

## **Study of a Secure Probabilistic Routing Algorithm for Ad-Hoc Networks**

### **Purpose:**

The object of this project is a detailed analysis of an original algorithm for secure routing in ad-hoc networks addressing the problem of efficient route selection in strong adversarial environment. This approach was recently proposed as a generic framework for designing robust routing protocols appropriate for wired overlay networks or mobile ad hoc networks. Qualitative comparison with other MANET secure routing solutions is set as a goal, especially to emphasize the peculiarities of this new protocol. The study is intended to constitute itself a technical specification for a subsequent software implementation in ns-2 network simulator.

### **Abstract:**

The main reference of our study is the Technical Report - “Provably Secure Competitive Routing against Proactive Byzantine Adversaries via Reinforcement Learning” by Baruch Awerbuch et al [1]. Some other papers are consulted, especially [2], [3], [4], [5] and [6]. The authors’ idea is inspired by other uses of “Swarm intelligence” and “Distributed Reinforcement Learning” paradigms in developing routing algorithms for networks with no adversarial intervention. They consider their scheme is operating even under extremely strong adversarial model. A Byzantine adversary is defined as authenticated intermediate node acting alone or in collusion with other nodes in order to generate disruption or degradation of the routing service. The basic idea of the routing protocol is to combine a probabilistic source routing scheme with a feedback mechanism implemented by probing the behavior of intermediate nodes using authenticated acknowledgment of forwarded data packets. Probability distributions per outgoing edges, used by source node when computing the source route, are adjusted periodically, penalizing the bad behavior of intermediate adversary nodes. Therefore “good” nodes are randomly selected with higher probabilities than before to route data packets. No dedicated control packets are used although acknowledgment of each data packet is an obvious overhead. Each node maintains its own view of the network as a graph with routes toward all the other nodes. Source routes are extracted from the originator graph and the packet is sent along that route. Authentication of the good behaving nodes is provided by an “onion encryption” scheme. Key material may be provided by classical methods using a PKI and shared keys established on-demand or some other methods. However, key establishment is beyond the scope of the paper and of this study.

### **Tentative list of questions to be answered:**

Which are the data structures and other resources (like buffers, timers, etc) that must be maintained on each node for proper operation of the algorithm? What should be the initial values of probability distributions and how is specified initially and then maintained the network topology?

How much can we argue by an intuitive line of reasoning pro and against the efficiency of the proposed scheme? Can we identify weak links in the operation of the algorithm? Then what measures may be used to alleviate them?

How is onion encryption providing required authentication? How is this different from other related approaches like hash chains used in SEAD and Ariadne routing protocols? Is the proposed adversarial model framework a promising start in modeling and simulating possible attacks in ad hoc networks? What is ultimately the specific gain of this approach in providing security compared with the already existing solutions?

Which parameters are responsible for the convergence of the algorithm and how this may be affected by a dynamic topology in a mobile setting? What is the potential for further development of the scheme? What approach is needed to make a performance comparison feasible between this protocol and others claiming similar purpose and utilization?

## **Tentative Table of Contents**

1. Introduction
  - a. Vulnerability to attacks of ad hoc networks
  - b. Dynamic Byzantine adversary model
  - c. Big picture description of the protocol
  
2. Probabilistic versus deterministic routing protocols
  - a. Idea of probabilistic routing
  - b. Drawbacks of classical proactive and on-demand protocols in ad hoc networks
    - i. Link-state approach drawbacks in Byzantine setting
    - ii. Occasional flooding of Route Requests in classical on-demand routing
  - c. Online randomized algorithm approach, proof of optimality based on competitive analysis
    - i. Algorithmic challenges
    - ii. Definition and proof of optimality
  - d. Features of the routing protocol
    - i. On-demand operation
    - ii. Flooding-free routing
    - iii. Fear optimal packet loss for strong adversarial patterns
    - iv. Incurred control overhead

3. Security model, adversarial model and considered attacks
  - a. Security assumptions
  - b. Possible attacks considered
    - i. Classical attacks in ad hoc networks
    - ii. Byzantine behavior
  - c. Classification of adversary models
    - i. By malignancy of the attacks
    - ii. By collusion power of adversary
    - iii. By adaptivity/intelligence of the adversary
4. Basic concepts, mechanisms and algorithms used throughout the study
  - a. Path kernels in a directed graph
  - b. Weight pushing algorithm
  - c. Probabilistic source routing
  - d. Authentication and symmetric cryptographic primitives
  - e. Path authentication by Onion Encryption
5. Operation of the proposed algorithm
  - a. Network topology assumptions
  - b. Transforming an undirected graph into a layered directed graph
  - c. Feedback mechanism using secure acknowledgment
  - d. Calculation of the incoming edges probabilities
  - e. Derivation of the outgoing edges probabilities
  - f. Source route generation
  - g. Probing less used part of the network
6. Assessment of an intended protocol implementation in ns-2
  - a. Analysis of the simulation results published in the paper
  - b. Evaluation of the implementation of the adversarial model
  - c. Important parameters of the algorithm
  - d. Sketch of data structures, classes and methods needed for implementation using ns-2 class hierarchy
  - e. Analysis of integration of a possible adversary model framework with already existent protocol implementations
  - f. Envisioned exploration of performance of the protocol by simulation
    - i. Mobility and adversarial attacks effects on convergence and throughput and delay performance
    - ii. Comparison with other similar secure protocols (SEAD, Ariadne) in terms of performance under no attacks or under different adversary models
7. Conclusion
  - a. Achievement of the present study
  - b. Potential for further development of this routing protocol

### **Tentative time schedule:**

October 4

- getting more insights about the detailed operation of the protocol
- study of basic concepts, mechanisms and algorithms used

October 11

- final project specification
- study of the whole routing protocol

October 15

- complete study of the whole routing protocol
- first set of viewgraphs and progress report

October 29

- complete set of viewgraphs
- work on report draft
- second progress report

November 12

- review of the first draft of the project
- third progress report

December 3

- final project report draft and viewgraph presentation draft

### **Possible changes:**

Part 2.6 needs advanced knowledge of randomized algorithms and may be treated superficially or excluded. Part 6d.-f. is still in an advanced tentative status. Other points and particular aspects may reveal to necessitate more attention and will be considered accordingly. Some aspects presently thought as important might become collaterally treated.

### **References and Literature:**

[1] Baruch Awerbuch, David Holmer, and Herbert Rubens: Provably Secure Competitive Routing against Proactive Byzantine Adversaries via Reinforcement Learning Technical Report Version 1, May 2003

[2] Eiji Takimoto and Manfred K. Warmuth: Path kernels and multiplicative updates, In COLT Proceedings, 2002

- [3] Paul F. Syverson, David M. Goldschlag, Michael G. Reed: Anonymous connections and onion routing. In IEEE Symposium on Security and Privacy, 1997
- [4] Baruch Awerbuch, Yishay Mansour: Adapting to a Reliable Network Path, In PODC, 2003
- [5] Yih-Chun Hu, Adrian Perrig, David B. Johnson: Ariadne - A secure On-Demand Routing Protocol for Ad hoc Networks, MobiCom, 2002
- [6] Yih-Chun Hu, David B. Johnson, and Adrian Perrig: SEAD - Secure Efficient Distance Vector Routing for Mobile Wireless Ad Hoc Networks: WMCSA 2002
- [7] P. Papadimitratos and Z.J. Haas: Secure Routing for Mobile Ad Hoc Networks, Working Session on Security in Wireless Ad Hoc Networks, EPFL, 2002
- [8] Manel Guerrero Zapata, N. Asokan: Securing Ad-Hoc Routing Protocols, In Proceedings of the 2002 ACM Workshop on Wireless Security (Wise 2002)
- [9] Manel Guerrero Zapata: Secure Ad hoc On-Demand Distance Vector (SAODV) Routing INTERNET-DRAFT draft-guerrero-manet-saodv-00.txt, August 2002
- [10] Alfred J. Menezes, Paul C. van Oorschot, Scott A. Vanstone: Handbook of Applied Cryptography, CRC Press, 1997
- [11] William Stallings – Cryptography and Network Security, Principles and Practice, Second Edition, Prentice Hall, 2003
- [12] Rajeev Motwani, Prabhakar Raghavan: Randomized algorithms, Cambridge University Press, 1995