An Approach for Establishing Trust in MANETs for Network Services

Amir Ghavam
PhD Candidate, U. Ottawa
aghavam@site.uottawa.ca

Supervisors
Michel Barbeau
Nicholas D. Georganas

MITACS – IT Theme Meeting
October 2003, Banff

Contents

- Security/Trust issues in MANETs
- Mobility helps Security
- Suggested Extensions
- Performance Evaluation
- Conclusion

Security Challenges in MANETs

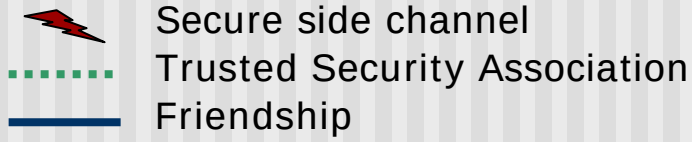
- Vulnerability of (wireless) Channels and Nodes
  - *Eavesdropping, Injecting fake messages*
  - *Lack of physical protection and strong access control*
- Lack of Dedicated Servers
  - *Naming Services, Certificate Authorities, Directories*
- Sophisticated Protocols, Hard to Secure
  - *Routing: Incorrect information or topology change?*
- Attacks on Routing and Data Traffic
  - *Attract or Avoid Traffic, Confusing others*
  - *Clogging Networks, Maliciously dropping packets, Manipulating user data*

Trust Issues in MANETs

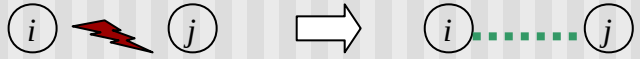
- In the context of this work
  Trusted Third Parties (Friends)
  Trusted (Authenticated) Security Associations
- Security Protocols require out-of-bound Key Exchange (Security Association) between the nodes
- Absence of online Trust Infrastructure such as Certificate Authorities Hierarchy
- PGP, Threshold Cryptography, Side Channel, Friends

Mobility helps Security [Capk]

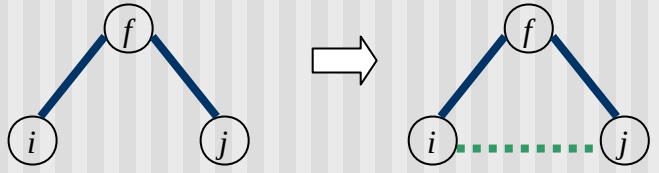
- Public Key Cryptography and verifiable Node Addresses



- *Secure Side Channel*
  - *Short range, point-to-point connection*
  - *Can be eavesdropped but not altered*

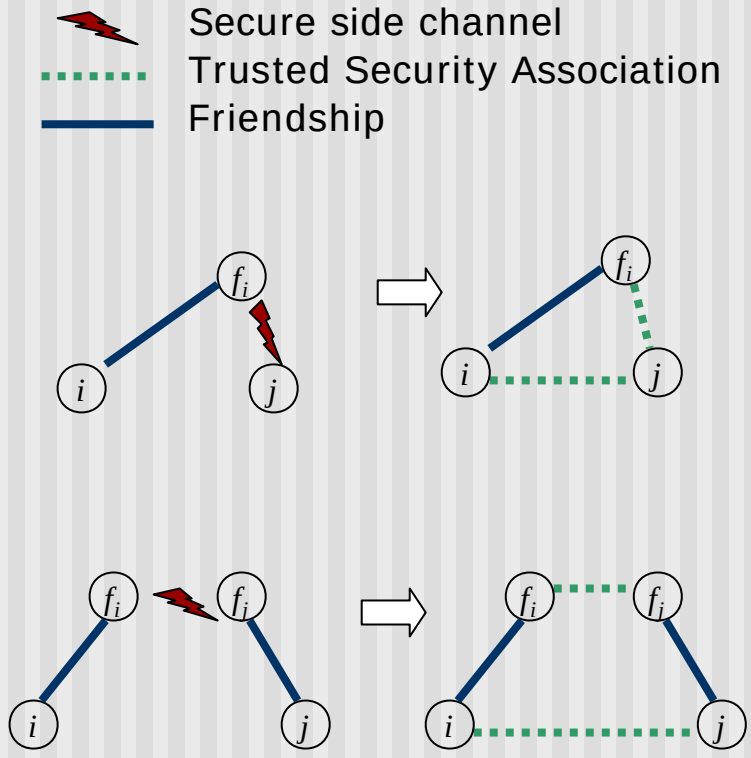


- *Friends*
  - *Trust each other to provide correct info.*
  - *Already established a security association*



Extending the Solution

- Beyond the range of side channel, and in absence of a common friend
- But Friend of one side can be in the vicinity of the other side
- Even Friend of one side can be in the vicinity of Friend of the other side



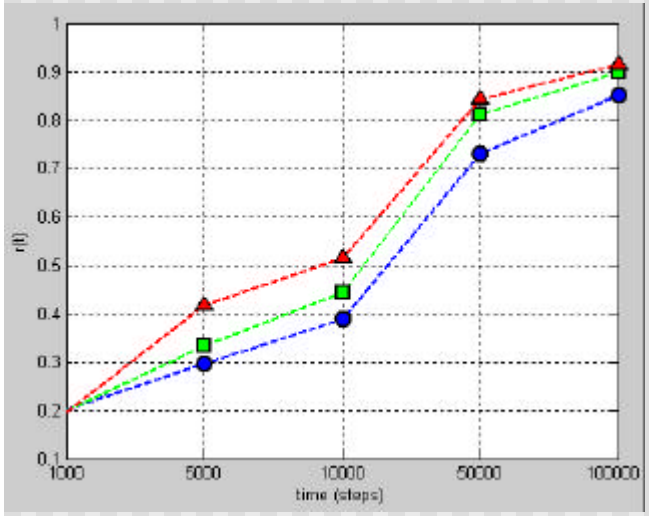
Performance Evaluation, Model

- $N=[n]$ nodes
- F friendship
- $E(t)=[e_{ij}(t)]$ SA at time t, $E(t_0)=F$
- $P=[p_{ij}]$ SA requests,
  - P_{ij} : user *i* wants to establish SA with user *j*

- *Convergence* $r(t)$*;* The fraction of required SA established at the time t

$$r(t) = \frac{\sum_{i,j}^{n} e_{ij}(t).p_{ij}}{\sum_{i,j}^{n} p_{ij}}$$

Performance Evaluation, Results



Random Waypoint Mobility Model, Simulated with MATLAB

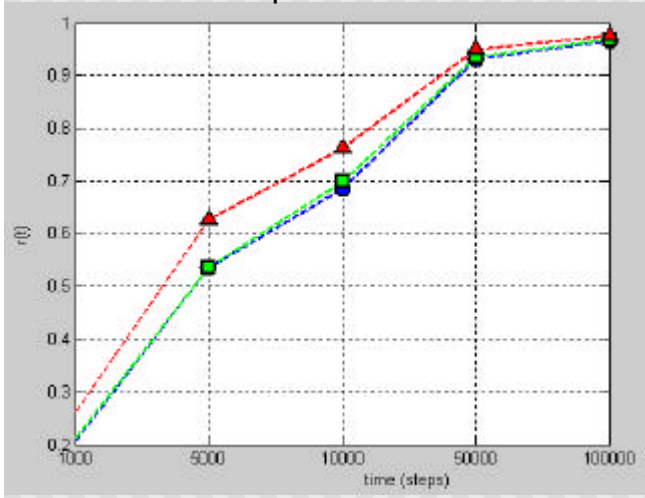
10 Nodes	Friends Distrib. 0.1	RF Range 20 units
100x100 Area	Request Distrib. 0.2	SC Range 1 unit
Speed 1 unit/step	Timeout 30	Sleep Ratio %25

--- Side Channel/Friends

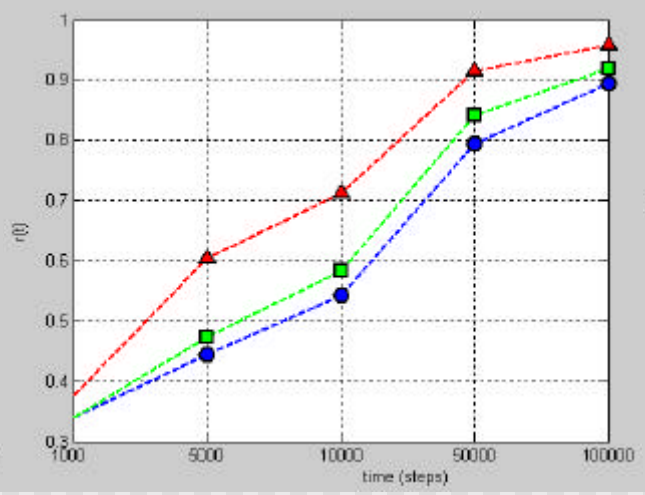
--- Friends/Neighbors

--- Friends/Friends

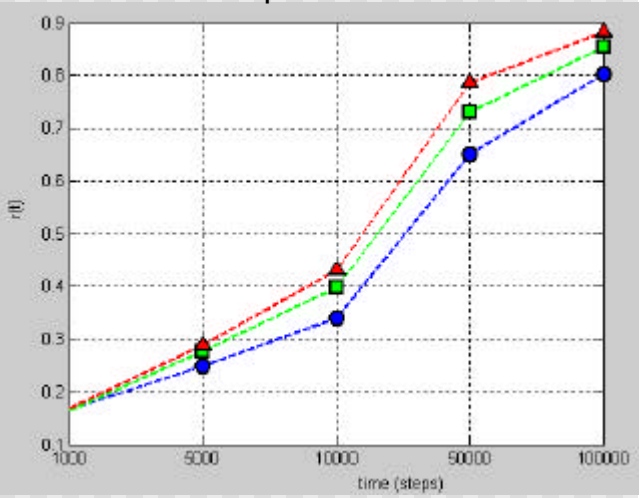
Speed x 4



Friends x 2



Requests x 4



Conclusion

- Two extensions by combining *SSC* and *Friends* mechanisms
- Resulted improvements verified by simulations
- Improvements more visible at lower speeds, higher densities of Friends, or higher request rates

References

[Lams] P. Lamsal, *Requirements for Modeling Trust in Ubiquitous Computing and Ad Hoc Networks*

[Esch] L. Eschenauer, *On Trust Establishment in Mobile Ad Hoc Networks*

[Haas] Z. J. Haas et al*, Wireless Ad Hoc Networks*

[Capk] S. Capkun et al*, Mobility Helps Security in Ad Hoc Networks*

[Zhou] L. Zhou and Z. J. Haas, *Securing Ad Hoc Networks*

[Just] M. Just, E. Kranakis, and T. Wan, *Resisting Malicious Packet Dropping in Wireless Ad Hoc Networks*

[Zhen] J. Zhen and S. Srinivas, *Preventing Replay Attacks for Secure Routing in Ad Hoc Networks*

[Staj] F. Stajano, *Security for Ubiquitous Computing*

[Mene] A. Menezes et al, *Handbook of Applied Cryptography*

References (Cont'd)

[Sufa] Sufatrio, Kwok Yan Lam, *Mobile IP Registration Protocol:A Security Attack and New Secure Minimal Public-Key Based Authentication*

[Bink] James Binkley, *Authenticated Ad Hoc Routing at the Link Layer for Mobile Systems*

[Reit] M. K. Reiter, *Authentication Metric Analysis and Design*

[Wan] T. Wan et al, *Reputation-based Mechanism for Validating Routing Information*

[Schn] B. Schneier, *Applied Cryptography, Protocols, Algorithms, and Source Code in C*

[Papa] P. Papadimitratos and Z.J. Haas, *Secure Message Transmission in Mobile Ad Hoc Networks*

[Pap2] P. Papadimitratos and Z.J. Haas, *Secure Routing for Mobile Ad Hoc Networks*

[Huba] J.-P. Hubaux et al, *The Quest for Security in Mobile Ad Hoc Networks*

References (Cont'd)

[Zimm]P. R. Zimmermann, *The Official PGP User's Guide*

[Herz] A. Herzberg et al, *Access Control Meets Public Key Infrastructure, Or: Assigning Roles to Strangers*

[Sta2] F. Stajano and R. Anderson, *The Resurrecting Duckling: Security Issues for Ad-hoc Wireless Networks*

[Yi] S. Yi et al, *Security-Aware Ad-Hoc Routing forWireless Networks*

[John] D. B. Johnson et al, DSR: *The Dynamic Source Routing Protocol for Multi-Hop Wireless Ad Hoc Networks*

[Perk] C. Perkins and P. Bhagwat, *Highly Dynamic Destination-Sequenced Distance-Vector Routing (DSDV) for Mobile Computers*

[Per2] C. E. Perkins and E. M. Royer, *Ad hoc On-Demand Distance Vector Routing*

[Desm] Y. Desmedt, *Threshold cryptography*