Secure Message Delivery Games for Device-to-Device Communications

GameSec 2014

Manos Panaousis

November 6, 2014

Future smartphones won't need cell towers to connect

- Vast demand for anytime-anywhere wireless broadband connectivity has posed new research challenges
- New feature being added to the LTE protocol will make it possible to bypass those towers
- Mobile devices are capable of communicating in both cellular (e.g. LTE) and unlicensed (e.g. Wi-Fi, LTE Direct) spectrum
- Phones will be able to "talk" directly to other mobile devices and to beacons located in shops and other businesses
- LTE Direct by Qualcomm
  - innovative **Device-to-Device (D2D)** technology that enables **discovering** thousands of devices and their services
  - proximity of approximately 500 meters

Applications

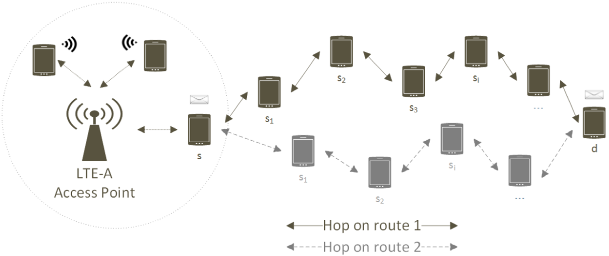
- Need for **localized applications**
- Need for **distributed communications** when telecommunications infrastructure:
  - are not presented at all (underground stations, airplanes, cruise ships, parts of a motorway, and mountains)
  - have collapsed due to physical damage to the base stations or insufficient available power (areas affected by a disaster such as earthquake)
  - are over congested due to an extremely crowded network (events in stadiums, and public celebrations)
- It can be leveraged for **commercial purposes**
  - promoting businesses due to the immediate identification of the clients in a surrounding area
  - voucher distributions (e.g. in large shopping centers)
- **Home automation**
- Provision of **anonymity** against cellular operators

Mobile malware

- **However**: devices can be a target for attackers
- Malware for mobile devices evolves in the same trend as malware for PCs
- It can spread for instance through a Multimedia Messaging System (MMS) with infected attachments
- An infected message might steal users personal data or credit stored in the device
- LTE Direct will open “new doors” to adversaries

Multi-hopping in D2D networking

- Emerging feature of D2D is the establishment and use of **multi-hop paths**
- enable communications among **non-neighboring devices**
- messages are delivered from a source (s) to a destination (d) via **intermediate devices**, independently of mobile operators' networks



System model

- We consider a D2D network with the set of mobile devices $\{s_i\}$
- We assume that each device has some host-based intrusion detection capabilities (e.g. antivirus)
- Each device has its own detection rate

Scenario

A device s injects a message to the network and requests its delivery to a destination device d

Challenge

Which is the **most secure route** to choose given the uncertainty about the message type?

Note

Apart from security, energy consumption and QoS need to be respected

System model

- R: the set of all routes from source to destination
- $\mathcal{M}$: all different types of messages
- $\mathcal{M} \triangleq \mathcal{M}_m \cup \mathcal{M}_b$ (i.e. malicious and benign)
- When $m_l \in \mathcal{M}_m$ stays undetected it causes harm $\mathcal{H}_l$ (e.g. data loss)
- Any false alarm has loss equivalent to $\mathcal{F}$ (e.g. loss of legitimate messages)

Confusion matrices

- **Device Confusion Matrix**
  - Linear mapping $C^{(s_i)}: \mathcal{M} \rightarrow \mathcal{M} \Rightarrow$ *detection capability* of s_i for a message received

$$C^{(s_i)} \triangleq [C_{uv}^{(s_i)}]_{\psi \times \psi}, \text{ where } 0 \leq C_{uv}^{(s_i)} \leq 1, \ \forall u, v \in \{1, \ldots, \psi\}$$

  - $C_{uv}^{(s_i)}$: probability of a message u being reported as message v
- **Route confusion matrix**
  - $C^{(r_j)}: \mathcal{M} \rightarrow \mathcal{M} \Rightarrow$ final detection capability on r_j
  - It is derived from the confusion matrices of the devices that constitute this route
  - **Linear combination algorithm**: each device contributes linearly to the final route detection capability by some weight
  - The device confusion matrix of the device can be seen as a classifier of a message
  - Route confusion matrix: representation of the weighted classifiers on the devices

Energy costs and QoS

- σ_i: detect any sign of malice (**security energy cost**)
- f_i: forward a message towards $\mathtt{d}$ (**forwarding energy cost**)
- $\mathtt{e_j} = \sum_{s_i} \sigma_i + f_i$: total *route energy cost* on r_j
- $\mathtt{E} \triangleq \langle \mathtt{e}_1, \ldots, \mathtt{e}_\xi \rangle$: energy costs of all routes between $\mathtt{s}$ and $\mathtt{d}$
- $\mathtt{H} \triangleq \langle \mathtt{h}_1, \ldots, \mathtt{h}_\xi \rangle$: #hops of all routes from $\mathtt{s}$ to $\mathtt{d}$ (**Quality-of-Service**)
- We measure the QoS of a route r_j as $\mathtt{h_j}/\mathtt{h}^\star$, where $\mathtt{h}^\star$ is the maximum possible number of hops in the network
- As the number of hops increases the probability of a message to be lost is higher i.e.

$$h \uparrow \Rightarrow \ QoS \downarrow$$

Network profile

$[w_s, w_{fa}, w_e, w_q]$

expresses preferences in terms of security, energy preservation, and QoS

- $\mathbf{w_s}$ - importance given to expected security damage (e.g. data theft)
- $\mathbf{w_{fa}}$ - importance of the false alarm cost (e.g. cost for dropping an innocent message)
- $\mathbf{w_e}$ - importance of the energy cost which can influence the network lifetime and speed up network fragmentation
- $\mathbf{w_q}$ - importance of the QoS (i.e. message success delivery rate and end-to-end delay)

Secure Message Delivery Game (SMDG)

- **Two players**:
  - **The defender** (D): abstracts any source (s) node which must establish a route to a message destination (d)
  - **The attacker** (A): abstracts any adversary who aims at infecting a destination by sending malware attached to a message
- **Game characterisation**
  - **Zero-sum game**: the attacker aims at causing the **maximum possible damage** to the network communications
  - **Complete information** game

Limitation

We see that as a starting point of our work and we intend to advance the model by investigating an incomplete information game

Strategies

- **Pure Strategies**:
  - ▷ D: Selects **a route** r_j to send a message from `s` to `d`
  - ▷ A: For a destination device, injects a **message** m_l (e.g. surveillance, benign, or malicious aka malware) to the network
- **Mixed Strategies**:
  - ▷ D: **Confuses** the attacker by using a mixed strategy
  - ▷ A: **Sends** several different messages to increase likelihood of damage

Payoffs

- The payoff of D for a given pair of players' pure strategies (r_j, m_l)

$$U_D(r_j, m_l) \triangleq -w_s(1 - C_{ll}^{(r_j)})\mathcal{H}_l \; - \; w_{f_a}(1 - C_{ll}^{(r_j)})\mathcal{F} - w_e e_j - w_q h_j.$$

- Mixed strategies
  - ▷ $\mathbf{D} \triangleq [q_1, \ldots, q_\xi]$
  - ▷ $\mathbf{A} \triangleq [p_1, \ldots, p_\psi]$
- When considering mixed strategies

$$\begin{aligned} U_D(\mathbf{D}, \mathbf{A}) \; & \triangleq -w_s[\sum_{m_l \in \mathcal{M}_m} \sum_{r_j \in R} q_j \, (1 - C_{ll}^{(r_j)}) \, p_l \, \mathcal{H}_l] \\ & -w_{f_a}[\sum_{m_l \in \mathcal{M}_b} \sum_{r_j \in R} q_j \, (1 - C_{ll}^{(r_j)}) \, p_l \, \mathcal{F}] \\ & -w_e \mathbf{D}\mathrm{E}^T \; - \; w_q \mathbf{D}\mathrm{H}^T \end{aligned}$$

Equilibria

Nash message delivery plan ($\mathbf{D}^*$)

It is a probability distribution over the different routes, as determined by the NE of the SMDG

- From minimax theorem

$$\mathbf{D}^* = \arg\min_{\mathbf{D}} \max_{\mathbf{A}} U_A(\mathbf{D}, \mathbf{A}) \Rightarrow \textbf{minimises the damage}$$

- **i.e.**: Regardless of the strategy the attacker chooses, the Nash message delivery plan is the defender's security strategy that guarantees a minimum performance

Secure Message Delivery (SMD) routing protocol

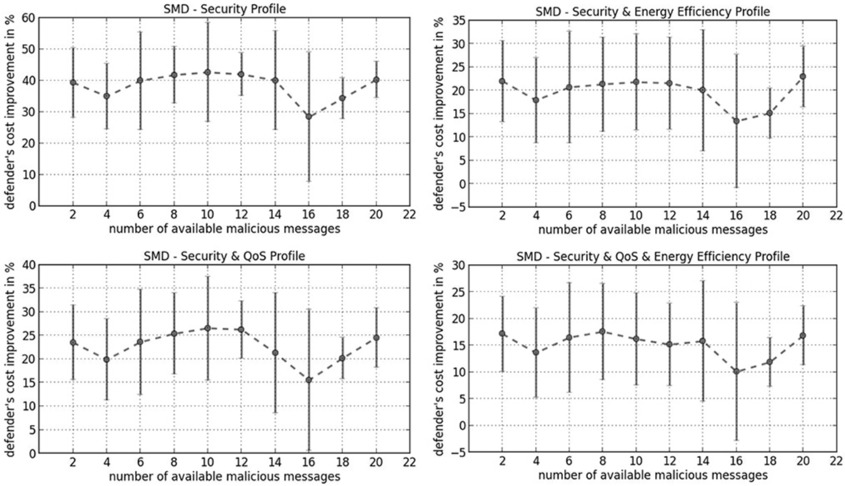
- Selects a route according to the Nash message delivery plan to increase the probability of detecting malicious messages
- The source device uses its latest information about confusion matrices, QoS and energy costs to derive the Nash plan
- A message is relayed and collaboratively inspected by the devices on its way to the destination

Simulations

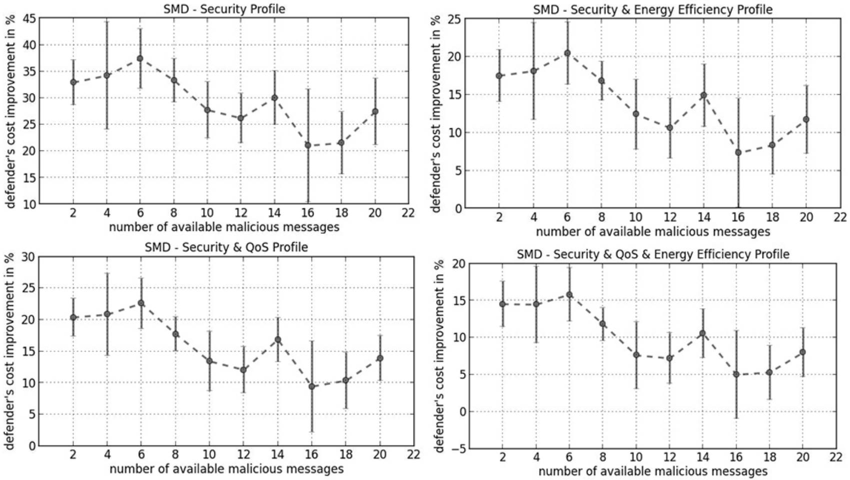
- 10 **Cases**: different number of available malicious messages
- For each Case we have simulated 1,000 **message deliveries**
- ⟨Case,#message deliveries⟩ by the term **Experiment**
- We have repeated each Experiment for 25 independent network topologies to compute the standard deviation
- We consider 2 different attacker profiles
  - ▷ **Uniform**: chooses any of the available messages with the same probability
  - ▷ **Nash**: plays the attack mixed strategy given by the NE of the SMDG

Network Profile	w_s	w_{fa}	w_e	w_q	Network Profile	w_s	w_{fa}	w_e	w_q
Security	10	0.5	0	0	Security & Energy Efficiency	5	0.5	5	0
Security & QoS	5	0.5	0	5	Security & QoS & Energy Efficiency	4	0.5	3	2.5

SMD vs. Shortest path routing protocol - Uniform attacker



SMD vs. Shortest path routing protocol - Nash attacker



Future Work

- Bayesian Games
  - ▷ Uncertainty about the adversary's payoff
  - ▷ We will investigate different attacker types by using different malicious types distributions from reports (e.g. Verizon Data Breach Investigations Report)
- Adversaries' Strategies
  - ▷ A pure strategy for the attacker will include both device destination and message type
  - ▷ In this way, targeted attacks will be mitigated
- Results Validation
  - ▷ A wireless testbed is under development, and actual malware infection of devices will be attempted
  - ▷ Also we will use a network simulator where wireless interface is taken into account along with other to test the scalability of results aka when the network size increases how does computation of the Nash message delivery plan perform?

Questions