MILCOM 2015
LEVERAGING TECHNOLOGY—THE JOINT IMPERATIVE
OCTOBER 26–28, 2015 • TAMPA, FL

On Detection and Concealment of Critical Roles in Tactical Wireless Networks

Zhuo Lu
University of Memphis

Cliff Wang
Army Research Office

Mingkui Wei
NC State University

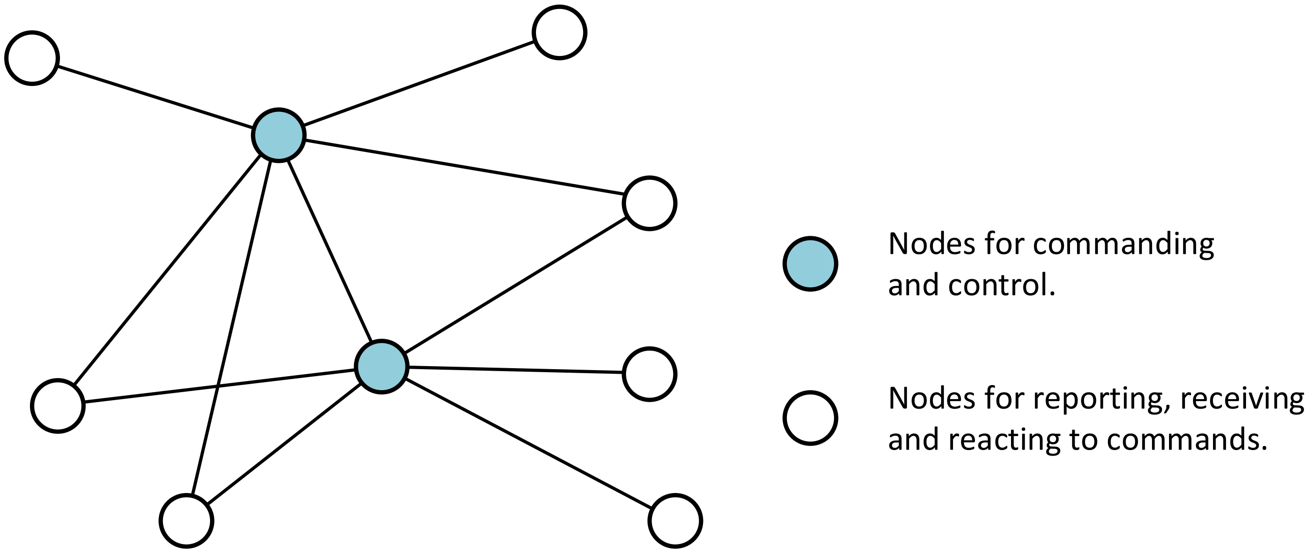
1. **Introduction**
2. System Models
3. Role Detection
4. Role Concealment
5. Conclusion

Introduction

- **Tactical wireless networks:**
  - Mission-critical mobile ad-hoc networks.
  - Allows two-way communication for warfighters.
  - Unique challenges due to tactical requirements, e.g., reliability and security in hostile environment.

Introduction

- **Characters of tactical wireless network:**
  - Nodes in the network are not homogenous.
  - Commanding and control nodes lead to a one-to-multiple communication model.



Research Question

- **How to detect and conceal the roles of nodes in tactical wireless networks?**
  - Roles of nodes:
    - Commanding role: # of active network flow with other nodes exceeds a given threshold (not necessarily real commanders).
    - Acting role: otherwise.
  - Two-fold questions:
    - Whether we can accurately identify commanding nodes in a network from an *adversary*'s point of view.
    - Whether we can protect such nodes from being identified from a *defender*'s point of view.

Contributions

- Provide an initial study on role detection and concealment, which are important in tactical wireless networks.
- Propose role detection and concealment methods and comprehensively evaluate their performance.

1. Introduction
2. **System Models**
3. Role Detection
4. Role Concealment
5. Conclusion

Network Model

- **Network Model**
  - Consider a network with *n* nodes distributed on region $\Omega = [0, \sqrt{n/\lambda}]^2$ independently and uniformly.
  - *Node density* λ is large enough such that the network is connected.
  - Two nodes are connected if within each other's transmission range r.

Roles of Nodes

- **Commanding and Acting roles:**
  - A node is *commanding* if it has network flows with rates in rate region Σ to/from at least n_c nodes.
    - For example, $\Sigma = [500Kbps, +\infty)$, $n_c = 10$.
  - A node is *acting* otherwise.
  - Mathematically representation:
    - $R_i = \begin{cases} 1 & if\ node\ i\ is\ commanding, \\ 0 & if\ node\ i\ is\ acting. \end{cases}$
    - A *role vector* $\boldsymbol{R} = [R_1, R_2, \ldots, R_n]^{\boldsymbol{T}}$ contains roles of all nodes.

Adversary Model

- **Goal of attackers**
  - To successfully detect the role of each node, i.e., $\boldsymbol{R}$, within a sufficiently long time period.
- **Capability of attackers**
  - Can overhear the data transmissions on each link.
  - Can estimate the transmission rate at each link.
  - Is aware of the network topology and knows the routing path between any source-destination pair.

Problem Statement

- **Role detection**
  - The goal of the *attacker* is to find an estimate $\hat{\boldsymbol{R}}$ which is close to the real role vector $\boldsymbol{R}$.
  - In the best case, $\|\hat{\boldsymbol{R}} - \boldsymbol{R}\|$ should be minimized.
- **Role concealment**
  - The goal of the defender is to make $\boldsymbol{R}$ difficult be estimated.
  - In the best case, the probability that $\hat{\boldsymbol{R}} = \boldsymbol{R}$ should be 0.5, i.e., a random 0/1 guess.

Role Detection

- **Network tomography**
  - A network with n nodes has at most $\frac{n(n-1)}{2}$ undirected flows.
  - Estimate the real flow vector $x \in \mathbb{R}^{\frac{n(n-1)}{2}\times 1}$, from the observed link rate vector $y \in \mathbb{R}^{L\times 1}$, where L is the p2p links in the network).
  - Linear relationship exist between x and y:

$$y = Ax,$$

where $a_{i,j}$ is 1 if i-th link is on the routing path of flow j.

Detection Approach

1. **Flow rate estimation**
   – Make estimation $\hat{x} = [\hat{x}_1, \hat{x}_2, \dots, \hat{x}_{\frac{n(n-1)}{2}}]^T$ to be close to the real value x.

2. **Role detection**
   – Estimate role of node i,

$$\widehat{\boldsymbol{R}} = 1_{\{\left(\sum_{f\in\mathcal{F}_i} 1_{\{\hat{x}_f\in\Sigma_1\}}\right)\geq\sigma_2\}},$$

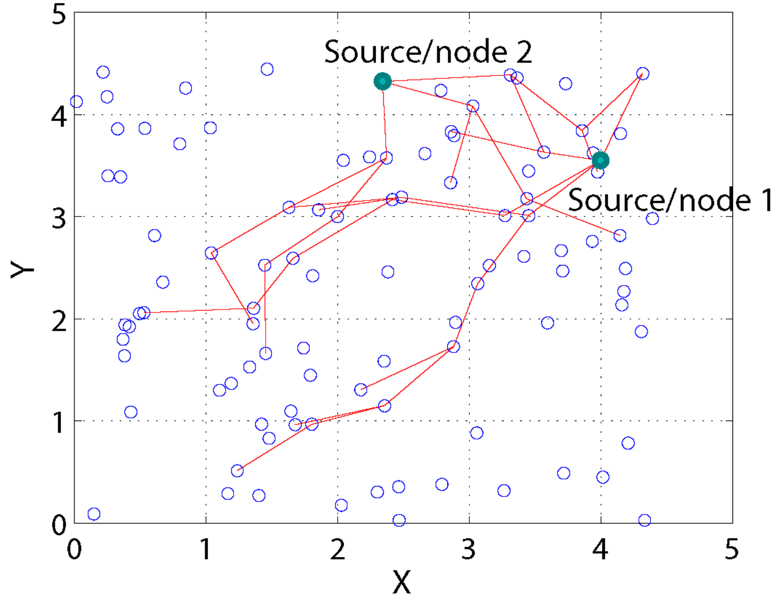
where Σ_1 is the rate threshold range, σ_2 is the threshold for role detection.

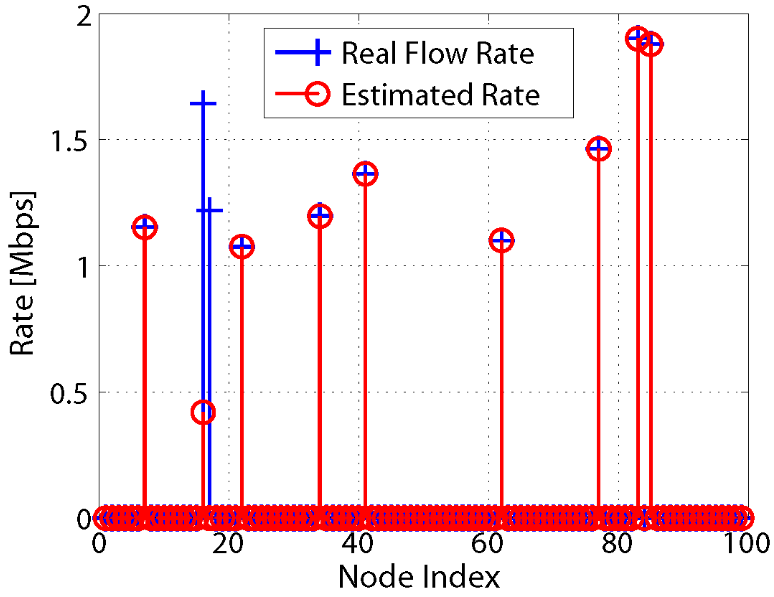
Evaluation

- **Simulation setup**
  - 100-nodes network with density 5;
  - Transmission range is normalized to 1;
  - 2 commanding nodes and 98 acting nodes;
  - Commanding nodes communicates to 10 other nodes.
  - 10 random acting to acting communication pairs.
  - Rate of each flow is random between 1M and 2M bps.

Evaluation

- **Result of flow rate estimation**





– Most of flow rates can be accurately estimated.

– Proper thresholds can help in role detection.

Evaluation

- **Result of role detection**

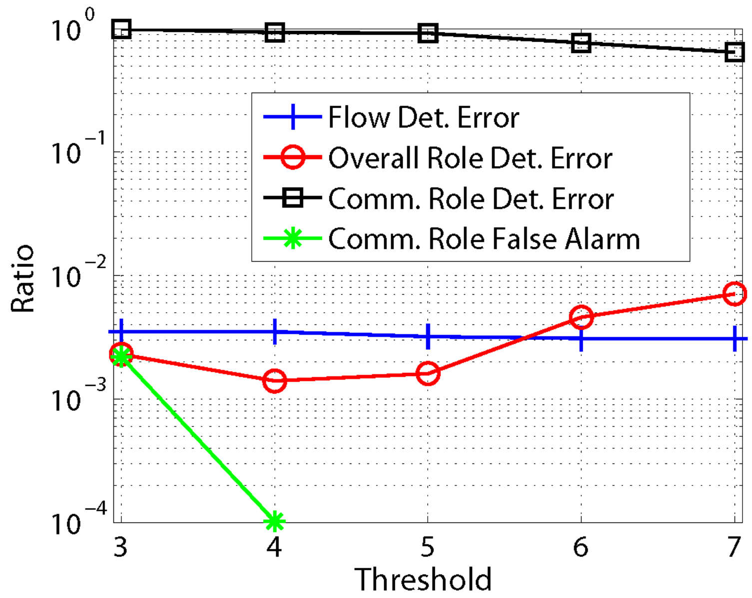
Flow Detection Error Rate:	1.4%
Commanding Role Detection Rate:	100%
Commanding Role False Alarm:	0%
Overall Role Detection Error Rate:	0%

  - $\Sigma_1 = [700Kbps, +\infty)$, and $\sigma_2 = 7$.
  - Metrics:
    - Flow detection error rate.
    - Commanding role detection rate.
    - Commanding role false alarm.
    - Overall role detection error rate.

MILCOM 2015 LEVERAGING TECHNOLOGY—THE JOINT IMPERATIVE
OCTOBER 26–28, 2015 • TAMPA, FL

Evaluation

- **Impact of threshold σ_2**

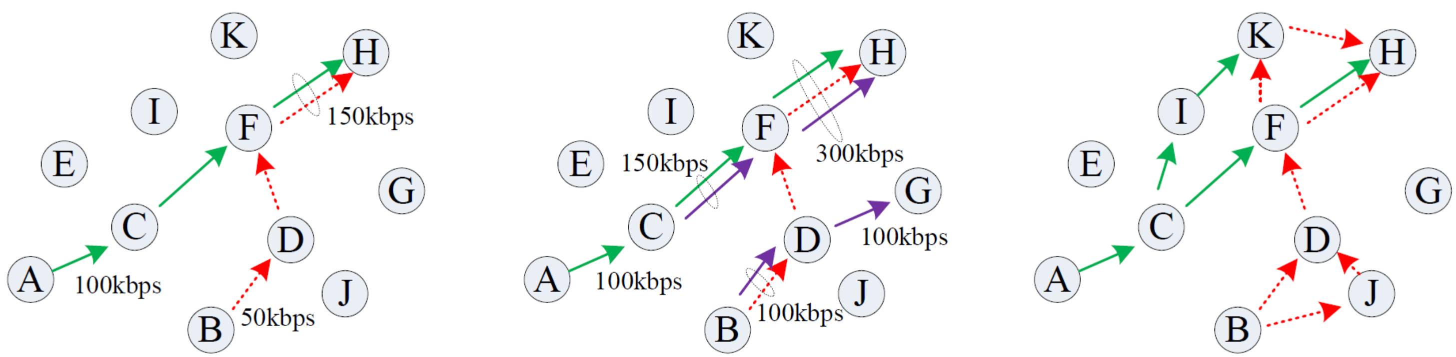


  - Keep $\Sigma_1 = [700Kbps, +\infty)$, and change σ_2 from 3 to 7.
  - $\sigma_2 = 5$ provides good performance (can be application specific as well).

1. Introduction
2. System Models
3. Role Detection
4. **Role Concealment**
5. Conclusion

Role Concealment

- **Flow detection and countermeasure**

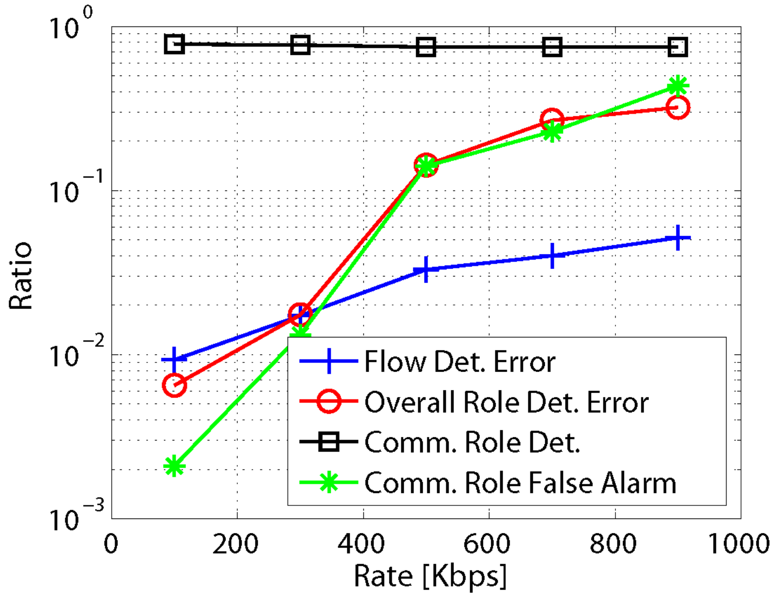


(a) (b) (c)

  - a: normal network operation.
  - b: deception traffic.
  - c: changing routing strategies.

Evaluation

- **Deception traffic**



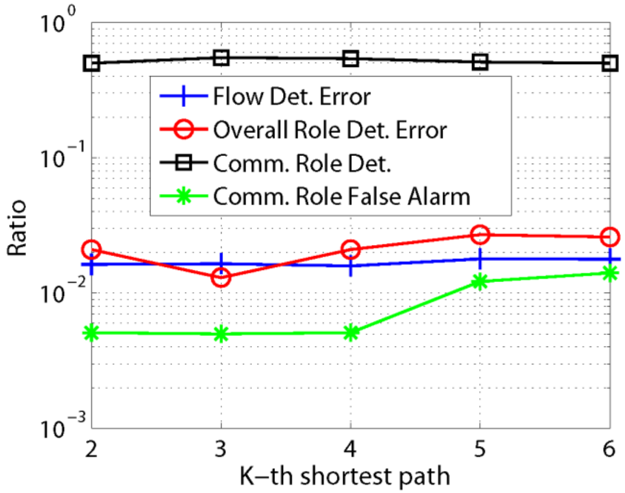
– Commanding role detection ratio ≈ 75%.

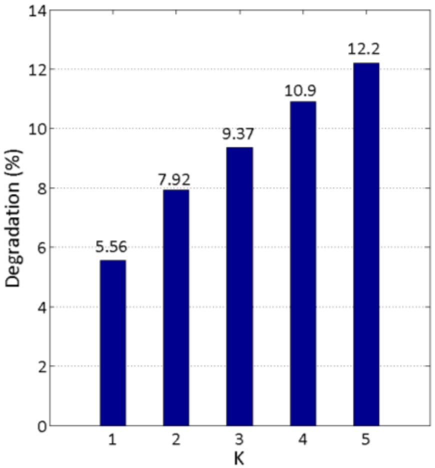
– Commanding role false alarm rise to 43.5%.

– Effective in conceal commanding roles.

Evaluation

- **Routing changing**





  - Use k-th shortest path, instead of the shortest path for routing.
  - Commanding role detection ratio ≈ 50%.
  - Delay degradation is notecible.

1. Introduction
2. System Models
3. Role Detection
4. Role Concealment
5. **Conclusion**

Conclusion

- **Role detection in tactical wireless networks**
  - It is possible to identify critical role of nodes accurately.

- **Role concealment in tactical wireless networks**
  - Deception traffic.
  - Routing changing.
  - Both can effectively conceal critical role of nodes with compromise in network performance.

Thank you!