Using Trajectory Sensor Data Stream Cleaning to Ensure the Survivability of Mobile Wireless Sensor Networks in Cyberspace

Dr. Niki Pissinou, PI
Dr. Laurent Yamen Njilla, Ph.D student (now at AFRL)
Dr. Charles Kamhoua, Collaborator, AFRL
Dr. S.S. Iyengar, Collaborator, FIU
Col. Jerry F. Miller USAF (Ret.)
Dr. S.S. Iyengar, Collaborator, FIU
Col. Jerry F. Miller USAF (Ret.)
Concepcion Zulema Sanchez de Rodriguez (Ph.D. Student)
Samia Tasnim (Ph.D. student)
Ming Ming Guo (Ph.D. Student)
NSF-DOD REU SITE, NSF RET Site participants
Project Objectives

1. Design and develop a context-based trajectory data model that illustrates the physical, spatial-temporal, symbolic, absolute, relative and uncertain context of trajectories in mWSNs.

2. Design and develop a game-theoretic trajectory secrecy safeguarding mechanism in mWSNs.

3. Design and develop a lightweight energy-efficient framework that integrates trajectory secrecy with security protection techniques.
What is it about?

- Mobile, Trajectory, Wireless Sensor Network
  - Sensor Nodes talking to each other
  - Nodes talking to “some” node in another network
  - Limited resources
    - E.g., limited in power, computation, memory prone to failures, sensor nodes may not have global id
- Trajectories
  - physical, spatial-temporal, symbolic, absolute, relative and uncertain context of trajectories
- Event mobility
  - Event that is to be observed moves around (or extends, shrinks)
  - Different nodes become “responsible” for surveillance of such an event
What is it about? (cont.)

- Do not only deliver bits from one end to the other
  - Provide information, not necessarily original bits
    - E.g., manipulate or process the data in the network
    - E.g., apply aggregation functions
- Exploit location information
  - Required anyways for many applications; can considerably increase performance
- Exploit activity patterns and context
  - E.g., stop and go
- Exploit heterogeneity
  - By construction: nodes of different types in the network
  - By evolution: some nodes had to perform more tasks and have less energy left; some nodes received more solar energy than others
Recap from IBM Meeting

• A belief-based sensor selection to help clean sensor data streams in sparse mWSNs

• Cleaning process consider unsynchronized sampling time of data streams from mobile sensors

• Game-theoretic trajectory secrecy safeguarding mechanism in mWSNs

• Area boundaries need to be known; however, in many scenarios they might be unknown and dynamic.

• Semantic Context: Information that can be used to characterize a situation. Examples: Location, time, date, social situation, traffic condition, network connectivity, communication cost, nearby resources, etc.
  E.g., Does a certain location or means home, office or road for a specific user?

• In-Networking processing was missing
First Year Status

• Context-Based Annotated Data Stream Model for Trajectory mWSNs
  – supports the development of a sensor selection process by providing the definition and format of dependencies among trajectory relationships.
  – illustrates the physical, spatial-temporal, symbolic, absolute, relative and uncertain context of trajectories in mWSNs.
  – defined relevant and meaningful annotation semantics for each trajectory type in a heterogeneous environment
    • At the lower level of granularity but beyond the spatio-temporal
  – characterized the relationship between two trajectories in an online fashion
  – classified the trajectory relations and designed an annotation algorithm that is computationally efficient
• A game-theoretic trajectory secrecy safeguarding mechanism in mWSNs.
  – illustrates the physical, spatial-temporal, symbolic, absolute, relative and uncertain context of trajectories in mWSNs.
  – supports the development of a sensor selection process by providing the definition and format of dependencies among trajectory relationships.
    • Modeling the spatio-temporal granularity to annotate meaningful semantics to each trajectory type in a heterogeneous
  – Focus on annotation data model for semantic trajectory data streams
  – Modeling the spatio-temporal granularity to annotate meaningful semantics to each trajectory type in a heterogeneous
  – How is the most relevant and helpful annotation data defined and chosen for cleaning sensor data?
  – classifying the trajectory relations and design the annotation algorithms to be computationally efficient
  – Characterizing the relationship between two trajectories in online fashion
• A game-theoretic trajectory secrecy safeguarding mechanism in mWSNs.

• Dynamics of Data Delivery
  
  • Nodes are completely mobile or semi mobile
  
  • The network topology constantly changing
  
  • The result is a limited amount of bandwidth due to the mobility of neighboring nodes
  
  • Node mobility can break down many solutions proposed to enforce cooperation.
  
  • Reputation may not be well-defined due to mobility
  
  • Previous research using game theory fail to characterize the mobility of individual rational and feasible payoff
A Bargaining Game Approach

Game Formulation

• Source node needs to forward data broadcasts its request to all node in transmission range.

• Neighboring nodes reply to source request with an answer including some detail attributes:
  - Speed, direction, coordinate, energy level, storage space available

• Prerequisites: intermediary node can only volunteer its service if it has the minimal requirements to carry out the work.
A Bargaining Game Approach

- The source can select from all the respondents the most appropriate based on attributes provided.
- The bargaining between the source and the intermediate node can start.
- There will be no data transfer unless both parties agree on the splitting rules before data communication starts.
A Bargaining Game Approach

- Player 1 has data to be forwarded to destination or AP
- $P_1$ also prefers to obtain as much resource as possible
- Player 2 is the intermediate node and he has the resource to carry out the data packets but prefers to keep as much as possible in order to fulfill other requests
- The bargaining game proceeds between players by alternating offers: by either “Accept” or “Reject”.
Our Approach

- K is the total amount of resource available to player 2.
- Delta (δ) is the discount factor δ ∈ [0, 1]
- P₁ proposes splitting rule is (x, K-x) to P₂ whom can accept or reject, if rejected
- P₂ makes an offer to P₁

<table>
<thead>
<tr>
<th>Periods</th>
<th>Offerer (Source Node)</th>
<th>Receiver (Mobile node)</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>K-l</td>
<td>1</td>
</tr>
<tr>
<td>2</td>
<td>K-Kδ^2 + δ^3</td>
<td>Kδ - δ</td>
</tr>
<tr>
<td>3</td>
<td>K-Kδ^2 + Kδ^3 + δ^3</td>
<td>Kδ^2 - Kδ^3 + δ^3</td>
</tr>
<tr>
<td>4</td>
<td>K-Kδ^2 + Kδ^3 + δ^3</td>
<td>Kδ^2 - Kδ^3 - δ^3</td>
</tr>
<tr>
<td>...</td>
<td>...</td>
<td>...</td>
</tr>
<tr>
<td>P</td>
<td>K-Kδ^2 + ... + δ^n</td>
<td>Kδ^2 + Kδ^3 + ... + δ^n</td>
</tr>
</tbody>
</table>

...
The Solution of the Bargaining Game

- the unique SPE in the last period before device goes out of range

$p$ is even: the SPE split offered by player $i$ is:

$$\frac{K(1 - \delta + \delta^2 - \ldots - \delta^{p-1})}{1 + \delta} = \frac{K(1 - \delta^p)}{1 + \delta} + \delta^{p-1}$$

Also, player $i$ accepts any split equal to or less than:

$$\frac{K(1 + \delta^{p-1})\delta}{1 + \delta} - \delta^{p-1}, \delta \in [0,1]$$

$p$ is odd: the SPE split demanded by player $i$ is:

$$\frac{K(1 - \delta + \delta^2 - \ldots + \delta^{p-1})}{1 + \delta} = \frac{K(1 + \delta^p)}{1 + \delta} - \delta^{p-1}$$

Also, player $i$ accepts any split equal to or less than:

$$\frac{K(1 - \delta^{p-1})\delta}{1 + \delta} + \delta^{p-1}, \delta \in [0,1]$$
The Unicity of SPE Solution

• According to Stahl [10], the safety payoff value of a player in a game is the guaranteed amount the player can get in the bargaining game.

• Let $m_1$ and $M_1$ be $P_1$ lowest and highest payoff values in any SPE where $P_1$ makes an offer.

• Denote $n_1$ and $N_1$ be the lowest and highest payoff values for $P_1$ game in which $P_2$ makes the offer.

• $m_1 \geq K - \delta M_2$;
• $M_2 \geq K - \delta M_1$; $P_1$ will not reject a split of more than $\delta M_1$
• $N_1 \geq \delta M_1$ because $P_2$ will never offer a share greater than $\delta M_1$.

• Since $P_1$ can obtain at least $m_1$ in the continuation game by rejecting $P_2$’s offer, $P_1$ will reject any $x$ such that $x < \delta m_1$. Thus, $n_1 \geq \delta m_1$
  • $m_1 = M_2 = K/(1+\delta)$;
  • $N_2 = n_2 = K\delta/(1+\delta)$
The Bargaining Algorithm

Require: # player, N=2; Time period before out of range, T; Payload, Q; time transferring a packet, t; Cost factor, δ;

Initialization: Commitment level value for player 1 and 2 is c_1 and c_2 respectively;

1: c_1 ← value; c_2 ← value;
2: While T > 0 do
3:   Player 1 proposes z_1 and z_2 = Q - z_1, (z_1, z_2) with \( z_1 \geq c_1 \)
4:   Player 2, accept ← (z_2 ≥ c_2; True, False)
5:   If !accept then
6:     T ← T - t; z_1 ← z_2; z_2 ← Q - z_1;
7:   player 2 proposes z_3; (z_3, z_2) with \( z_3 \leq c_2 \)
8:   player 1, accept ← (Q - z_2 ≥ c_1; True, False)
9:   If !accept then T ← T - t; goto 4; Else Transfer Q; Break; End if
10:  Else Transfer Q; Break; End if
11:  4: z_1 ← z_2, δ; z_2 ← Q - z_1
12:  End While

The OMNET++ is a discrete-event network simulation framework. The goal of this framework project is to develop a preferred, and open simulation environment for networking research.
Simulation Results

TOPSIS: Technique for Order Preference by Similarity to Ideal Solution
BGANS: Bargaining Game based Access Network Selection
What about Colluding Nodes?

• This far we showed that each autonomous mobile node’s participation in network lifetime depends on its whilst to route other nodes packets.

• The game theoretic model helps minimize the waste of resources during data transfer.

• The resources allocation takes into consideration multiple contextual factors: duration of connection, the mobility pattern, payload, etc..

• But what about colluding nodes?
Resource Allocation with Colluding Nodes

Assumptions

• Each node is autonomous and selfish
  • Node acts only for its own self-interest
  • Node tries to maximize its expected payoff
• Malicious nodes acts against network objectives
• Malicious node deliberately wastes others resource
• Malicious nodes can regroup as a coalition to attack
• Communication channel is bidirectional
• Energy consumption is high when node uses its wide radio transmission
Resource Allocation with Colluding Nodes

• The players are the nodes
• Players can ‘accept’ or ‘reject’ offers made by the arbitrator
• An arbitrator is a node with specific functions
  • Only arbitrator makes multiple offers
  • Arbitrator acts as a cluster head
  • Arbitrator generates offers randomly
  • Arbitrator can estimate dwelling time
• Arbitrator computes decisions from response based on simple majority
3-Player Bargaining Game

- An offer from the arbitrator is accepted if at least 2 out of 3 players consent.
- The utility \((U_k)\) value of the negotiation game for \(P_1\) meets:
  - at period \(k\) and \(U_0 << \frac{1}{3}\) for simple majority.
  
  \[
  U_k = \frac{1}{3} - 2\delta^2 U_{k-1}^2 + 6\delta^3 U_{k-1}^3
  \]

- For complete consent, the utility \((U_k)\) payoff value of the negotiation for \(P_1\) meets:
  - at period \(k\) and \(U_0 << \frac{1}{3}\).
  
  \[
  U_k = \delta U_{k-1} + \frac{1}{3}(1 - 3\delta U_{k-1})^3
  \]
Simulation Environment

- A predetermined amount of nodes colluding to subvert the arbitrator.
- Colluding nodes are one-hop away from each other and move within the area to keep their connectivity.
- Minimum number of colluding nodes is 2.
Percentage of successful negotiation sessions, with minimum payload 1667-3334 bytes

Percentage of successful negotiation sessions, with minimum payload 3500-4000 bytes
The Road Ahead

- In certain scenarios, context of sensor operations can be used to find out correlation of sensor streams better than sensors’ trajectory relationships.
  - E.g., the readings of two soldiers’ stress level are not necessarily reflected by the proximity of the soldiers. Instead, the readings might be reflected by other “context semantics,” such as the number of hours a soldier sleeps per night and number of hours on duty.
  - In contrast to the previous direction that considers only trajectory relationships, in this stage one will focus surrounding environments and contexts.
  - develop a comprehensive data cleaning method for mWSNs that integrates context awareness and semantic trajectory relationships
- Focus on uncertainty
  - sensors’ trajectory data are uncertain: localization uncertainty, indoor data loss, etc.
  - develop an efficient online trajectory knowledge extraction technique for estimating imprecise sensor locations that tolerates trajectory uncertainty
- Augmenting Game to safeguard trajectories
Selected Publications

- Do, Tran, Hong, Kamhoua, Blascch, Ren, Pissinou, Iyengar, Game Theory for Cyber Security and Privacy, ACM Computing Surveys (under review)