ON SECURITY-ENERGY TRADEOFFS AND COOPERATION FOR WIRELESS AD HOC NETWORKS

Cristina Comaniciu
Stevens Institute of Technology
A DIFFERENT PERSPECTIVE ON SECURITY FOR WIRELESS

- Security is a key requirement for wireless communications
- Energy is also a key performance metric
- Typically security and energy are treated as separate topics
- A different perspective: security and energy are inter-related
  - Security assurance mechanisms are usually energy hungry
  - Some types of attacks may lead to depleted battery for individual nodes
Security-Energy Tradeoffs

- Security mechanism often put a high toll on energy resources, as they may require extensive data acquisition, complex processing algorithms or/and substantial overhead for coordination.

- **Some Examples:**
  - Encryption – Algorithms – shown to consume a significant portion of a terminal’s battery (early work [Krishnamurthy et all, 2001]: 600 encryption operations for triple-DES reduces the battery availability to 45%)
  - Intrusion Detection Systems (IDSs) – require gathering, and complex analysis of substantial amounts of data
  - Physical Layer Security – requires additional transmissions for friendly jammers to mask the useful transmission
HOW TO CHARACTERIZE SECURITY-ENERGY TRADEOFFS

- Need to measure “the amount of security you get” for the “price of energy spent”
- **Security Gains** – related to classic performance metrics, such as:
  - IDSs – probability of miss detection
  - Encryption – resilience to cryptanalysis attacks.
  - Physical layer security – secrecy capacity
- **Energy Costs** – The amount of energy spent to obtain the security gains
  - Typically characterized by measurements + Some model fitting for specific security applications
EXAMPLES FOR ENERGY-SECURITY TRADEOFFS – ANALYTICAL MODELS - ENCRYPTION

[Chandramouli & all, 2006] – characterizes the power battery consumption for encrypting using various block cipher algorithms.

- Linear regression:
  - $P(r) = 0.0486r + 17.7335$ DES
  - $P(r) = 0.0975r + 18.015$ IDEA
  - $P(r) = 0.03321r + 17.90204$ GOST
Examples for Energy-Security Tradeoffs – Analytical Models – Intrusion Detection

- Security application: detect anomalous traffic behavior in the network using IDS – **security performance metric**: probability of detection

- **Energy Utility**: [Futaci, Runser, Comaniciu, 2008] extends and validates work in [Sinha et al, 2001]
  - measurements on the Freescale Semiconductor MC9S08GT60 Microcontroller (typical for a wireless ad hoc node) \( \rightarrow \) **first order approximation formula for energy expenditure as a function of algorithm complexity**

\[
E_{TOT} = V_{DD} \cdot I_0(V_{dd}, f) \cdot \frac{t(n) \cdot N \cdot c}{f}
\]

- Energy depends on:
  - supply voltage and current,
  - \( t(n) \) - time complexity function giving the total step count, \( n \) is the instance characteristic,
  - \( N \) - average number of machine instructions per step count,
  - \( c \) - average number of machine cycles per machine language instruction
  - \( f \) is the operation frequency of the computing platform.
COOPERATION FOR IMPROVING THE ENERGY-SECURITY TRADEOFFS

- Take advantage of the network structure – a sufficiently dense network may “time-share” the security duties

Challenges:
- Implement distributed algorithms – nodes take decisions independently with no centralized infrastructure
- Potentially selfish nodes: “Tragedy of the commons” – everybody would like to benefit, no one would like to pay the price – a classic game theoretic problem formulation – Incentivize cooperation?
- Selfish versus malicious nodes – ensure that cooperation is among trusted nodes, or/and security algorithms (e.g. IDS) are robust to malicious behavior.
DISTRIBUTED INTRUSION DETECTION SYSTEM (IDS)

Requirements:
- Independent decisions based on local information
  - Monitor, not monitor, or type of monitoring algorithm employed
- Local convergence to a given network operating point
- Game Theoretic Modeling – useful analysis tool
  - Players: nodes in a network neighborhood
  - Actions (Strategies): nodes’ monitoring decisions
  - Objective for individual nodes: maximize their individual utility (security gains – monitoring costs)
  - Nash equilibrium – the convergence point of the distributed algorithm → no player has incentive to unilaterally deviate
An Example IDS for Wireless Sentinel Networks

- Security application – wireless sentinel networks – monitor for illicit wireless transmissions in a network neighborhood (with or without ongoing legitimate traffic).
- No knowledge about the transmission waveforms of the intruder → energy detector
- Multiple nodes report estimated energy levels – soft information
- Access point aggregates reports - exploits diversity – MRC for overlapped sensing regions → builds 3D likelihood map
- Detection based on threshold – fixed probability of false alarm
**COOPERATION BENEFITS**

- Multiuser diversity enhances the detection accuracy
- Localization area → multiple reports with overlapped sensing regions
- Energy requirements reduced by “time-sharing” the monitoring load.
QUESTIONS TO BE ANSWERED

- Optimal strategy for nodes?
- Existence of Nash equilibrium?
- Cooperation gains?
- As a finite game a MIXED STRATEGY NASH Equilibrium is guaranteed to exist → nodes will monitor with an equilibrium probability $p_M$
  - Indifference principle: determined such that the average utility for monitoring = average utility for not monitoring.
- Game can be formulated as a
  - **Strategic form game** – we know that the intruder is present in the system (complete information), or
  - **Bayesian game** (static or dynamic) – we believe that the intruder might be present in the system (incomplete information)
  - The cost and utility definitions determine the operating point (NE) of the network
COOPERATION GAINS – A NASH EQUILIBRIUM ANALYSIS

- Cooperative detection – a form of MRC for individual energy readings – multiuser diversity gains

- Energy gains = [energy required for monitoring × (1-probability of monitoring) - collision resolution energy](multiple reports may collide)
Energy and security cost functions can be weighted by price functions

- Security value: $\varepsilon$
- Price per unit energy consumption: $\omega$
- $\varepsilon/\omega$ defines the relative importance of security and energy – can change the NE solution
CONCLUDING REMARKS

- Energy-Security Tradeoffs can be found that characterize security choices for individual nodes.
- Cooperation – provides better energy-security tradeoff curves for individual nodes.
- Cooperative security assurance algorithms – another form of exploiting multiuser diversity in wireless networks.
- Current research on security-energy tradeoffs still in its infancy - Many intriguing open problems remain to be solved for practical implementations.
QUESTIONS?

Thank you!