ALGORITHMS FOR ADVANCED CLANDESTINE TRACKING IN SHORT-RANGE AD HOC NETWORKS

The 2nd International ICST Conference on Security and Privacy in Mobile Information and Communication Systems (MobiSec ’10)

May 27th, 2010

Saif Al-Kuwari\textsuperscript{1,2} \quad Stephen Wolthusen\textsuperscript{1,3}

\textsuperscript{1}Info. Sec. Group, Royal Holloway, University of London, Egham TW20 0EX, UK
\textsuperscript{2}Dept. of Info. and Research, Ministry of Foreign Affairs, P.O.Box 22711, Doha, Qatar
\textsuperscript{3}Norwegian Info. Sec. Lab., Gjøvik University College, P.O.Box 191, N-2802 Gjøvik, Norway
OUTLINE

- Motivation & Overview
- Basic tracking
  - *Single-tracker single-target tracking*
- Advanced Tracking
  - *Multiple-tracker single-target tracking*
    - *Handover tracking*
  - *Single-tracker multiple-target tracking*
    - *Virtual tracking*
  - *Multiple-tracker multiple-target tracking*
- Transmission algorithm
- Fault Tolerance
- Simulation results
- Tracking Accuracy
- Privacy & Legal Implications
OVERVIEW & MOTIVATION

- Tracking is an emerging application can either be:
  - **Active**: target is aware of tracking (e.g. tracking children)
  - **Passive**: target is unaware of tracking (e.g. criminals tracking)
- In this work, we consider passive tracking because it is more relevant to law enforcement and slightly less studied.
- Proposed tracking algorithms are generic (applicable to any mobile ad hoc technology)
- We proposed an agent-based tracking, entities involved:
  - **Target**: entity to be tracked (e.g. suspect/criminal)
  - **Tracker**: entity initiating the tracking (e.g. law enforcement)
  - **Agent**: random entities from the public that happen to present around the target during tracking, and are being recruited by the tracker to carry out the tracking.
OVERVIEW & MOTIVATION

Agents form small master-slave ad hoc networks (called piconets) which are either:

- **Tracking piconet**:
  - This is where localization takes place
  - Master is called *tracking-master*, and slave is *tracking-slave*
  - There is only one tracking piconet (per target)
  - This piconet must consist of at least 3 agents

- **Connecting piconet**:
  - connect tracking piconet with tracker(s)
  - Master is called *connecting-master*, slave is called *connecting-slave*
  - There can be arbitrary no. of connecting piconets (as necessary)
  - This piconet must consist of at least 2 agents
OVERVIEW & MOTIVATION
TRACKING SCENARIOS

- **Scenario 1:**
  - *Single tracker* tracking *single target*

- **Scenario 2:**
  - *Multiple trackers* tracking *single target*

- **Scenario 3:**
  - *Single tracker* tracking *multiple targets*

- **Scenario 4:**
  - *Multiple trackers* tracking *multiple targets*
**Basic Tracking**

- Single tracker tracking single target [AW09]
- The target is localized by the tracking piconet
  - *Trilateration* is used to localize the target where 3 reference points (agents) localize the target
- Tracking info. is then sent to the tracker and saved in a *tracking database*.
TRACKING SCENARIOS

- **Scenario 1:**
  *Single tracker* tracking *single target*

- **Scenario 2:**
  *Multiple trackers* tracking *single target*

- **Scenario 3:**
  *Single tracker* tracking *multiple targets*

- **Scenario 4:**
  *Multiple trackers* tracking *multiple targets*
ADVANCED TRACKING

- Multiple tracker tracking single target
- In this scenario, we introduce *handover tracking*
- We assume trackers are securely connected
  - This allows them to synchronize *tracking database*
- Usually, tracking network is handled by single tracker, but if the network breaks down, the *detecting-piconet* searches for any genuine tracker
  - If found, handover the tracking to it
  - Otherwise, the tracking-master becomes a *temporary tracker* and creates a *temporary tracking table*
- **Problem:** how can the *detecting piconet* authenticate a genuine tracker?
ADVANCED TRACKING

- Multiple tracker tracking single target
- Secure handover!
  - Trackers and all agents share a secret key (supplied to agents upon recruitment)
  - We proposed a simple 3-way handshake authentication protocol, similar to CHAP ($r_i$ is a random number, $h(.)$ is a hash function, tempTT is the temporary tracking table)
TRACKING SCENARIOS

- **Scenario 1:**  
  *Single tracker* tracking *single target*

- **Scenario 2:**  
  *Multiple trackers* tracking *single target*

- **Scenario 3:**  
  *Single tracker* tracking *multiple targets*

- **Scenario 4:**  
  *Multiple trackers* tracking *multiple targets*
ADVANCED TRACKING

- Single tracker tracking multiple target
- In this scenario, we introduce *virtual tracking*
- In this scheme,
  - Every target has a separate *Virtual Tracking Network (VTN)*
  - VTN’s consist of:
    - Virtual Piconets (VP): each has a VPID
    - Virtual agents (VA): forming VP’s and each has a VAID
  - A single (physical) piconet or agent may possible have multiple VPID’s and VAID’s, respectively.
ADVANCED TRACKING

- Single tracker tracking multiple target
TRACKING SCENARIOS

- **Scenario 1:**
  - *Single tracker* tracking *single target*

- **Scenario 2:**
  - *Multiple trackers* tracking *single target*

- **Scenario 3:**
  - *Single tracker* tracking *multiple targets*

- **Scenario 4:**
  - *Multiple trackers* tracking *multiple targets*
TRACKING SCENARIOS

- **Scenario 1:**
  - *Single tracker* tracking *single target*

- **Scenario 2:**
  - *Multiple trackers* tracking *single target*

- **Scenario 3:**
  - *Single tracker* tracking *multiple targets*

- **Scenario 4:**
  - *Multiple trackers* tracking *multiple targets*
TRANSMISSION ALGORITHM

- To minimize the observability, it is recommended that the tracking-master doesn’t always send the tracking information through the same route to the tracker.
- By recruiting *additional* agents around the tracking-master, we create additional (redundant) routes.
FAULT TOLERANCE

- Minimum number of agents:
  - Tracking piconet: 3
  - Connecting piconet: 2

- **Recommendation**: recruit extra *backup* agents, so:
  - Tracking piconet: 3 + 3 (backups) = 6
  - Connecting piconet: 2 + 2 (backups) = 2

- Every agent is paired with a backup agent, so a failure in either is detected by the other by means of alive messages which are exchanged frequently among them.
FAULT TOLERANCE
SIMULATION

- We investigate the effect of mobility models and node density on the tracking process.
- In particular, we are mostly concerned about the period under which the tracking network is under *temp tracker*.

Scenario setting:
- Simulation area: 250 m²
- Targets: 10
- Trackers: 3
- Node densities:
  - Scenario 1: 20
  - Scenario 2: 50
  - Scenario 3: 80
  - Scenario 4: 100
  - Scenario 5: 120
- Mobility models:
  - *Random Waypoint*
  - *Brownian Walk*
  - *Gauss-Markov*
SIMULATION

Random Waypoint

Time

Node Density

Brownian Walk

Time

Node Density

Gauss-Markov

Time

Node Density

Target 10
Target 9
Target 8
Target 7
Target 6
Target 5
Target 4
Target 3
Target 2
Target 1
TRACKING ACCURACY

- RF measurements have an unavoidable error margin
- However, careful investigation of the signaling used in a particular technology may lead to better estimation
  - E.g. recent work [HS07] showed that measuring the Bluetooth’s **Received Power Level** usually yields better estimation than other Bluetooth parameters.
Privacy & Legal Implications

- Passive and agent-based tracking raise a number of legal and ethical concerns
- However, we assume that such procedures are conducted by law enforcement, where they are covered by national legislation, e.g. Regulation of Investigatory Powers Act (2000), in UK.
THANK YOU ...