agenda

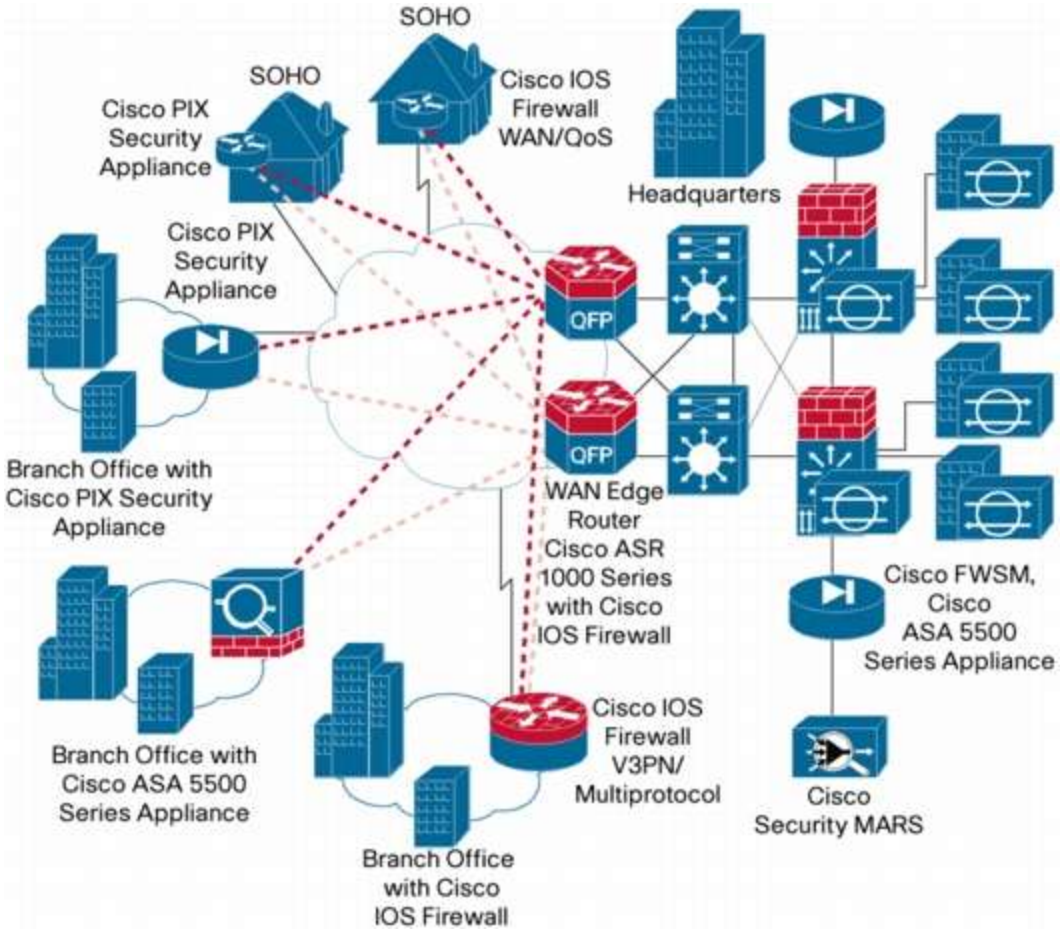
- A peek at Networks of Today
- Framework for Cyber Security in India
- Indian Scenario
  - National Cyber Security
- Real time Traffic Intelligence
- Emerging paradigms
- Conclusion

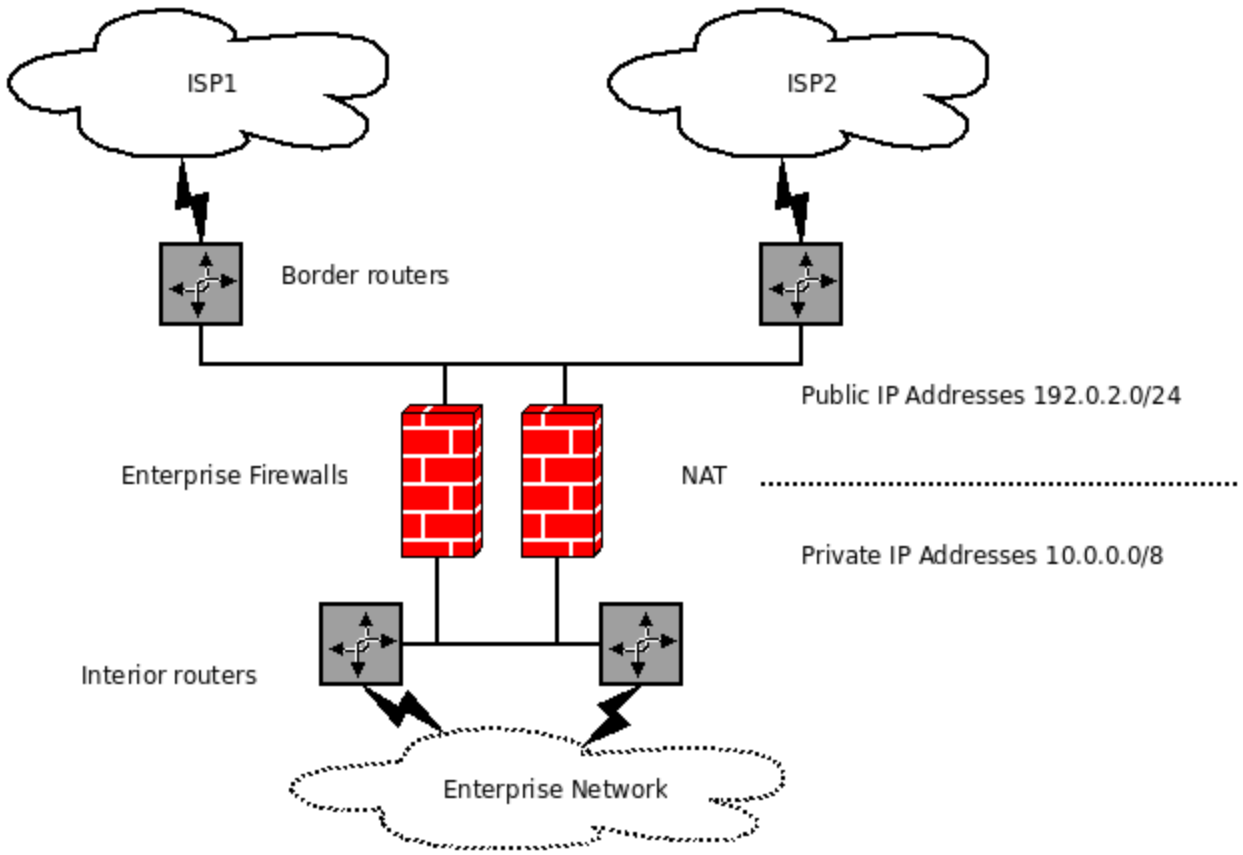
A Peek at Networks Today



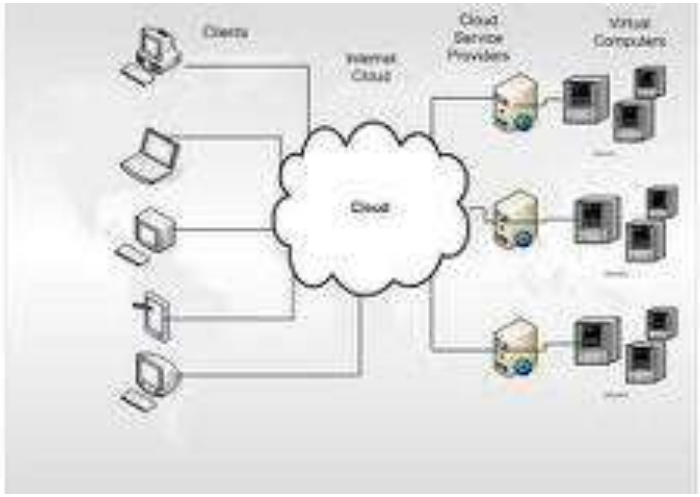
Networks Today



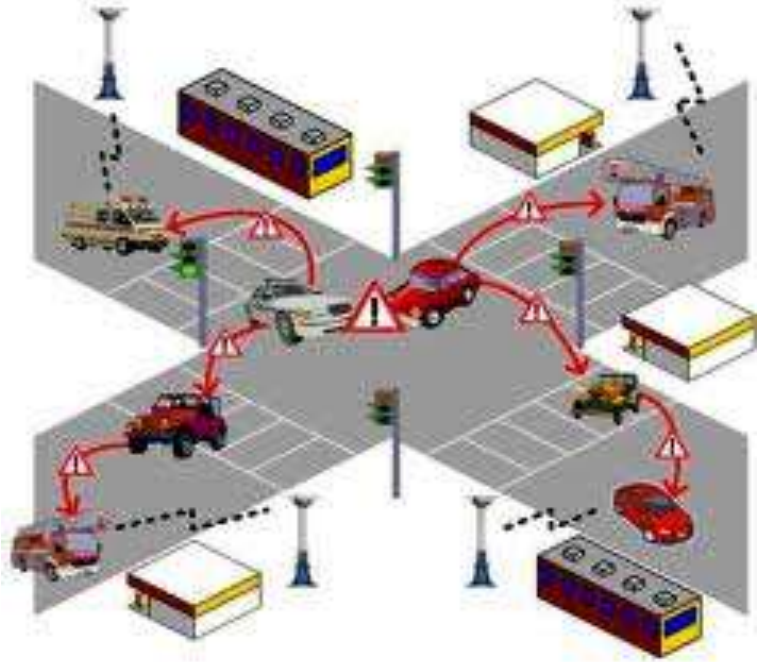

SOHO
SOHO
Cisco PIX
Security
Appliance
Cisco IOS
Firewall
WAN/QoS
Headquarters
Cisco PIX
Security
Appliance
QFP
QFP
Branch Office with
Cisco PIX Security
Appliance
WAN Edge
Router
Cisco ASR
1000 Series
with Cisco
IOS Firewall
Cisco FWSM,
Cisco
ASA 5500
Series Appliance
Branch Office with
Cisco ASA 5500
Series Appliance
Cisco IOS
Firewall
V3PN/
Multiprotocol
Cisco
Security MARS
Branch Office
with Cisco
IOS Firewall

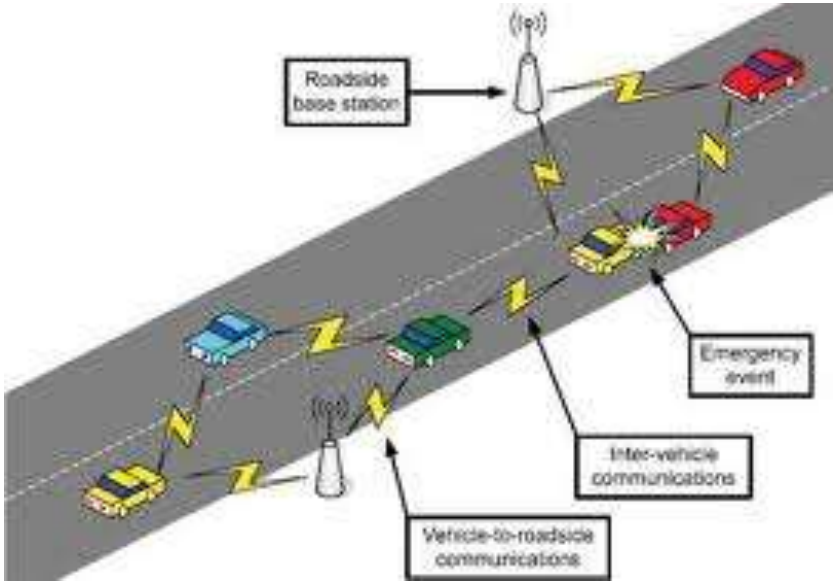

ISP1
ISP2
Border routers
Public IP Addresses 192.0.2.0/24
Enterprise Firewalls
NAT
Private IP Addresses 10.0.0.0/8
Interior routers
Enterprise Network

Cloud Computing



Vehicular Ad Hoc Networks

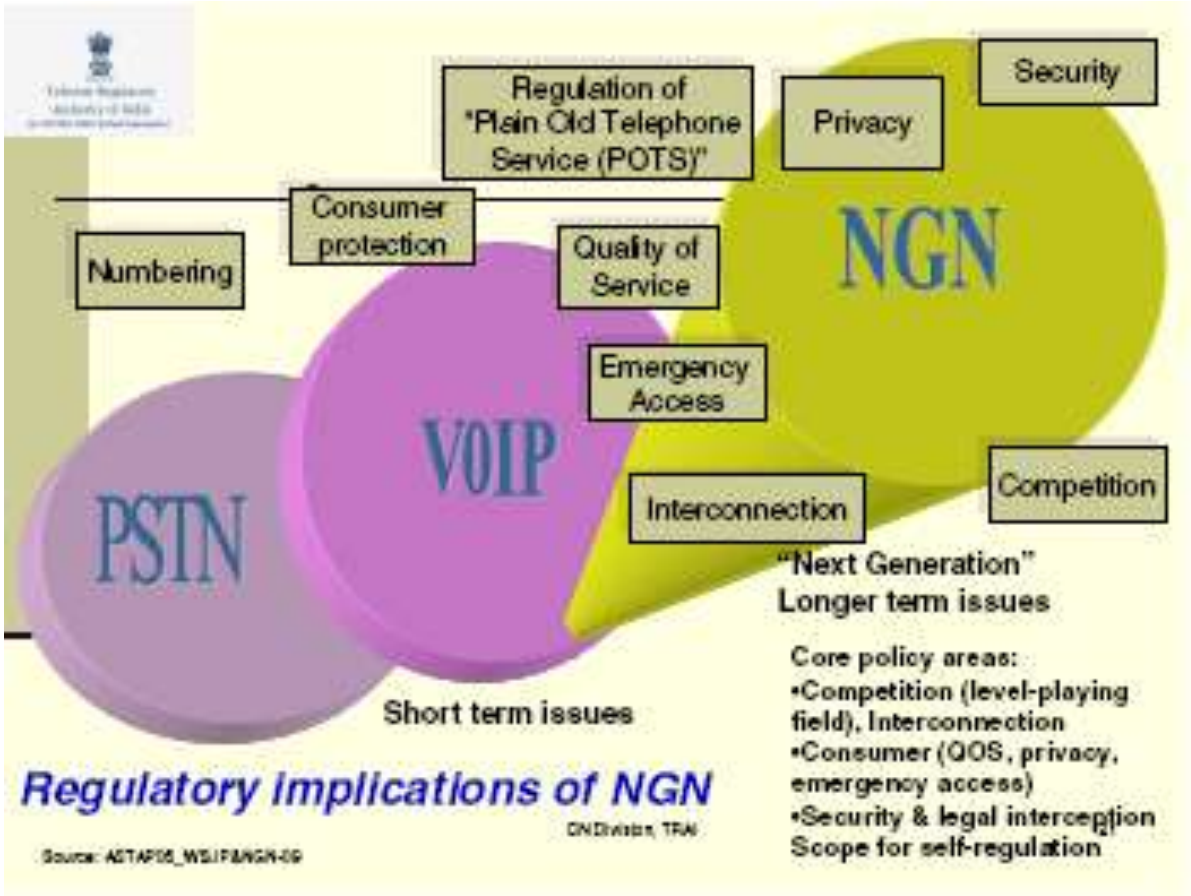




Take Away

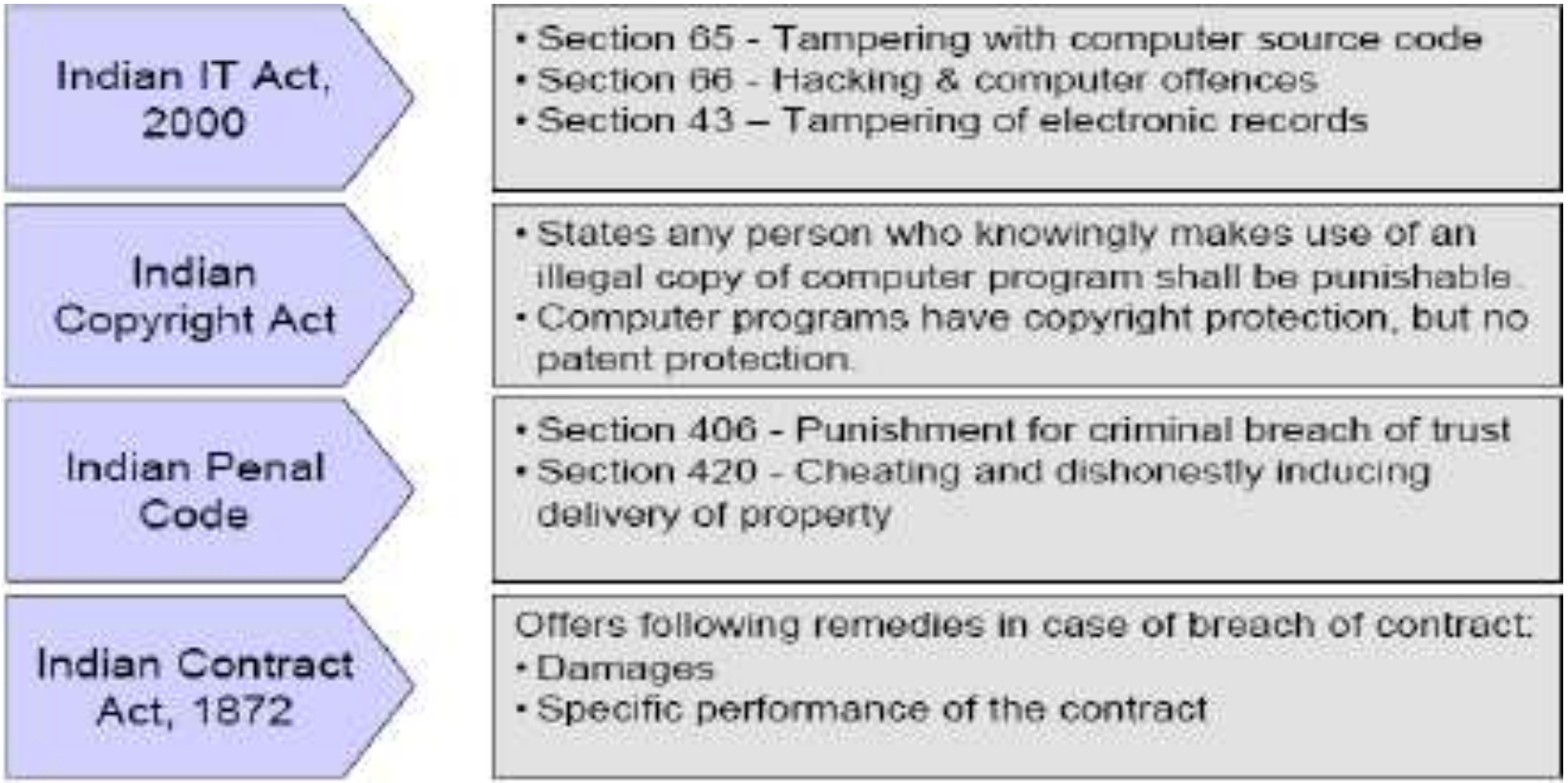
- Today's systems are Heterogeneous
- Pervasive environment
- Complex Architecture
- No 'one' ownership of the complete system
  - Different modules owned by possibly different vendors
- Cyber Security is a huge challenge in today's environment

ICT Infrastructure: Regulatory Issues

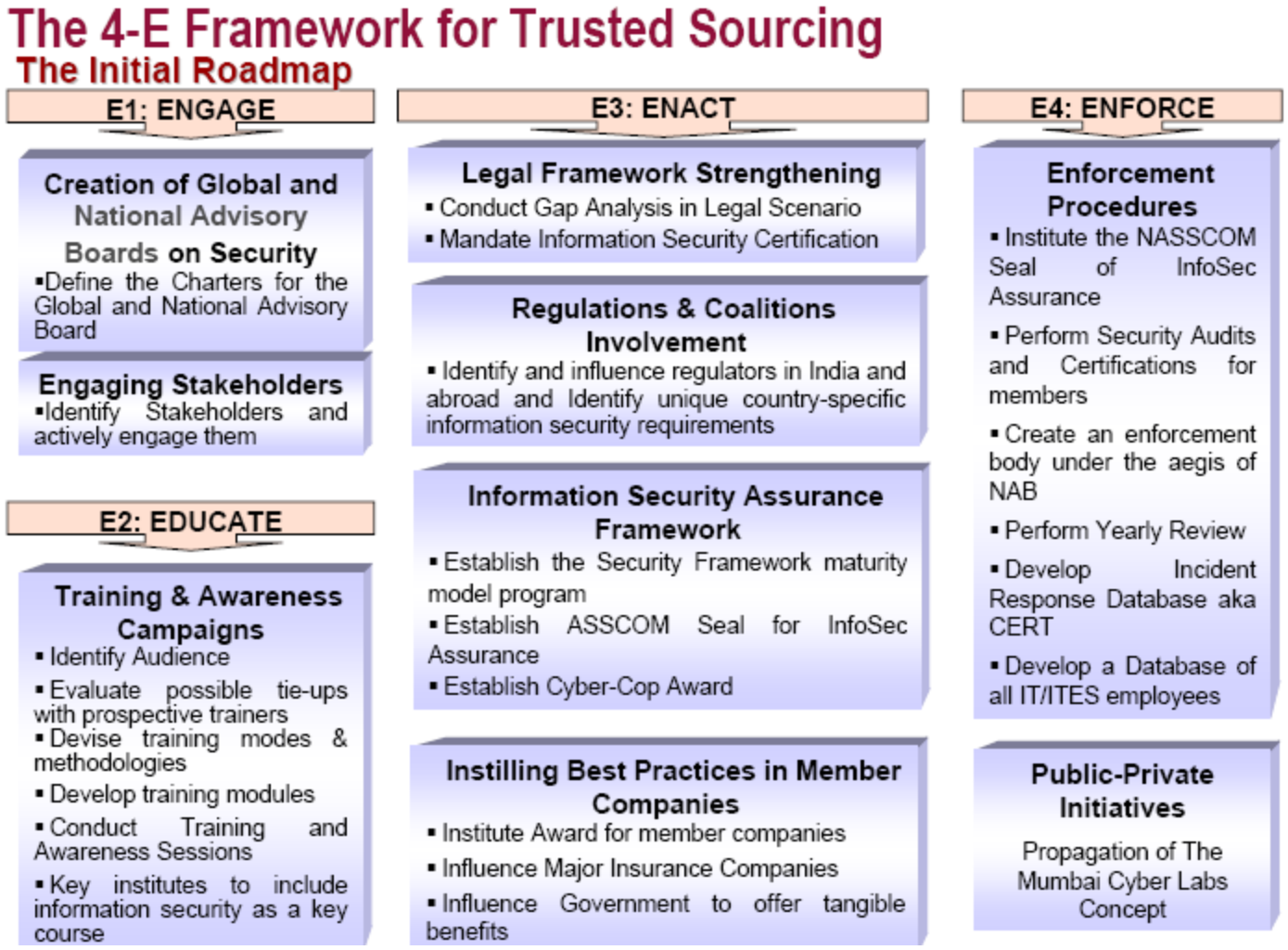


(Adapted from TRAI Consultation Paper on NGN)

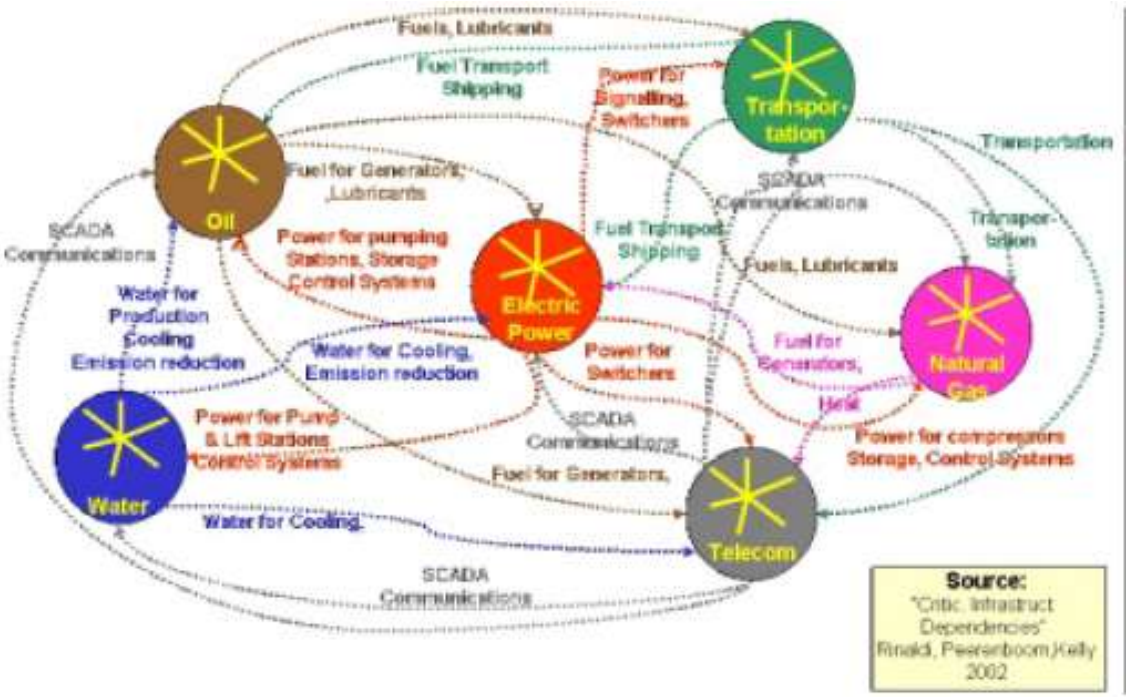
Legal Framework to Support Cyber Security in India



NASSCOM proposed 4-E Framework for Trusted Sourcing



Interdependencies of Critical Infrastructures



Scenario in India

- Inadequate cyber security in India, particularly for wireless networks
- This makes "wireless hacking" possible
  - Often used for committing cyber crimes
- Wireless hacking
  - Four step process that includes war driving, victim identification, passwords and encryption keys sniffing and finally hacking
  - If MAC filtering is in place the offender may go for the MAC address spoofing to trick the authentication process

USA: Cyber Security Act of 2010

- The bill seeks to increase collaboration between the public and the private sector on Cybersecurity issues
  - Especially those private entities that own infrastructures that are critical to national security interests
- Increase public awareness on Cybersecurity issues
- Foster and fund Cybersecurity research
- Controversial parts of the bill: Paragraph 315
  - Grants the President the right to "order the limitation or shutdown of Internet traffic to and from any compromised Federal Government or United States critical infrastructure information system or network”

National Cyber Security

- http://www.nationalcybersecurity.in/index-3.html
- **Penetration Testing**
  - A valuable first step in discovering the vulnerabilities in the Network, Servers and Applications
  - With expert security consulting to help clients cost-effectively reduce risk, achieve and maintain regulatory compliance and reach the security goals

.

- **Vulnerability Assessment**
  - Providing a clear and in-depth understanding of how vulnerable clients Network, Servers and Applications are to attack
  - Moreover determining vulnerabilities with network configurations and server configurations working with intranet applications and which have bugs or loopholes in them

- **Website Security Testing**
  - Reviewing clients custom applications to determine security weaknesses and provide a secure extension of business applications to increase customer confidence and minimize security issues and downtime of Network or Servers

- **Disaster Recovery And Source Code Audit**
  - ensures that you are prepared so that the business can continue to function with the least amount of impact possible in the case of a digital or physical disaster
  - Also thoroughly assess your applications, from both a technical and non-technical perspective, to determine security weaknesses and mitigate risks to the organization by providing detailed recommendations.

Real-time Traffic Intelligence

- What is Real-time Traffic Intelligence?
  - Real-Time Traffic Intelligence is the ability to protect and manage large IP networks by analyzing traffic behavior for a deeper understanding of the networks' health and safety

Challenges

- Today's service providers and government organizations face a diverse set of challenges in keeping their networks healthy while ensuring compliance with government mandates
- These organizations have become targets for increasingly complex and destructive attacks as well as targets for non-malicious, yet unwanted traffic such as spam
- Beyond the risk of network issues, terrorists and criminals are utilizing IP services to communicate and coordinate, leading to a variety of government mandates

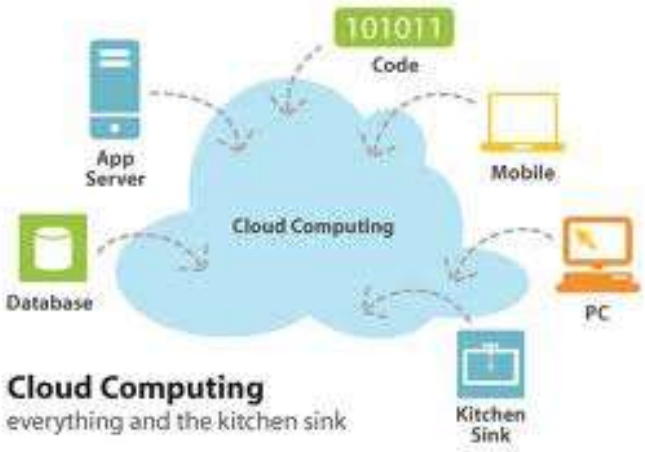
- With new services, new attacks and new behaviors becoming a regular part of daily network operations, monitoring and protection solutions need to be dynamic and adaptable or they risk becoming obsolete before being deployed
- Historically, service providers and government organizations have taken a siloed approach to monitoring and managing their networks, installing applications incrementally to address specific needs and to solved specific problems
  - This approach led to a dispersion of information across many products that do not interact with each other and further required a large operational investment to manage and maintain

Complex Systems Today

Cloud Computing

Cloud Computing Security

- Security in the cloud is challenging
  - Varied degree of security features and management schemes within the cloud entities
- One logical protocol base need to evolve so that the entire gamut of components operate synchronously and securely



Cyber Security Laws in India

- Wireless Security
  - http://perry4law.com/ptlb/cs.html
- http://www.csi-sigegov.org/emerging_pdf/9_70-84.pdf

Complex Systems Today

PKI Design for Secure V2X Communications for Safety

Vehicular Communications

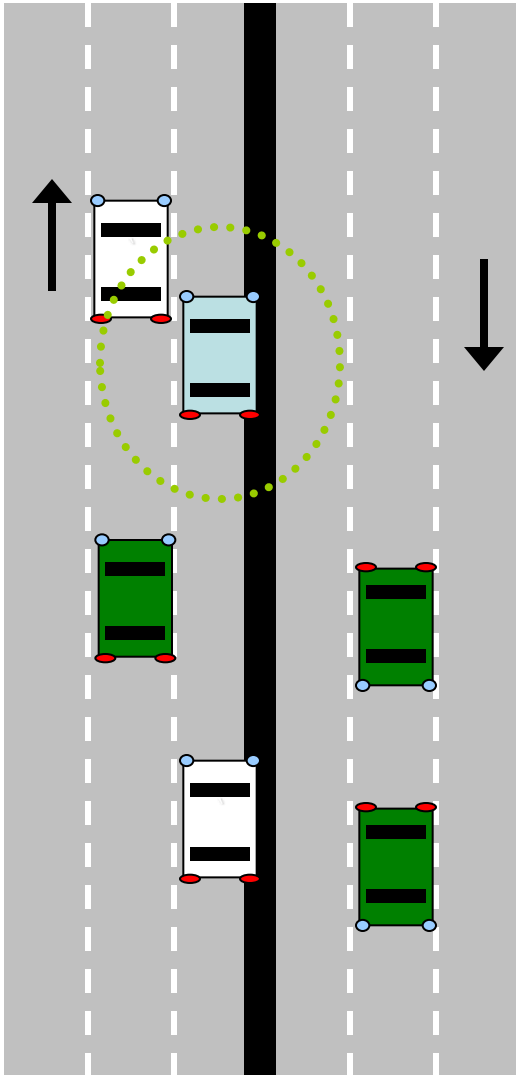
Approaches

- Vehicle to Infrastructure
  - Roadside Units
    - WLAN technologies
  - Base stations
    - Cellular technology
- Vehicle to Vehicle
  - DSRC standard
- In Vehicle
  - ZigBee

V2X Active Safety Applications

- **Event reporting** applications: (Early Apps)
  - Generate messages only for the duration of the event
  - Report events based only on information present at sending vehicle
  - Examples: EEBL (Emergency Electronic Brake Lights), RCHA (Road Condition Hazard Ahead)
- **Persistent** applications: (Later Apps)
  - Require repeated exchange of vehicle kinematics in a local neighborhood
  - Predict and report events by processing exchanged information
  - Examples: CCW (Cooperative Collision Warning), BSW (Blind Spot Warning)

Driver Interaction: Applications raise advisories or warnings to help the driver avoid accidents

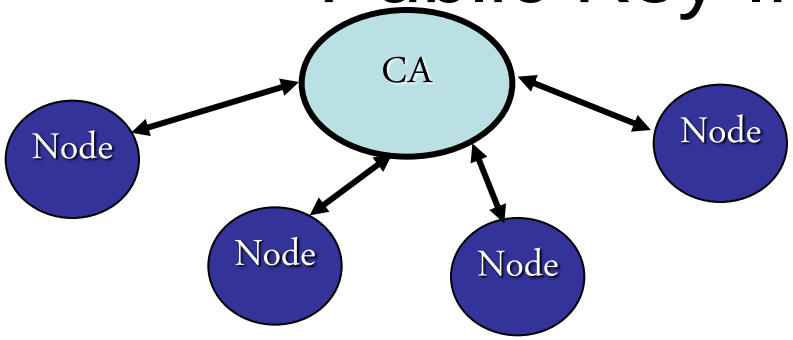


Security Attributes for V2X Safety Apps

- Message Integrity and Entity Authentication
  - Message has been transmitted by a **genuine** vehicle, and has **not been tampered** with in transit
- Non-repudiation
  - The receiver of a message is able to prove afterwards that the sender in fact did transmit this message.
- Privacy: Multiple notions of privacy
  - **Anonymity**: Not possible to determine the identity of the vehicle from a message transmitted by the vehicle.
  - **Unlinkability**: Not possible to deduce that multiple transmissions were from the same vehicle.
- Correctness based on non-cryptographic techniques
  - For detecting compromised/malfunctioning units

Design Objective: Satisfy above attributes without affecting performance of V2X Safety Apps

Reference Solution: Public Key Infrastructure (PKI)



PKI High-level Architecture

Message payload (m)
Digital signature on 'm'
Digital certificate

Message Structure

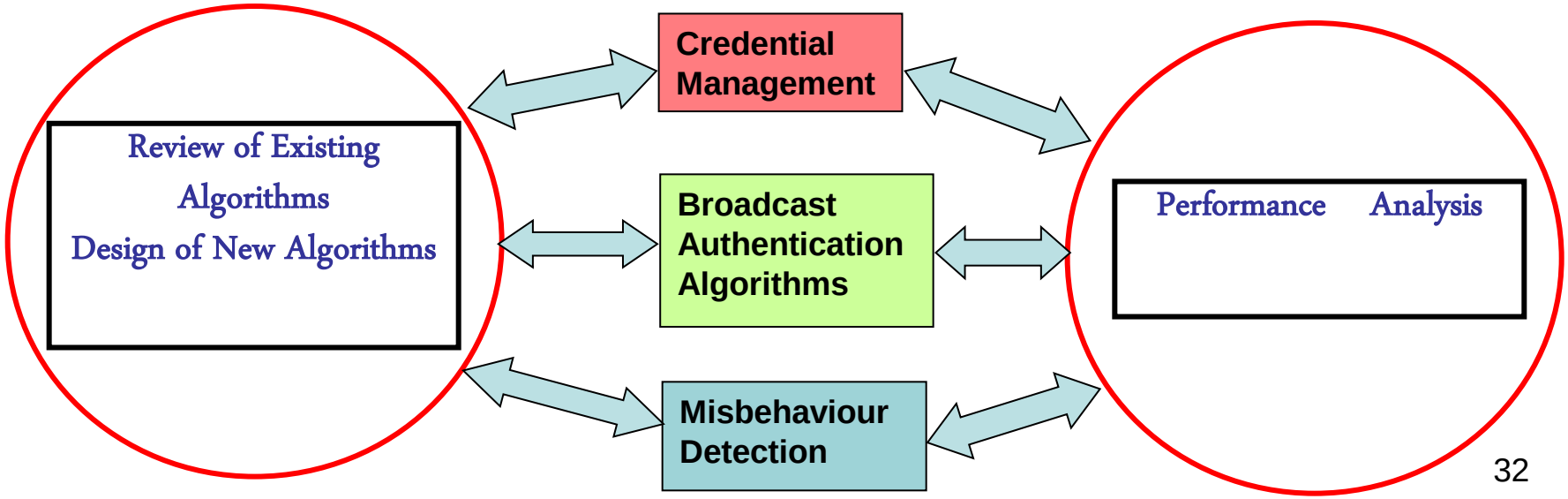
- How PKI enables nodes to talk to one another:
  - Asymmetric Key Cryptography: A message is signed using the Private key of the sender and verified using the Public key of the sender.
  - Certificate: A message signed by a trusted entity called the Certificate Authority (CA) that binds a principal and its public key
- How PKI evicts compromised/malfunctioning nodes from system:
  - Certificate Revocation List (CRL): A message signed by the CA that lists all the revoked principals
  - Freshness Certificate: A message signed by the CA that a certificate is valid as of the time of signing (proposed alternative mechanism)

Design drivers for a PKI for V2X Communications for Active Safety

- Resource-constrained Platform
  - Participants have **limited** computational prowess
  - Limited memory and storage
- System-wide Scalability Issues
  - **Large** number of participants with **many-to-many** interaction (individual participants need to authenticate one another)
  - However, interactions are also expected to be **spatially localized**
- Communication Aspects
  - Connection to Infrastructure is expected to be either **intermittent** or **costly**
  - Message transmissions are likely to be lossy and **unreliable**
- Interoperability
  - Security Architecture needs to be **extensible**

Securing V2V Communications

- Credential management (Infrastructure support)
  - Key distribution
  - Key renewal
  - Misbehaving node eviction
- Security processing at the signing/verifying entities
  - On board processor
  - On board memory
  - Wireless channel access mechanism
- Misbehavior Detection



Thank You

References

- http://www.cse.wustl.edu/~jain/cse574-06/ftp/j_bsec/sld010.htm
- http://www.narus.com/

References

- http://cyberlawsinindia.blogspot.com/2010/07/cyber-security-policy-of-india.html
- http://www.expresscomputeronline.com/20070409/market08.shtml
- http://www.thaindian.com/newsportal/uncategorized/cyber-security-in-india-another-wake-up-call_100155330.html
- http://cyberlawsinindia.blogspot.com/2010/04/cyber-security-of-india-is-in-poor.html

References

- http://www.thaindian.com/newsportal/press-release/cyber-law-in-india-where-are-we-heading-to_100152667.html
- http://www.mi2g.com/cgi/mi2g/frameset.php?pageid=http%3A//www.mi2g.com/cgi/mi2g/press/200110a.php