Multi-Path-Based Avoidance Routing in Wireless Networks

Kazuya Sakai, Min-Te Sun, Wei-Shinn Ku, Jie Wu, and Ten H Lai

Tokyo Metropolitan University, National Central University, Auburn University, Temple University, The Ohio State University

ksakai@tmu.ac.jp

July 2nd, 2015

Outline

1. Introduction to avoidance routing
2. The Problem Formulation
3. Multi-Path Based Avoidance Routing (MPAR)
4. Performance Evaluation
5. Conclusions

1. Introduction

- We are interested in designing a secure routing protocol in ad hoc networks
- Cryptographic operations can protect end-to-end communications
- Two issues
  - Computing power are more and more accessible and inexpensive, i.e., encryption is no longer a perfect solution
  - Software implementations of cryptographic protocols may be seriously flawed (e.g., generating prime numbers)
- Avoidance routing
  - Avoiding insecure areas is the primary countermeasure against potential adversaries

Avoidance and Multi-Path

- What is "avoidance" in ad hoc routing?
  - Motivations for non-shortest path routing
  - Load balancing, energy-aware, congested links, etc.
- How to utilize "multi-path"?
  - Improving throughput by parallelizing message transmissions
  - Fault tolerance, e.g., backup paths
- Our definition
  - A routing path physically avoids insecure areas
  - e.g., malicious countries, compromised nodes, etc.
  - We utilize the idea of multi-path with the XOR coding in a very different way

Avoidance Routing

- The avoidance routing problem
  - Avoid insecure area that adversaries can eavesdrop on communications

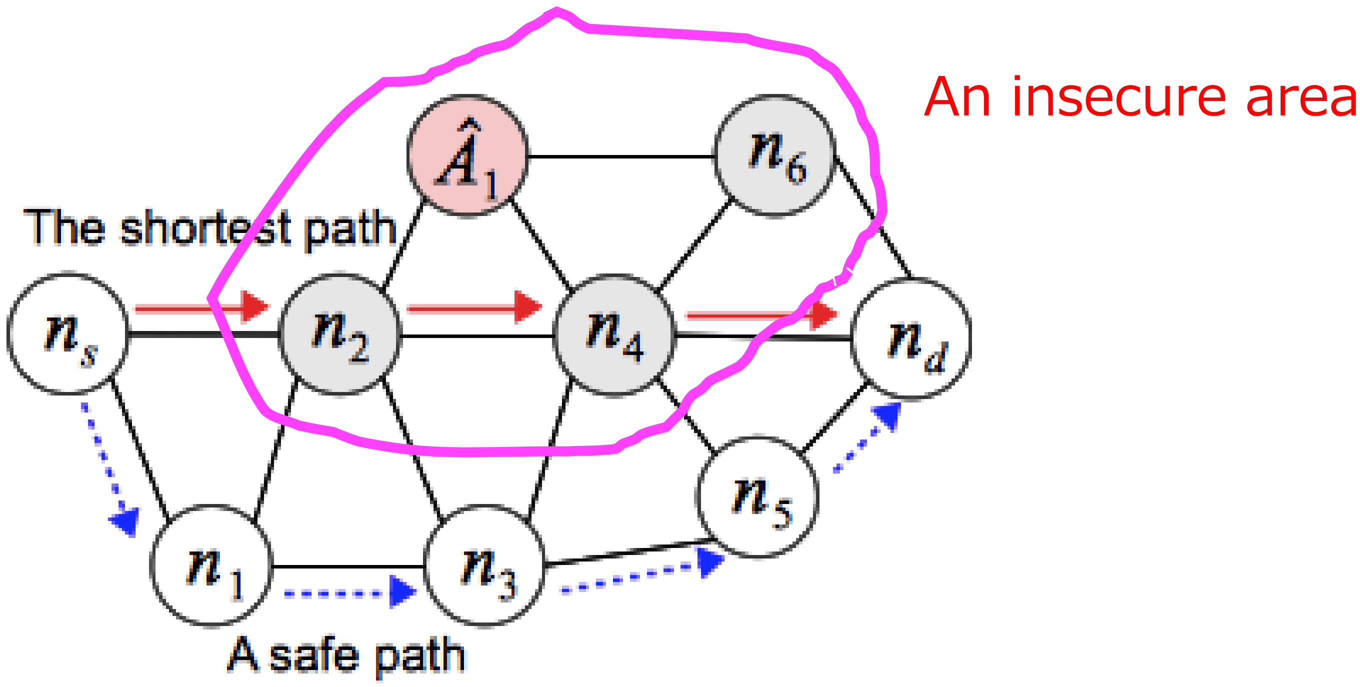


Fig. An insecure area in a graph

2. The Problem Formulation

1. Introduction to avoidance routing
2. The Problem Formulation
   - The Adversary Model
   - Our Assumptions
   - The Bounded Condition
   - The Safe Path Condition
3. Multi-Path Based Avoidance Routing (MPAR)
4. Performance Evaluation
5. Conclusions

The Adversary Model

- Adversaries are assumed to have unbounded computational power
  - A nation may spend a large amount of computing and human resources in a critical environment, e.g., a battlefield
  - Traffic analysis is also of concern
- Perfect secrecy and polynomial secrecy
  - An encryption scheme with perfect secrecy is secure against adversaries with unbounded computational power
    - e.g., the one-time pad, i.e., $c = m \oplus k$, where $|m| = |k|$ and the key can be used only once
  - An encryption scheme with polynomial secrecy is secure against adversaries with polynomial amount of compt. power

The Adversary Model

- Attack 1: eavesdropping
  - Polynomial secure encryptions are assumed not to be safe
- Attack 2: denying message forwarding
  - Intermediate nodes can compromise encrypted data and drop packets
- The protocol design goals
  - A routing path should never contain adversaries
  - A routing path should avoid insecure area

Our Assumptions

1. Known adversaries' location
   - Each node knows binary information (if malicious nodes are in its transmission range
2. Collusion attacks
   - The adversaries in a connected component can collude

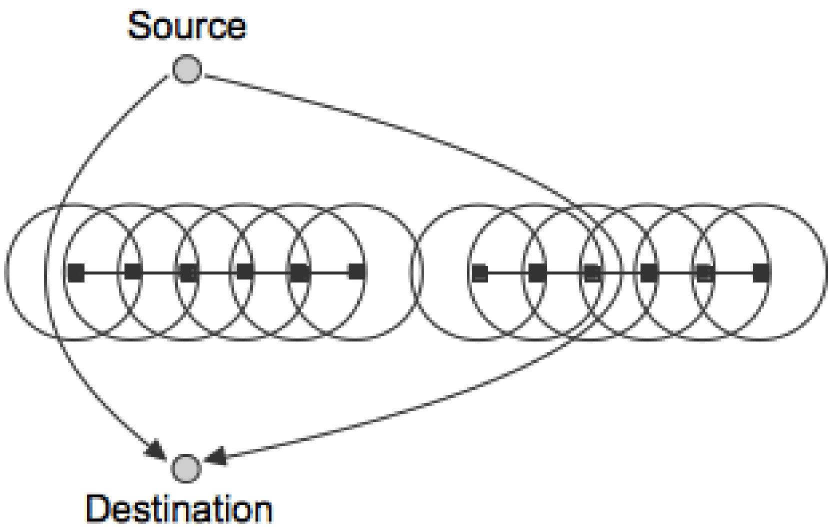


Fig. Connected components of adversaries

Table. Realistic scenario

	Unknown location	Known location
Independent	likely	unlikely
Collusions	unlikely	likely

The Performance Bound

- Condition 1: The bounded condition
  - A set of adversaries does not consist of a graph cut
  - This tells us the upper bound of performance
    - No routing protocol can securely deliver messages if there exists a graph cut by a set of adversaries

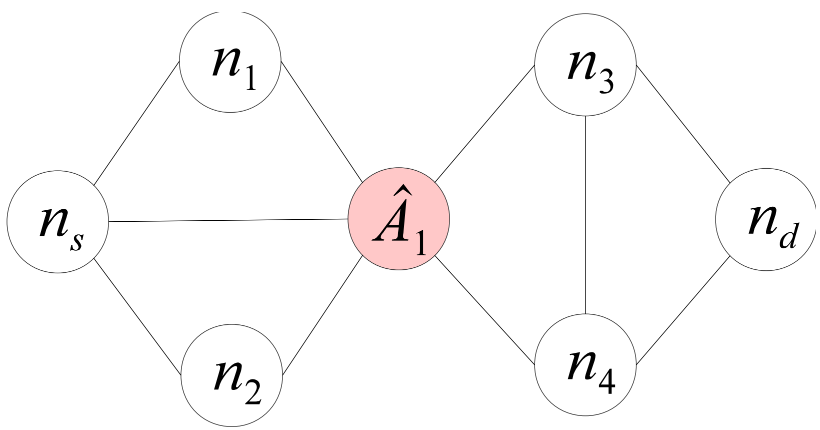


Fig. 1. A graph cut

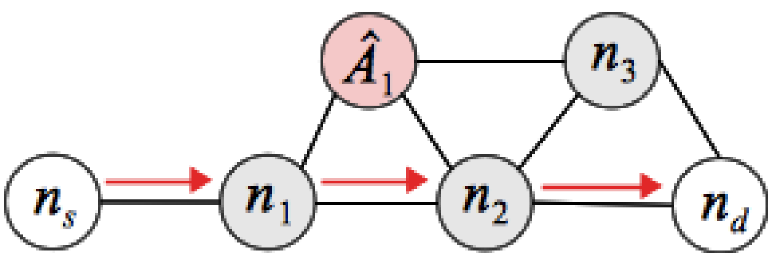


Fig. 2. A path w/o adversaries

An ideal protocol w/ a perfectly secure encryption protects messages from eavesdropping

The Existing Solutions

- The existing solutions
  - Avoidance routing for the internet
  - Distance vector-based or beacon vector-based routing
- Condition 2: The safe path condition
  - There exists a path s.t. no node on the path has any adversary in its neighbors

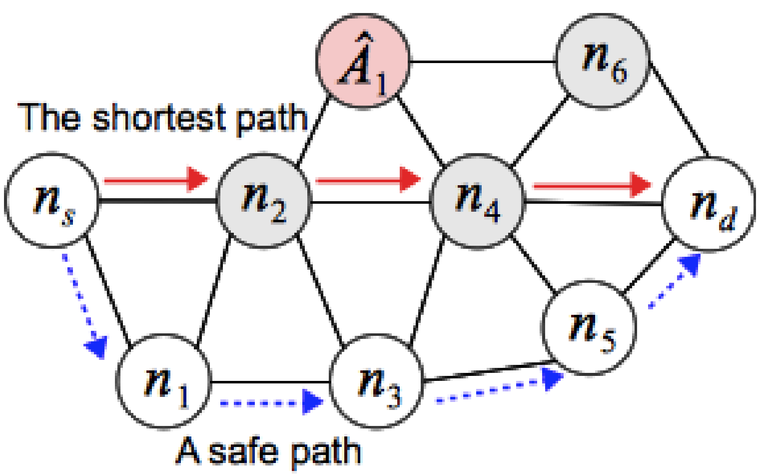


Fig. 1. A safe path

All the existing solutions are single-path-based, and thus the safe path condition dominates the upper bound

The Gap

- There is a big gap between the bounded condition and the safe path condition
  - Any single-path routing with a polynomial encryption scheme requires the safe path condition

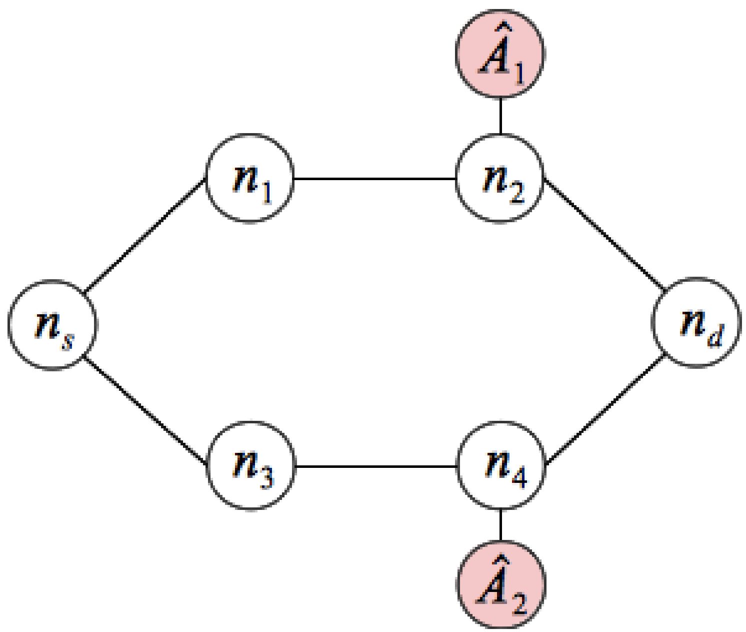


Fig. A graph with no safe path

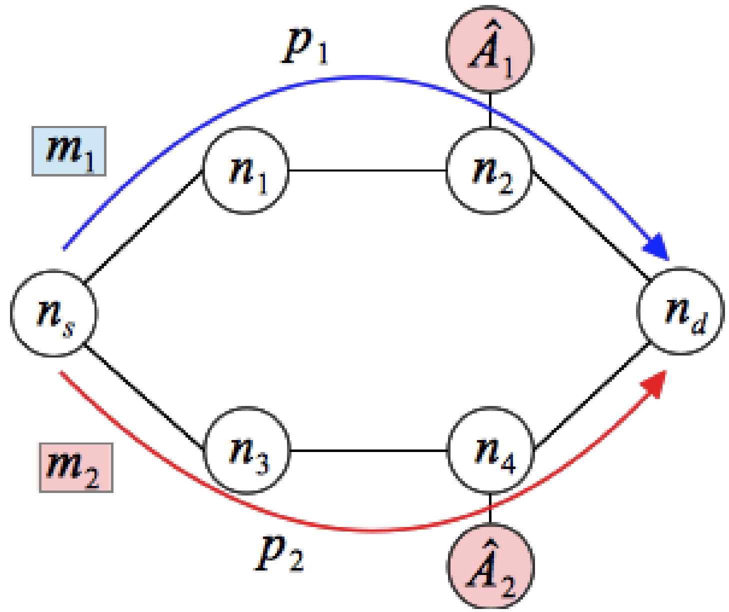
- There is no graph cut by a set of adversaries
- There is no safe path between n_s and n_d

3. Multi-Path Avoidance Routing (MPAR)

1. Introduction to avoidance routing
2. The Problem Formulation
3. Multi-Path Based Avoidance Routing (MPAR)
   - The Overview of MPAR and Definition
   - A Framework
   - The K-Path Discovery protocol
   - The Performance and Security Properties
4. Performance Evaluation
5. Conclusions

The Overview of MPAR

- We propose multi-path avoidance routing (MPAR)
  - An on-demand protocol
- The XOR coding
  - No common secret
  - Perfect secrecy by a one-time pad like scheme
- Multi-path
  - An adversary cannot recover a message unless she wiretaps all the paths



$$m := m_1 \oplus m_2$$
$$m_1 \leftarrow_{rand} Gen(|m|)$$
$$m_2 \leftarrow m \oplus m_1$$

Fig. The idea of MPAR

Adversary Disjoint Paths

- Definition: adversary disjoint paths
  - A set of paths that have no common adversary is said to be adversary disjoint paths

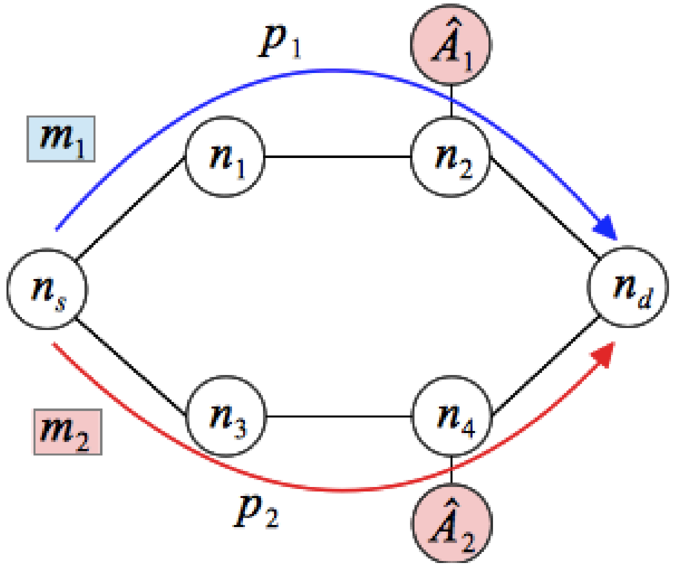


Fig. 1. Adversary disjoint paths

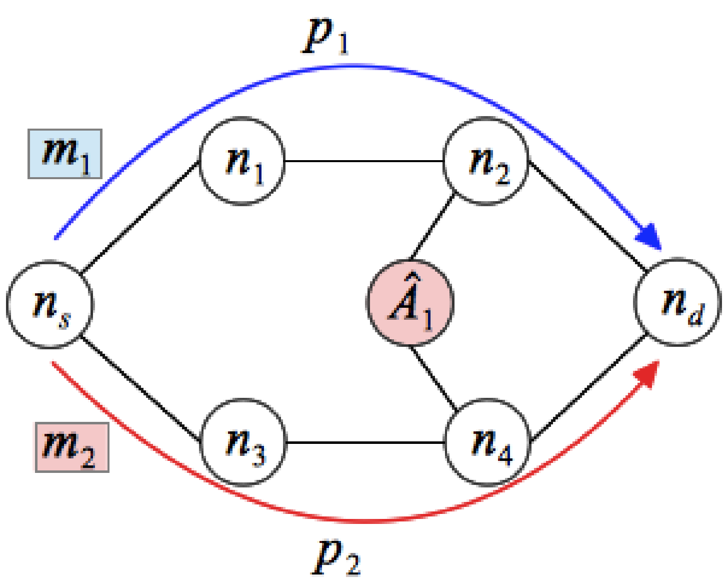


Fig. 2. Not adversary disjoint

Adversary disjoint paths with collusion attacks

- Adversary disjoint paths with collusion attacks

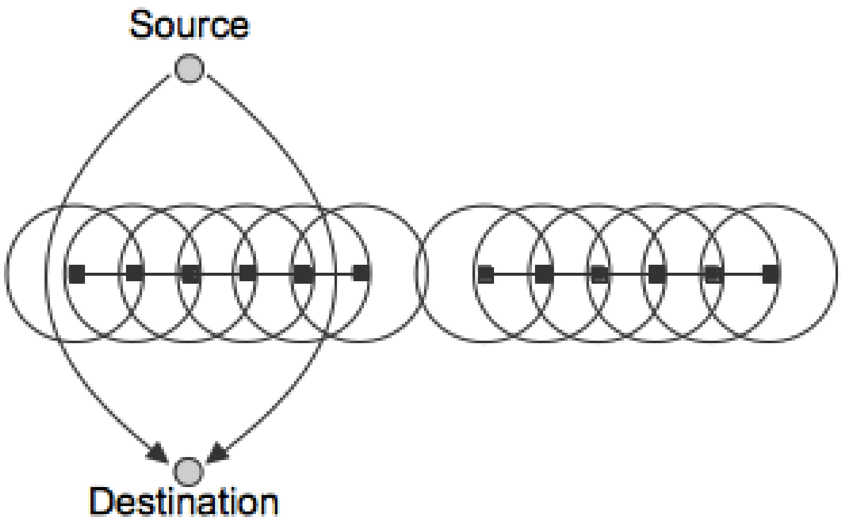


Fig. 1. Not adversary disjoint

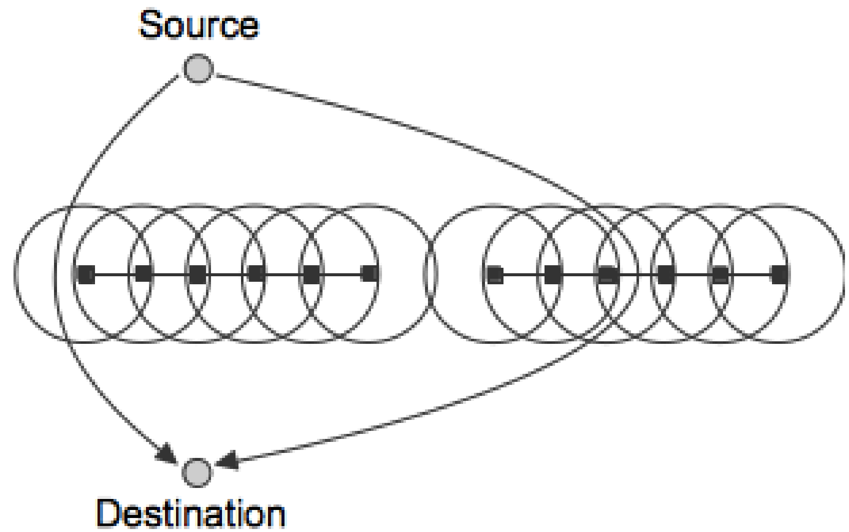
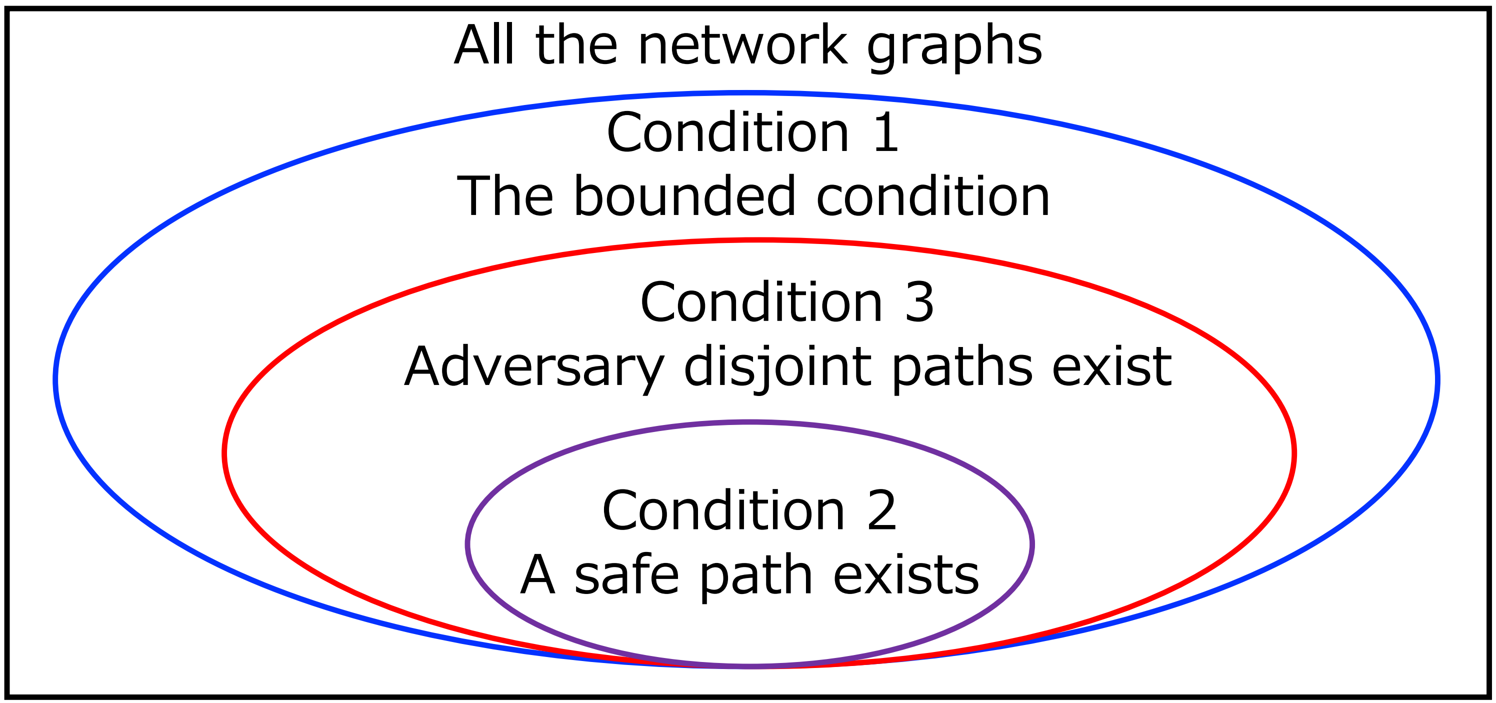


Fig. 2. Adversary disjoint

The Performance Bound of MPAR

- Condition 3 : the MPAR condition
  - There exists at least one set of adversary disjoint paths between the source and destination
  - MPAR requires condition 2 or 3



The MPAR Framework

MPAR (n_s, n_d, m, k_{max})

    Route_Discovery(n_s, n_d, k_{max})

    if a safe path p is found

        n_s sends m via p

Condition 2 is met
The single-path mode

    else if there is adversary disjoint paths $\mathrm{P} = \{p_1, p_2, \dots, p_k\}$

        computes m_i $(1 \leq i \leq k-1)$ by $Gen_u(|m|)$

        let $m_k = m \oplus m_1 \oplus m_2 \oplus \cdots \oplus m_{k-1}$

        n_s sends m_i via p_i

Condition 3 is met
The k-path mode

    else

        routing fails

Neither Condition 2 nor 3 are met

The Route Discovery

- The k-path route discovery : (n_s, n_d, k_{max})
  - It consists of the route request and reply phases
    - $RREQ_k$ and $RREP_k$, where k is path ID
  - A set of adversary's IDs are kept in RREQ and RREP
  - A path is set up in the reverse order

Table. An entry of routing table

The path ID
The source ID
The destination ID
The predecessor ID
The descendant ID

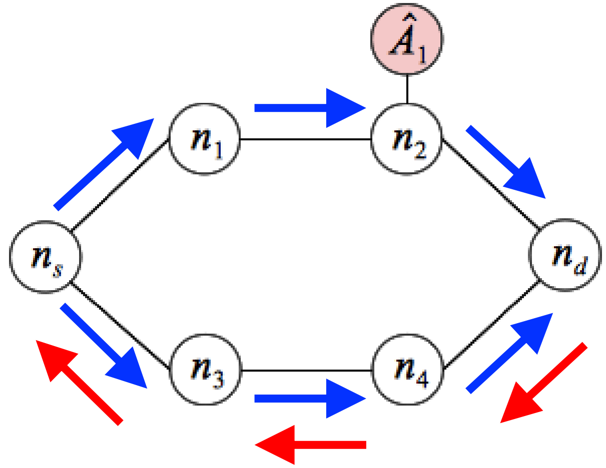


Fig. The route discovery

The Route Discovery (Cont.)

- Flooding is repeated until a safe path or a set of adversary disjoint paths are found, or the number of flooding exceeds k_{max}

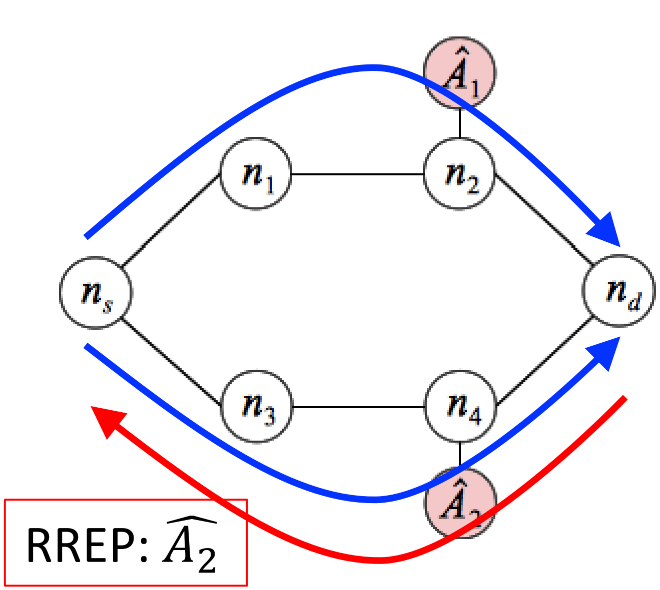


Fig 1. The first RREQ

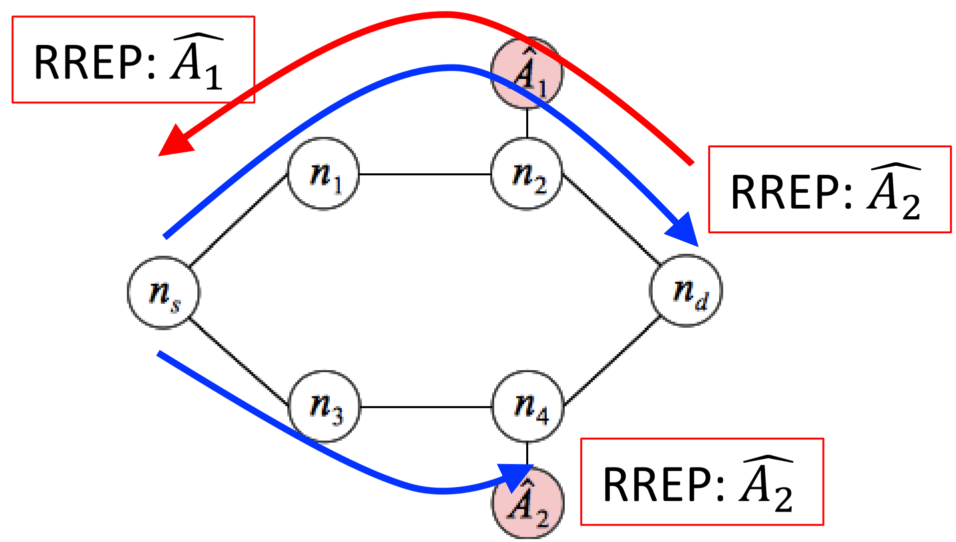


Fig 2. The second RREQ

Limitations

- MPAR does not work if an adversary is located in proximity of the source and destination
  - Probably only the ideal routing protocol with a perfectly secure encryption scheme can handle this case
  - Or cooperative jamming is required
- We have not optimized the k-path discovery yet
  - The optimal set is $\{p_1, p_3\}$
  - The worst case is $\{p_1, p_2, p_3\}$

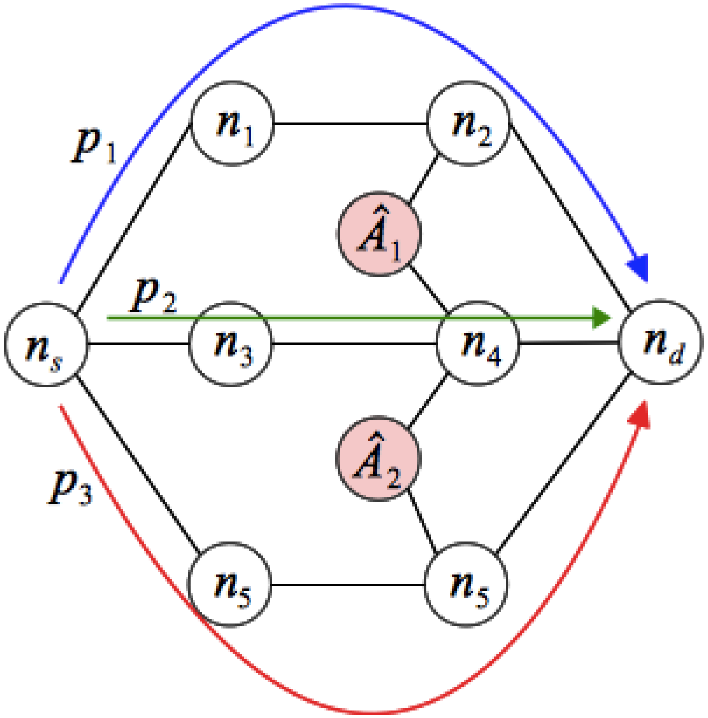


Fig. Three paths

The Key Properties

- The cost of the k-path discovery
  - MPAR introduces additional flooding cost only when a safe path is not found
- The cost of the message transmission cost
  - MPAR switches to the k-path routing mode, which requires k number of message transmissions, only when a safe path is not found

The Security Property

- The security property of MPAR
  - MPAR achieves the perfect secrecy unless a set of adversaries obtain all the XORed messages
- The proof is by Shannon's Theorem
  - The encryption scheme over the message space M is perfectly secure for which $|M| = |K| = |C|$ is perfectly secure if and only if
    - Every $k \in K$ is chosen with equal probability $1/|K|$ by a random generator
    - For every $m \in M$ and every $c \in C$, there exists $k \in K$ s.t. the encryption scheme outputs c

The Security Property (Cont.)

- The proof overview
  - Assume that $m \coloneqq m_1 \oplus m_2 \oplus \ \ldots \oplus m_k$ are sent out, and MPAR achieves the perfect secrecy as long as a set of adversaries do not have m_i for some i
  - $m^i \coloneqq m_1 \oplus m_2 \oplus \ \ldots \oplus m_{i-1} \oplus m_{i+1} \oplus \cdots \oplus m_k$ works as a cipher
  - The missing part m_i works as a key
  - $m_1, m_2, \ldots, m_{k-1}$ are randomly generated, and thus m_k is random
  - => $\Pr[key = \ m_i] = 1/|K|$
  - For every $m \in M$ and $m^i \in C$, there exits a unique m_i s.t. $m = m_i \oplus m^i$

4. Performance Evaluation

1. Introduction to avoidance routing
2. The Problem Formulation
3. Multi-Path Based Avoidance Routing (MPAR)
4. Performance Evaluation
   - Simulation Configurations
   - Simulation Results
5. Conclusions

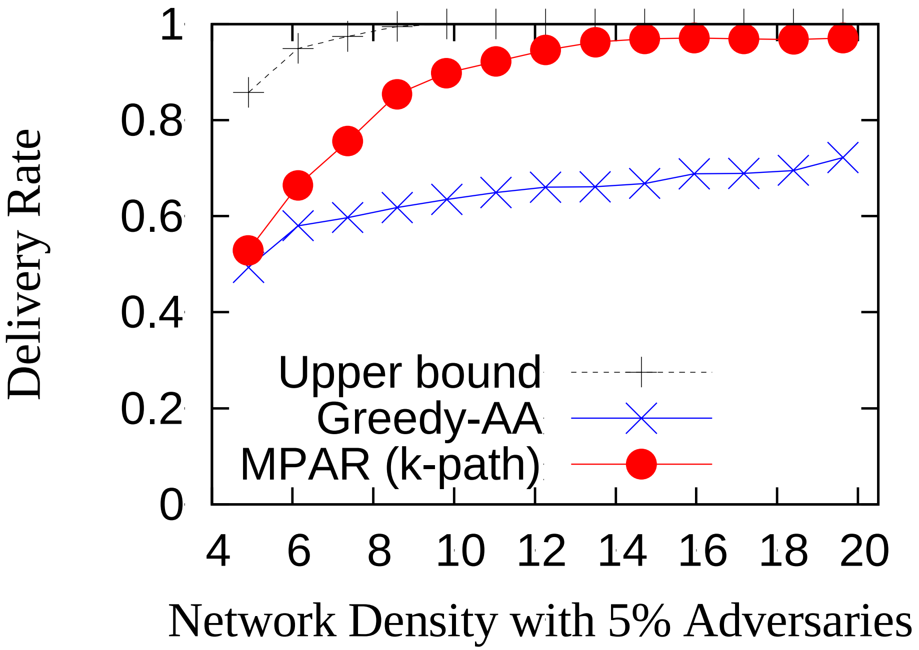
Simulation Configurations

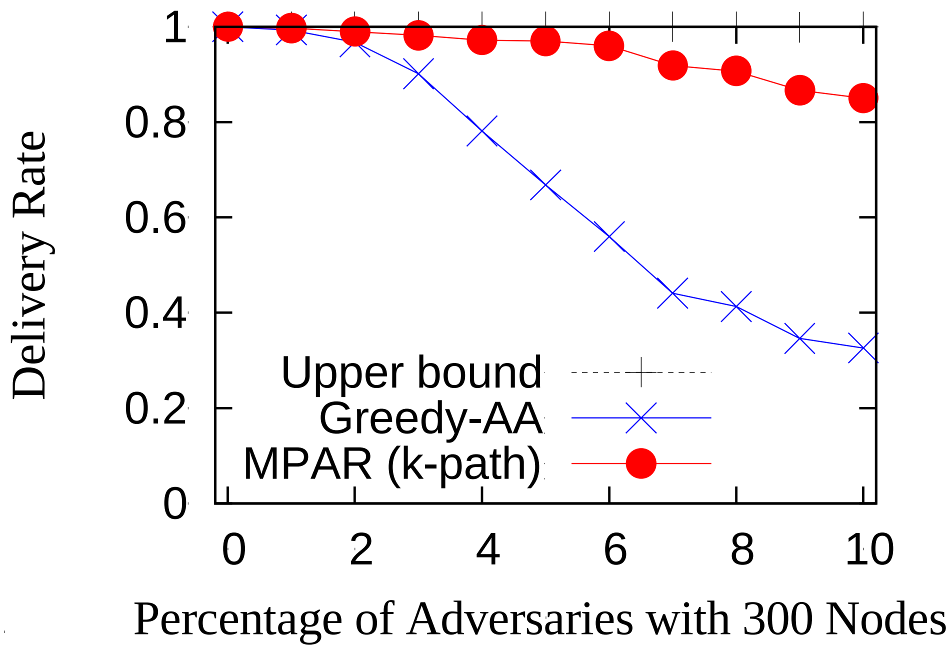
- We compared MPAR with two protocols
  - The ideal protocol w/ a perfectly secure encryption scheme (The upper bound of avoidance routing performance)
  - Greedy-AA (a distance vector-based protocol)

Table. Simulation parameters

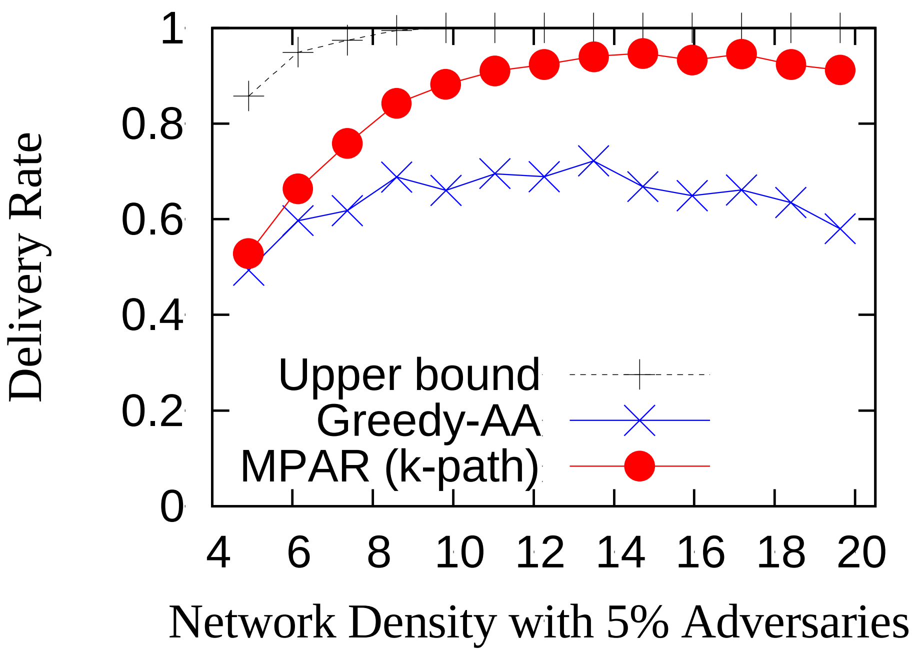
Parameters	Values
Simulation area	800 by 800
Communication range	100
Number of nodes	100 to 400 (4.9 ~ 19.6 neighbors / node)
Percentage of adversaries	0 to 10 % (Adversaries are randomly deployed)

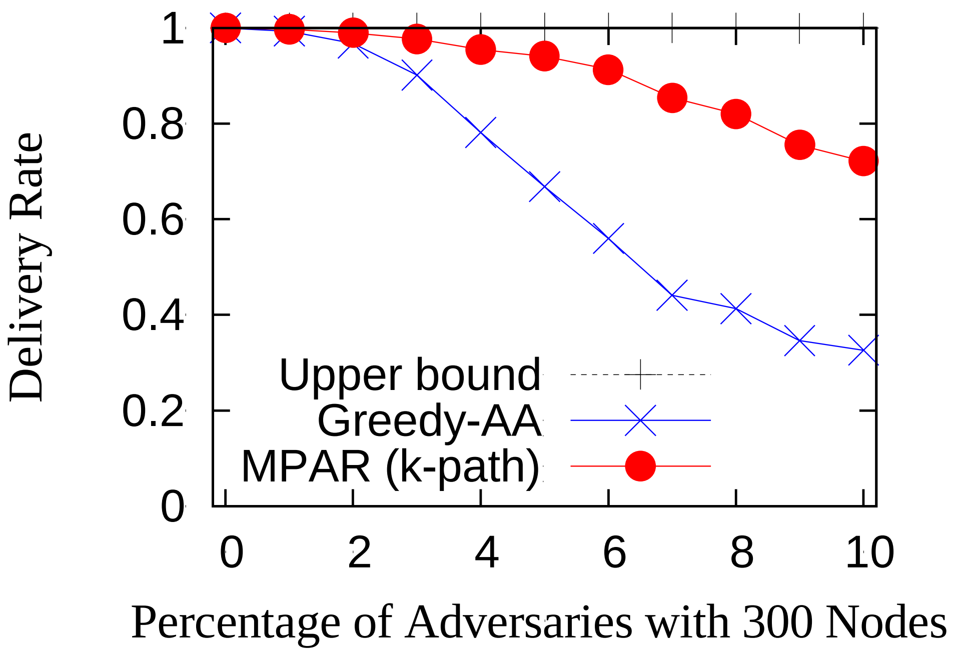
Independent Adversaries





Collusion Attacks





5. Conclusions

- In this work,
  - We study avoidance routing in ad hoc networks
  - We derive the bounded condition and the safe path condition
  - We propose multi-path avoidance routing (MPAR)
    - The XOR cording and k-path route discovery
    - The perfect secrecy
    - A weaker condition than that required by the existing protocols
  - We demonstrate the performance of the proposed scheme by simulations
- Future works
  - The optimization of a set of adversary disjoint paths and the cost of finding k-path