Secure Message Transmission (SMT) in Mobile Ad hoc Networks

Hafeth Hourani

hafeth.hourani@nokia.com

Spring 2004

Outline

- Overview
- Overview of SMT
- SMT in Detail
- SMT Evaluation
- Conclusions

This presentation is based on "*Secure Message Transmission in Mobile Ad hoc Networks*", by Panagiotis Papadimitraros, Zyhmunt H. Hass

Outline

- **Overview**
- Overview of SMT
- SMT in Detail
- SMT Evaluation
- Conclusions

MANET Security

- Security is significant challenge in Ad hoc networking
- MANET is an open collaborative environment
- Any node can maliciously or selfishly disturb and deny communication of other nodes
  - Every node in the network is required to assist the in the network establishment, maintenance and and work operation
- Traditional security mechanisms are inapplicable
  - No administrative boundaries for classification of a subnet or nodes as trusted
  - No monitoring of node's transactions with rest of the network (difficult to implement)

MANET Vulnerabilities

- The communication in MANET comprises to phases:
  - Route Discovery
  - Data Transmission
- Both phases are vulnerable to attacks
  - Adversaries can disrupt the route discovery phase
    - By obstructing the propagation of legitimate route control traffic
    - By adversely influencing the topological knowledge of benign nodes
      - Impersonating the destination, responding with corrupted routing information, by disseminating forged control traffic, etc.
  - Adversaries can disturb the data transmission phase
    - Incur significant data loss
      - By tampering with fraudulently redirecting, dropping data traffic, etc.

Safeguarding MANET

- To provide comprehensive security, both phases of MANET communication must be safeguarded
- Authenticating all control and data traffic will provide security to the MANET
  - Nodes must establish the necessary trust relationships with each and every peer they transiently associated with
  - Not feasible !
- Safeguarding Route Discovery
  - SRP
- Safeguarding Data Transmission
  - SMT

Outline

- Overview
- **Overview of SMT**
- SMT in Detail
- SMT Evaluation
- Conclusions

What is SMT

- Secure Message Transmission (SMT) is a protocol that allows tolerating rather than detecting and isolating malicious nodes
- SMT protocol is introduced to safeguard the data transmission against arbitrary malicious behavior of the network nodes
- SMT is a lightweight and operates solely in an end-to-end manner

Why SMT

- SMT safeguard pair-wise communication across unknown frequently changing network in the presence of adversaries
- The goal of SMT is promptly detect and tolerate compromised transmissions

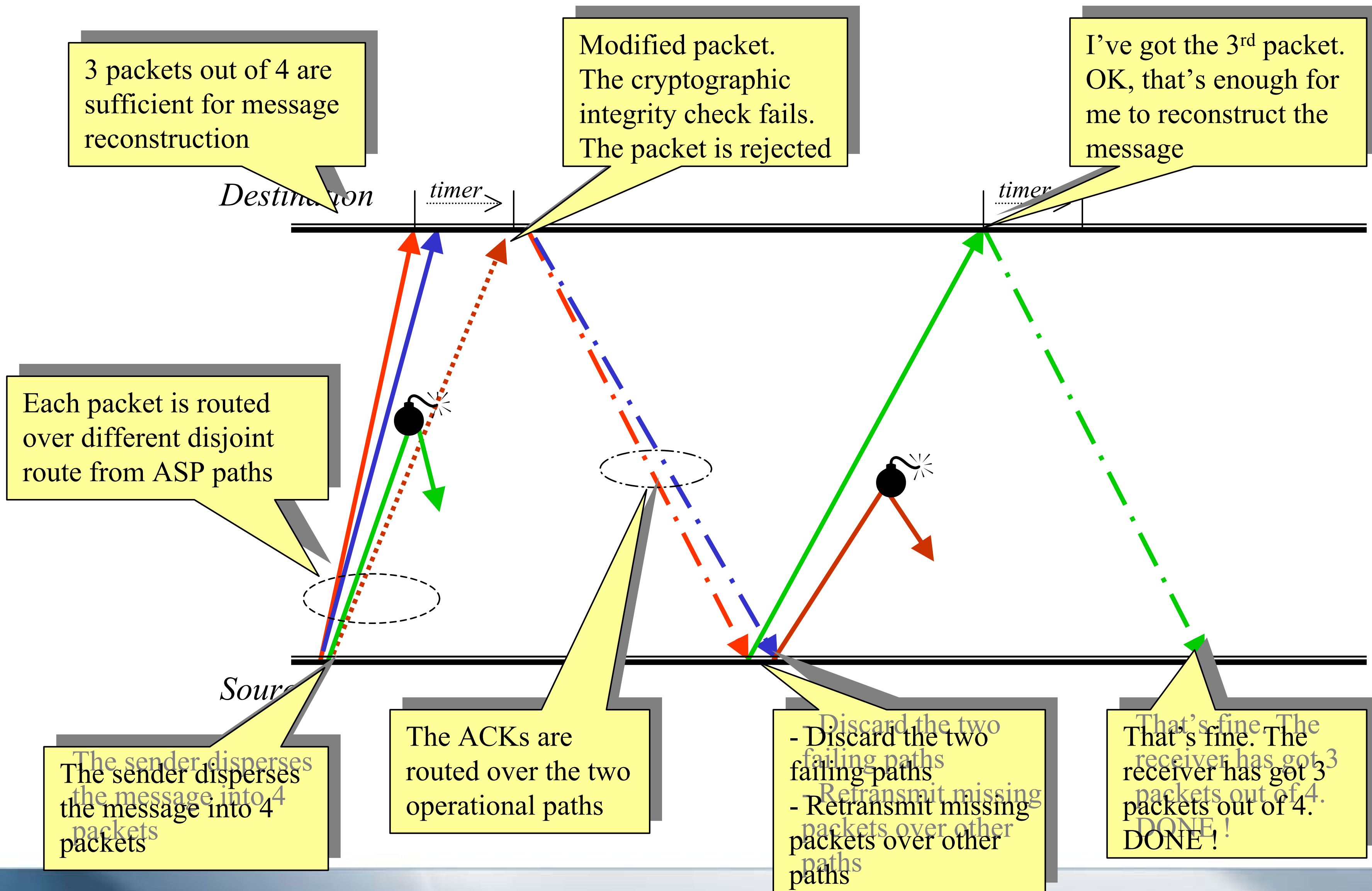
SMT Requirements

- SMT requires a security association (AS) only between the two end communicating nodes, i.e., the source and destination only
  - Both source and destination should establish a trust relationship (using public key for example)
- Active Path Set (APS)
  - A set of diverse disjoint paths between the two end nodes
  - These paths must be valid for some particular time
- This APS is a result of route discovery protocol
  - APS is maintained by the source

SMT Basic Approach

- SMT combines four elements
  - End-to-end secure and robust feedback mechanism
  - Dispersion of the transmitted data
  - Simultaneous usage of multiple paths
  - Adaptation to the network changing topology

SMT in Action



Outline

- Overview
- Overview of SMT
- **SMT in Detail**
- SMT Evaluation
- Conclusions

SMT Operations

- Determination of the APS
- Message dispersion and transmission
- ASP adaptation
- Protocol autoconfiguration

Determination of APS

- SMT can operate with any underlying secure routing protocol
  - SMT is independent of the route discovery protocol
    - It can work with both proactive and reactive protocols
- Every time the route discovery protocol is executed, the source constructs an APS of k node-disjoint paths
- The source should have a node connectivity view of the network

Message Dispersion and Transmission

- The message dispersion is based on Rabin's algorithm
  - It adds limited redundancy to the data
- The message and redundancy are divided into a number of pieces
  - A partial reception of can lead to a successful message reconstruction
- The dispersion allows the successful reconstruction of the original message if M out of N transmitted pieces are received successfully
- *Redundancy factor r = N / M*

APS Adaptation

- The source updates the rating of each path in its APS based on the feedback provided by the destination
- Each path is associated with two ratings:
  - Short-term rating r_s
    - Decreased by α each time a failed transmission is reported
    - Increased by β for each successful reception
    - If r_s drops below a threshold value r_s^{thr}, the path is discarded
  - Long-term rating r_l
    - Function of successfully received (and acknowledged) pieces over the total number of pieces transmitted across the route
    - If r_l drops below a threshold value r_l^{thr}, the path is discarded

Protocol Autoconfiguration

- The protocol adaptation to highly adverse environment can be viewed by
  - K: the number of utilized APS paths
  - k: the maximum number of disjoint paths from between the source and the destination
  - r: the redundancy factor of information dispersal
  - x: the number of malicious nodes
- The larger x is, the larger K should be for fixed r
  - The condition for successful reception: $x \leq \lceil K \times (1-r^{-1}) \rceil$

Outline

- Overview
- Overview of SMT
- SMT in Detail
- **SMT Evaluation**
- Conclusions

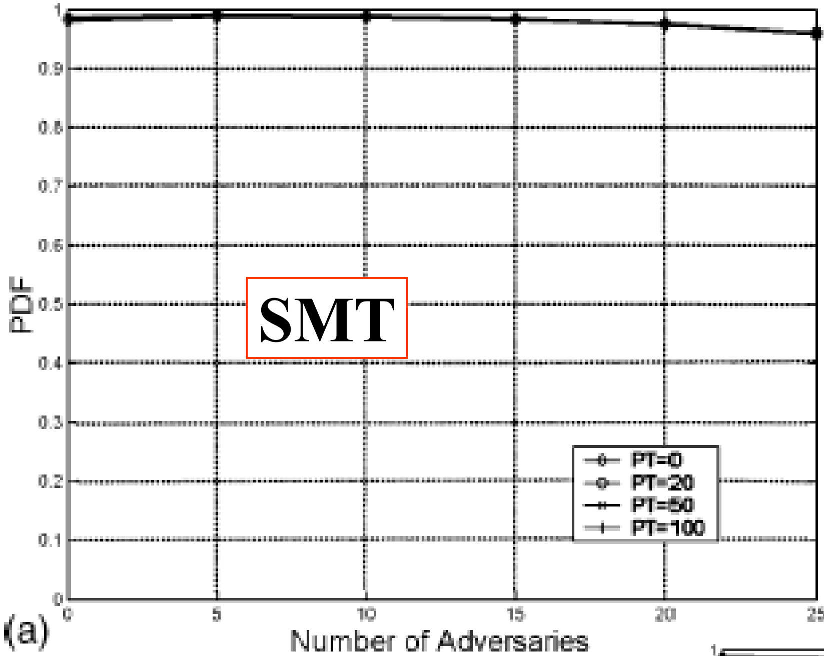
Simulation Setup

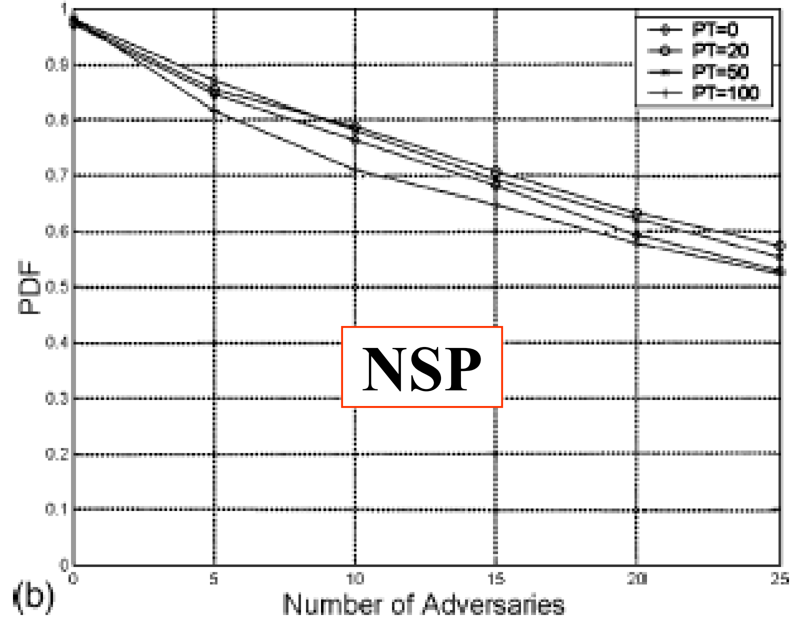
- Simulation parameters:
  - Network coverage area: 1000 m × 1000 m
  - Mobile nodes: 50
  - Node coverage area: 300 m
  - Simulation time: 300 sec
  - Network topology: for any two nodes, it is highly likely that two node-disjoint paths exist
  - Mobility model: random waypoint
    - Speed: 1 to 20 m/sec, Pause time (PT) = 0, 20, 50 and 100 sec
  - Number of adversaries nodes: 0, 5, 10, 25, 20 and 25
    - Attackers discard all data packets forwarded across routes they belong to
  - Simulation runs: 15 runs
- OPNET was used for the simulation

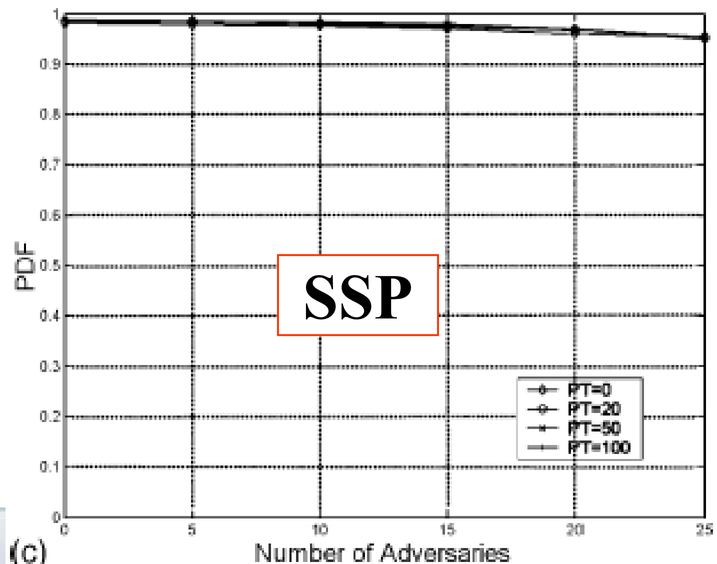
Evaluated Protocols

- For comparison purposes, three protocols were evaluated:
  - Non-secure single-path (NSP) data forwarding protocol
    - No data retransmission
  - Secure single path (SSP) transmission protocol
    - No message dispersion
  - SMT protocol
- The route discovery was assumed secure
- SMT protocol parameters
  - $r_s^{thr} = 0.0$, $r_s^{max} = 1.0$
  - $\alpha = 0.33$, $\beta = 0.033$
  - Transmission retry = 3 times

Results: Message Delivery



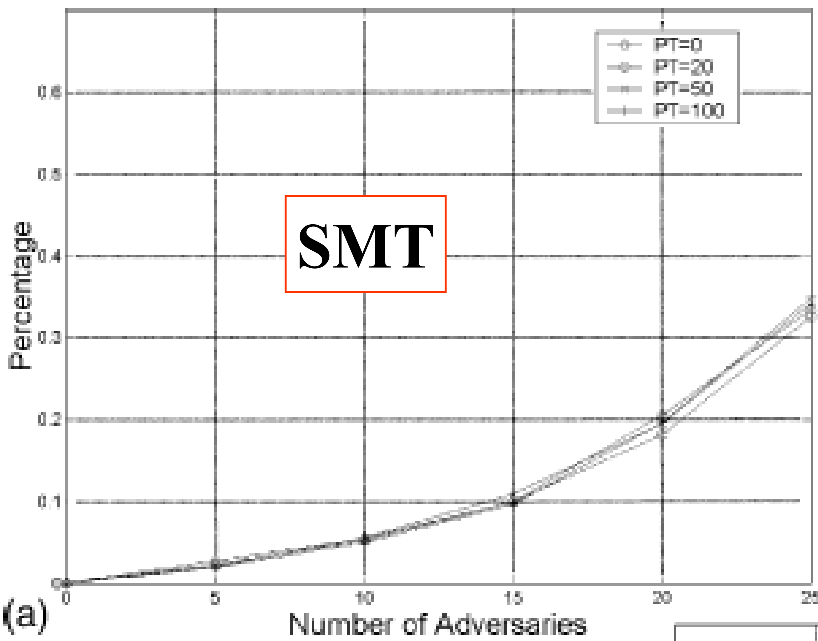


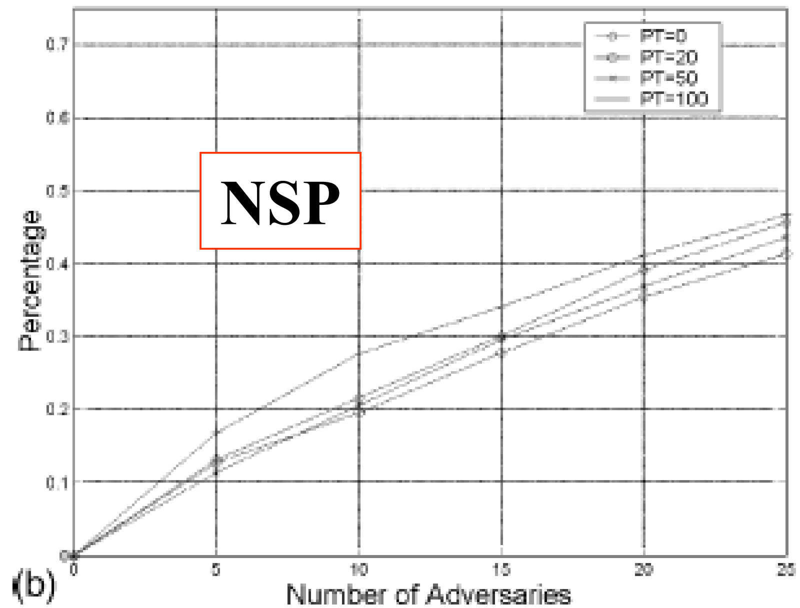


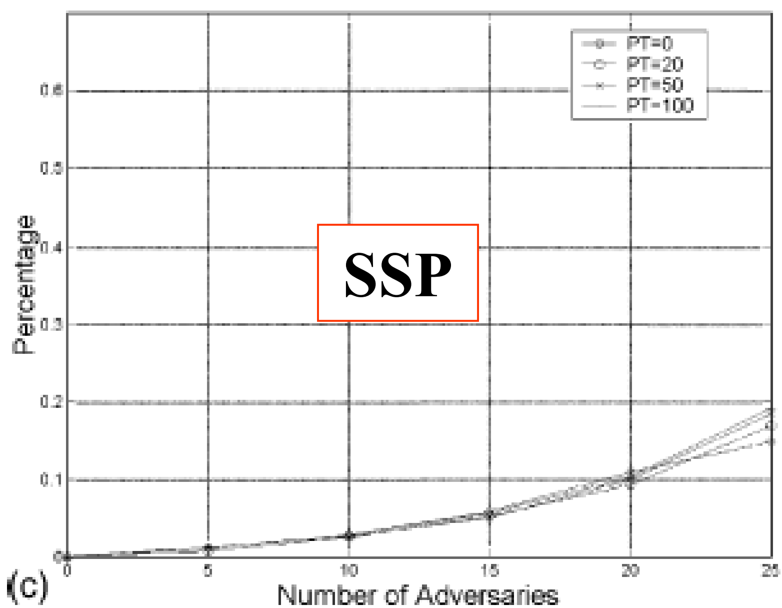
Comments

- SMT and SSP performance was almost the same
  - 99% message delivery within a range of 5 to 15 adversaries
  - More than 95% delivery when 50% of nodes are malice
- NSP experienced sharp degradation in message delivery
- The improvement of SMT over NSP ~ 14% to 83%

Results: Packets Dropped by Attackers







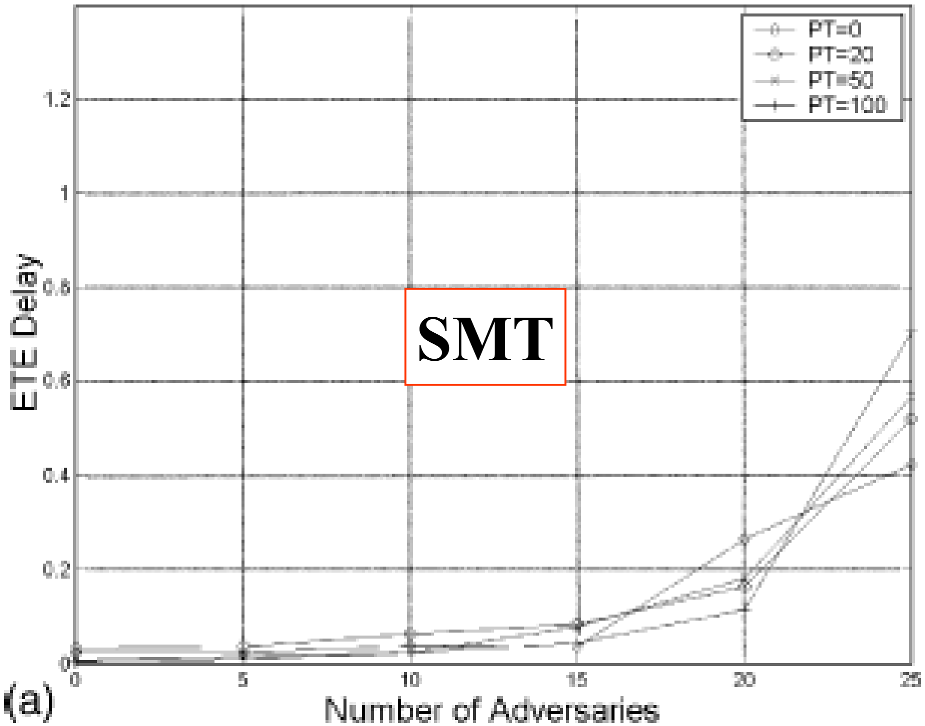
Comments

- NSP experienced substantial packet loss
  - Even for small number of adversaries
    - Packet lost ~ 17% when 10% of nodes are malice
- In case of SMT and SSP, the effect of adversaries is much less
  - SMT
    - ~ 10% of packets are dropped when 30% of nodes are malice
    - ~ 20% of packets are dropped when 40% of nodes are malice
  - SSP
    - ~ 6% of packets are dropped when 30% of nodes are malice
    - ~ 11% of packets are dropped when 40% of nodes are malice

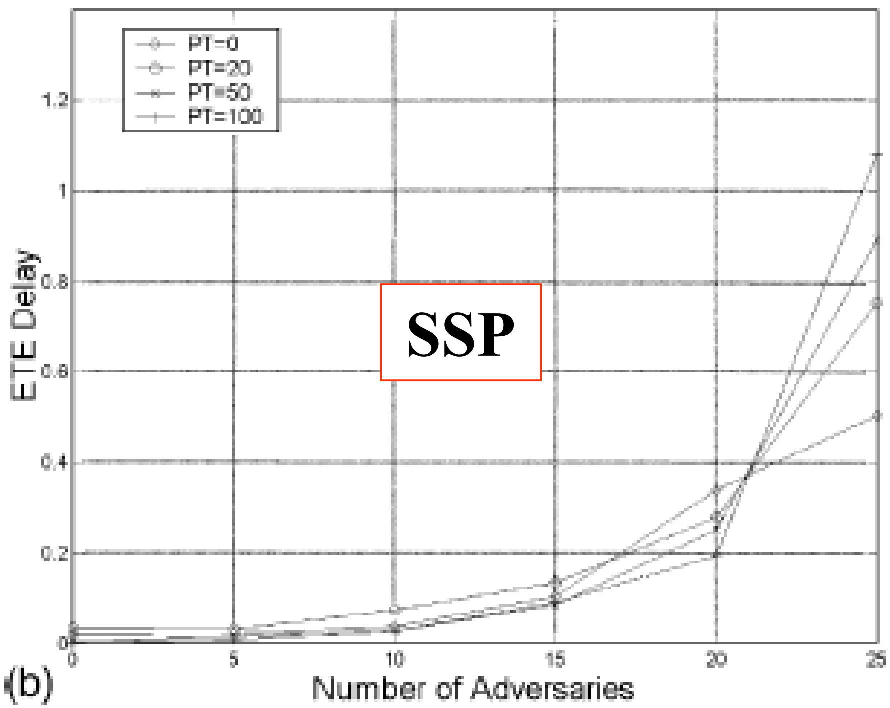
Comments: SMT vs. SSP

- SSP has shown better performance regarding the percentage of dropped packets by attackers
- Explanation
  - As the number of adversaries increase, SMT increases the dispersion factor and the number of utilized routes
    - Recall the relationship : $x \leq \lceil K \times (1-r^{-1}) \rceil$
  - The higher the number of paths, the more likely it is subjected to adversaries

Results: End-to-End Delay



(a)

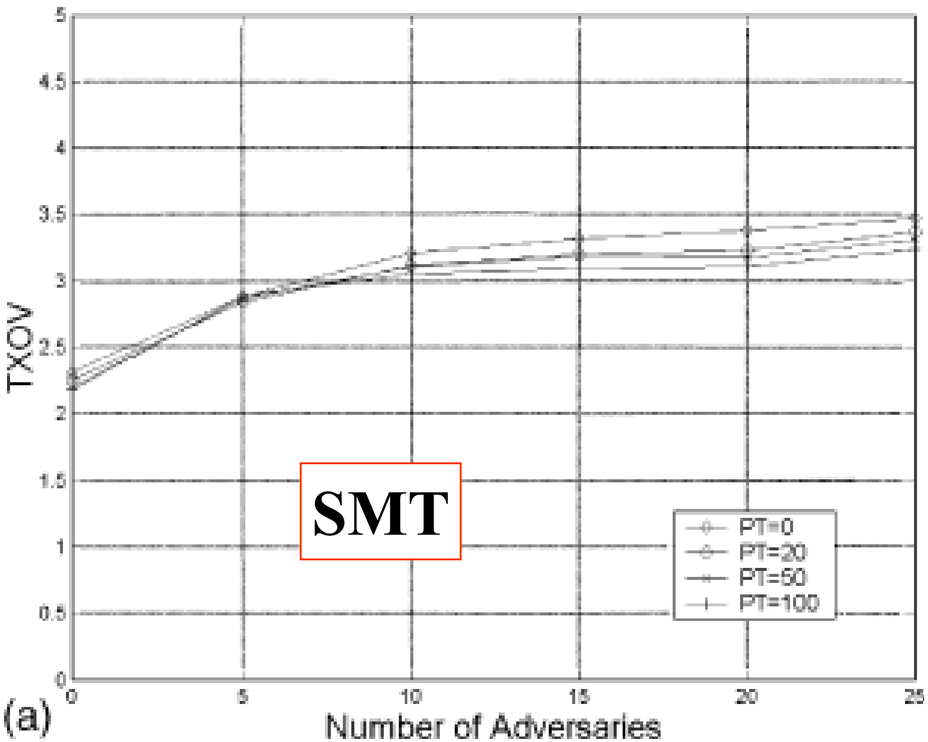


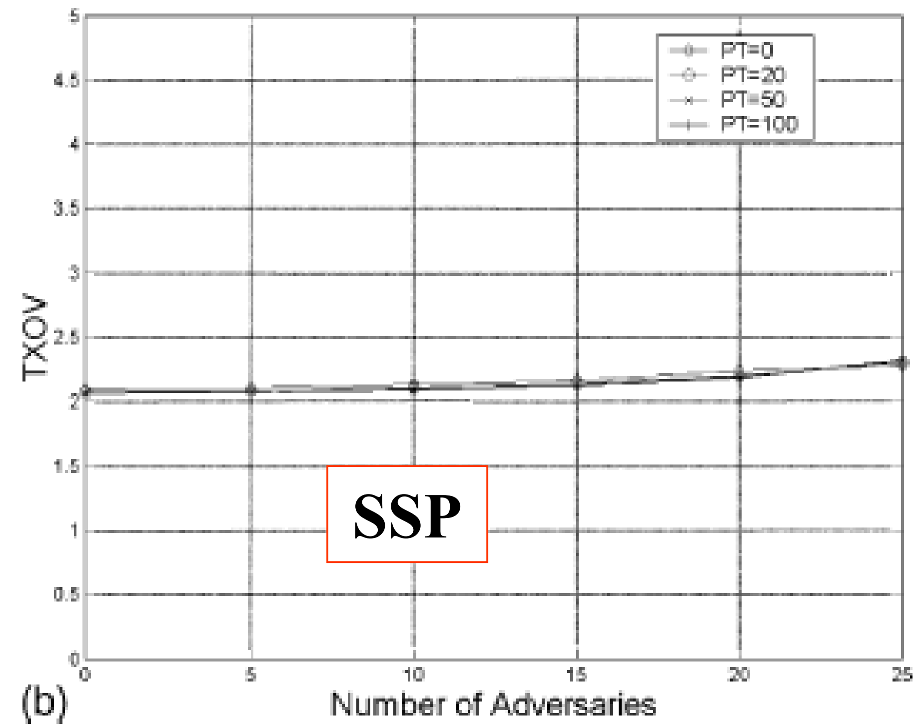
(b)

Comments

- SMT vs. SSP
  - SMT achieves less end-to-end delay
    - Due to the simultaneous usage of multiple routes by SMT
  - SMT provides lower variability of the end-to-end delay
- SMT is more capable of supporting real-time traffic

Results: Transmission Overhead





Comments

- SMT introduces more overhead compared with SSP
  - Additional SMT overhead: ~6% to ~52% higher than SSP

Outline

- Overview
- Overview of SMT
- SMT in Detail
- SMT Evaluation
- **Conclusions**

Conclusions

- SMT can counter any attack pattern either persistent or intermittent, by promptly detecting non-operational or compromised routes
- SMT takes a full advantage of MANET's route multiplicity
- SMT does not require any prior knowledge about the network trust model
  - Based on end-to-end security association
- SMT deliver 83% more data packets than NSP
- SMT can support QoS for real-time communications due to the low end-to-end delay

Critique

- In general, I don't see that SMT is something special !
- The performance evaluation does not show that SMT is superior to other security protocols such as SSP
- SMT assumes the availability of node-disjoint paths …
  - Racal $x \leq \lceil K \times (1-r^{-1}) \rceil$
    - If we have r = ¾ , and 10 different disjoint paths (K=10),
    - The $x \leq \lceil 10 \times (1-¾) \rceil = 3$
    - ➔ To tolerate 3 adversaries, you need to have 10 disjoint routes
- SMT introduces a significant overhead
  - Scarifies a lot of bandwidth for the sake some security

References

- Panagiotis Papadimitratos, Zygmunt J. Hass, "*Secure Message Transmission in Mobile Ad hoc networks*"

Q&A

Thank You!