Enabling Secure Ad-hoc Group Collaboration over Bluetooth Scatternets

Somil Asthana (asthana@cse.buffalo.edu)
Dimitris Kalfonos (dimitris.kalofonos@nokia.com)

Outline

- Introduction
- Related Work
- Motivating User Scenario
- Design Goals
- Secure Scatternet Topology Formation Protocol
- Secure Scatternet Topology Update Protocol
- Experimental Setup
- Performance Results
- Conclusions and Future Work

Introduction

- An application-driven framework to enable secure ad-hoc group collaboration using Bluetooth scatternet.
- Our scatternet protocol is designed for scenarios like secure group meeting, where individuals can participate with their private piconets.
- During scatternet formation existing sessions and security associations are maintained.
- Our scatternet protocol creates loop free compact tree topology.
- We describe a prototype implementation and provide some initial experimental and simulation results.

Related Work

- BTH Network Formation Protocol can be divided into following categories:
  - Resulting Topology:
    - Mesh

      C. Petrioli and S. Basagni. “*Degree-constraint multihop scatternet formation for Bluetooth networks*”. In IEEE Globecom,2002.
    - Tree

      G. Tan, A. Miu, J. Guttag, and H. Balakrishnan. “*An efficient scatternet formation algorithm for dynamic environments*”. In IASTED Comm. and Comp. Networks (CCN'02), 2002.
    - Variant of mesh

      C. C. Foo and K. C. Chua. “*Bluerings - bluetooth scatternets with ring structures*”. In IASTED International Conference on Wireless and Optical Communication (WOC'02), 2002.
  - Adaptation Capabilities:
    - Static

      T. Salonidis, P. Bhagwat, L. Tassiulas, and R. LaMaira. “*Distributed topology construction of bluetooth personal area networks*”. In IEEE INFOCOM, 2001.

Related Work contd…

  - Dynamic

    F. Cuomo, G. Di Bacco, and T. Melodia. "*SHAPER: a self-healing algorithm producing multi-hop Bluetooth scatternets*". In IEEE Globecom, 2003.

- Centralized / Decentralized approach:
  - Centralized

    T. Salonidis, P. Bhagwat, L. Tassiulas, and R. LaMaira. "*Distributed topology construction of bluetooth personal area networks*". In IEEE INFOCOM, 2001.

  - Decentralized

    G. Zaruba, S. Basagni, and I. Chlamtac. "*Bluetrees - scatternet formation to enable Bluetooth-based ad hoc networks*". In IEEE Int. Conf. on Comm. (ICC'01), 2001.

- None of the above protocols consider the impact of security except
  - Karl E. Persson and D. Manivannan. "*Secure connections in Bluetooth scatternets*". In Proceedings of 36th Hawaii International conference on System science, 2003.

Motivating User Scenario

- User Scenario:
  - John decides to organize a secure meeting with his teammates.
  - Everyone except Mary bring their BTH-enabled devices in the meeting.
  - Frank comes with his laptop paired with his mobile phone.
  - John initiates the meeting, passes the meeting name and the password.
  - During scatternet formation Frank continues synchronizing his phone.
  - All of them connect and start exchanging presentations and files.
  - Eventually, Mary turns up and requests Frank to let her in the meeting.
  - Frank passes the meeting name and the password and opens the door for her.

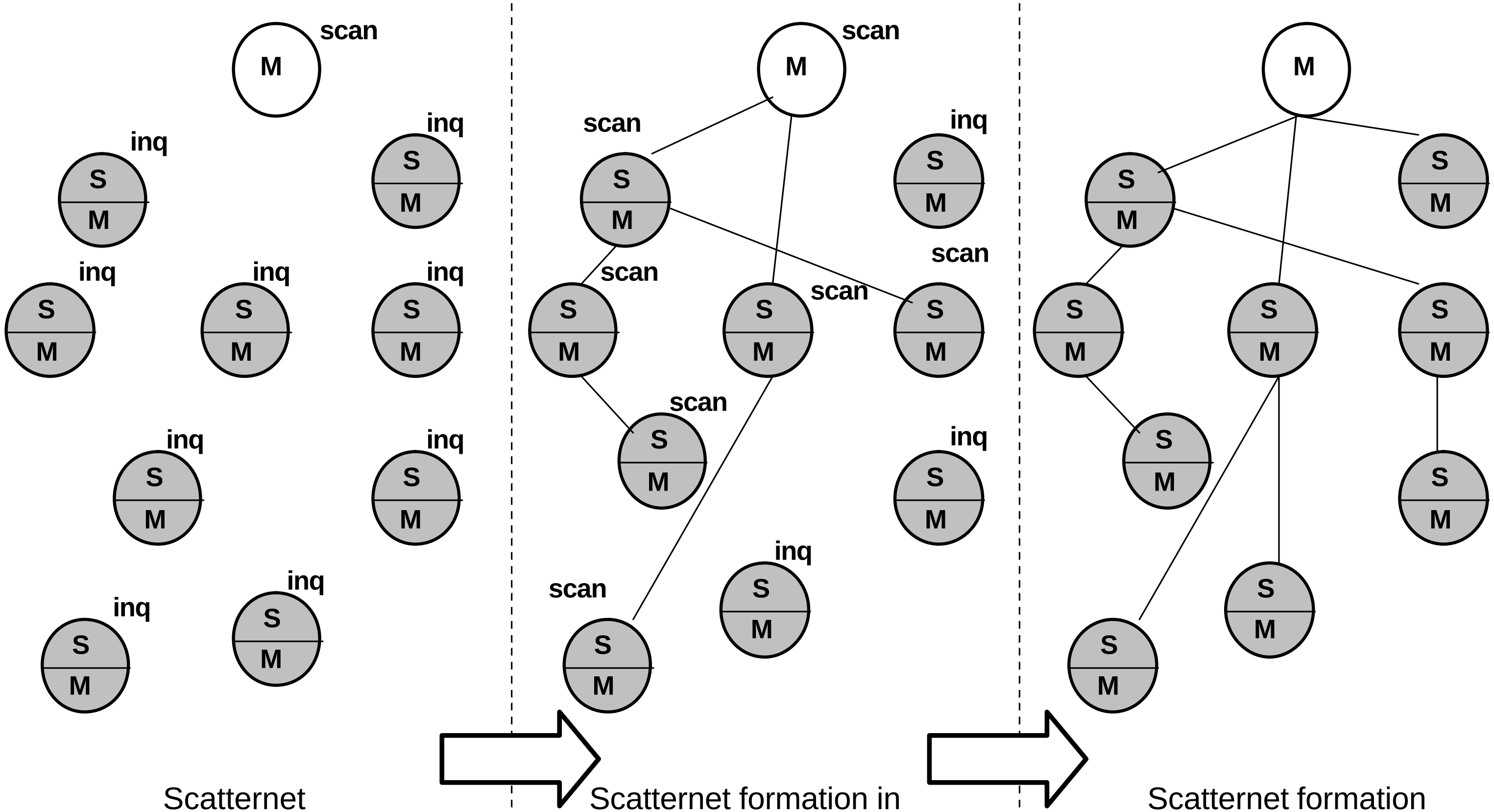
Design Goals

- Design goals :
  - Scatternet formation involves pre-configured private piconets with existing security associations.
  - Devices should be properly authenticated before associating with the scatternet, new devices can join only by invitation.
  - All scatternet traffic is encrypted.
  - The scatternet formation should involve minimal (if any) user interactions.
  - Once scatternet formation completes the devices dedicate all their energy in communication.
  - Create a topology which simplify routing.
  - BTH 1.1 compliant.

Secure Scatternet Topology Formation Protocol

- Our scatternet protocol only allows a master of the piconet called as Pico-Head (PH), to participate.
- A particular user chooses its PH as ROOT, takes an action like “hosting” a meeting and enters the *scatternet PIN.*
- Other users wanting to participate take an action like “joining” a meeting and enter their *scatternet PIN*.
- Root PH starts scanning (both inquiry and page scanning) and other PH start inquiring.
- On successful inquiry, the PH pages the discovered PH, which authenticates using the *scatternet PIN*.
- If authentication succeeds, devices connect and perform a role-switch.
- Each PH on attachment starts scanning inviting other free PHs.
- Once scatternet is formed, all devices stop scanning.

Secure Scatternet Topology Formation Protocol contd…



Scatternet formation starts

Scatternet formation in progress

Scatternet formation completes

Secure Scatternet Topology Formation Protocol contd…

USER A

Creating Meeting…

Meeting Name : project

Password : PIN

DONE

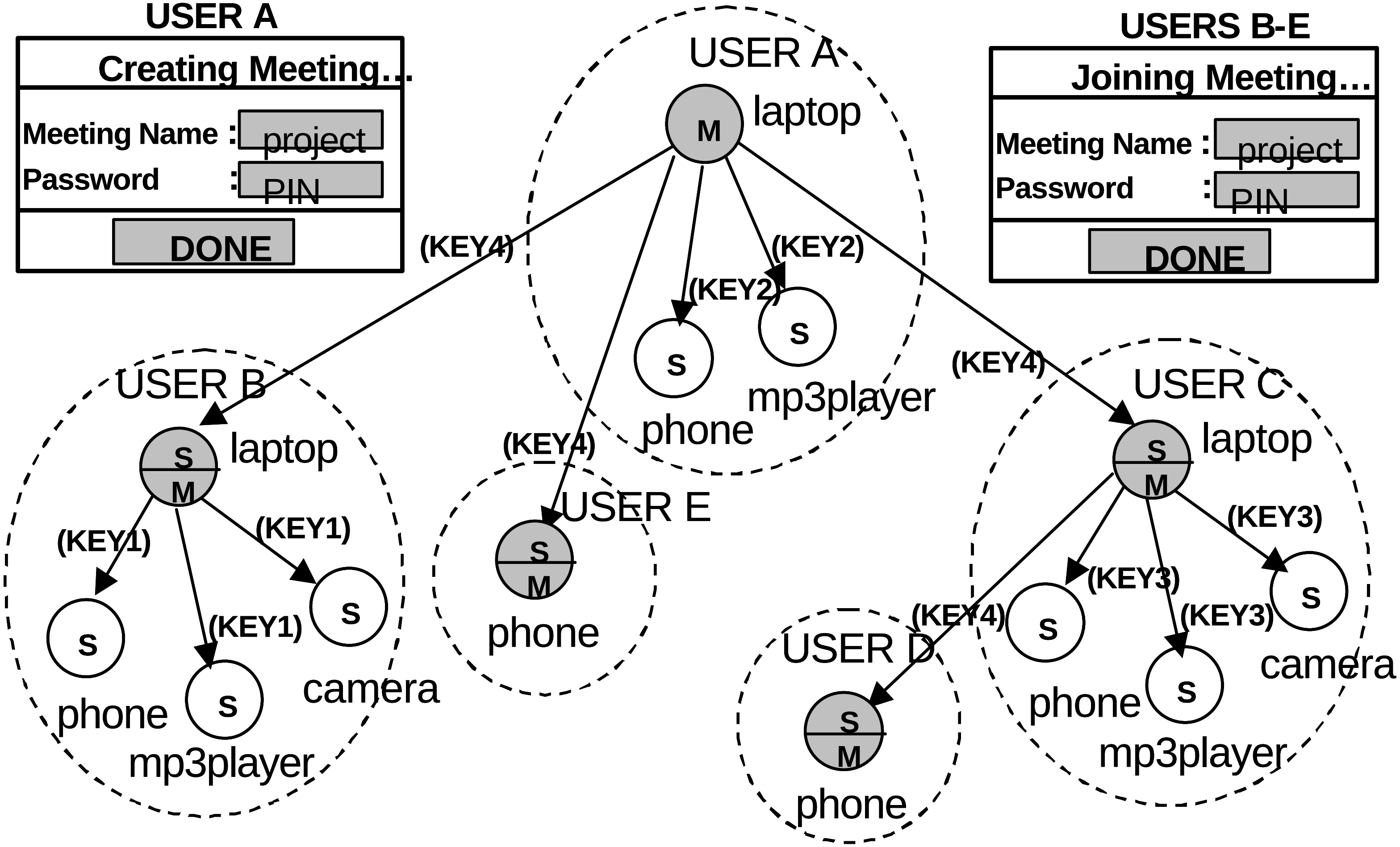
USERS B-E

Joining Meeting…

Meeting Name : project

Password : PIN

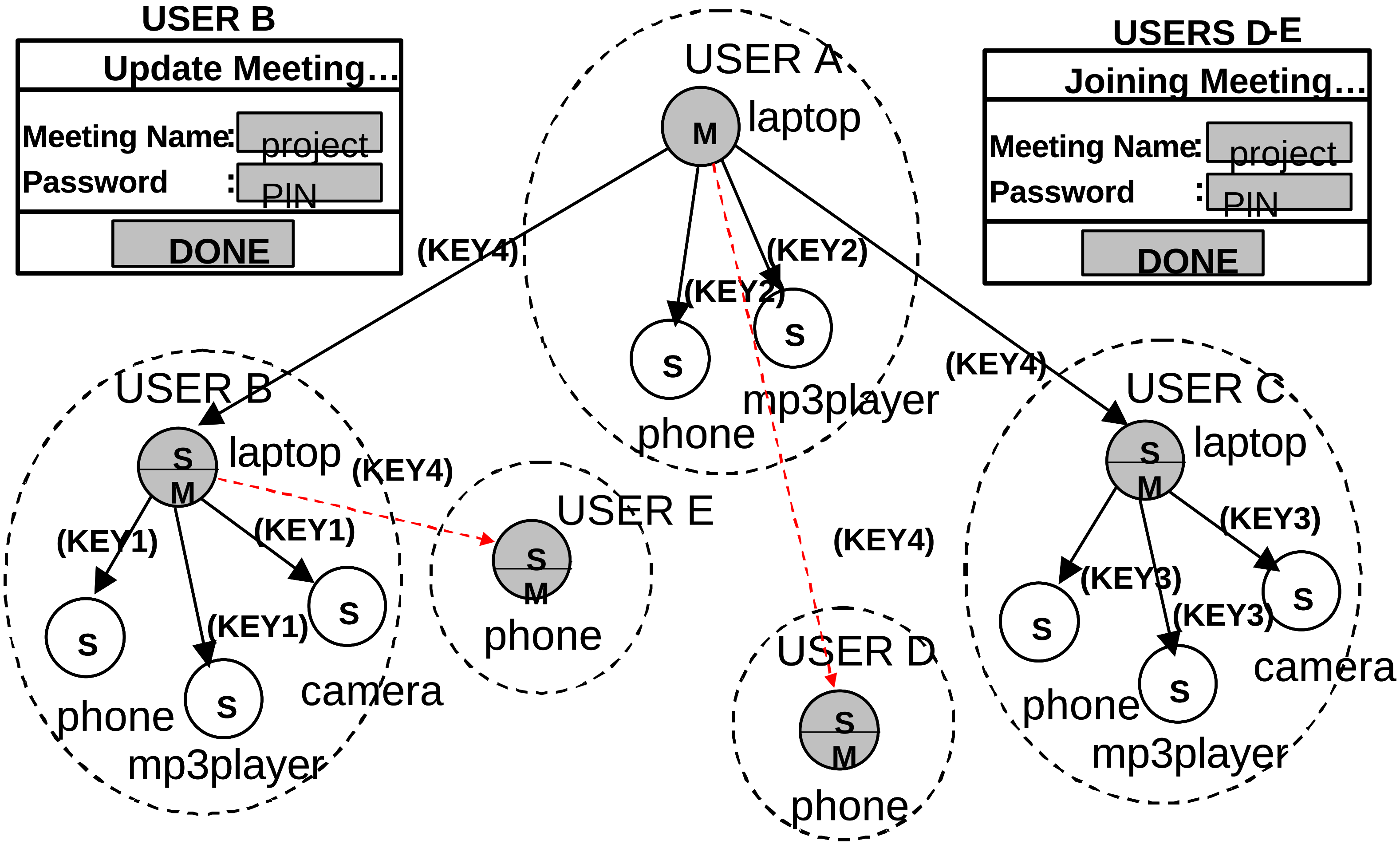
DONE



Secure Scatternet Topology Update Protocol

- Our protocol allows new users to join the scatternet by invitation.
- Participating user takes an action like “updating” a meeting on any PH.
- That PH broadcasts an UPDATE scatternet message to all PH in the scatternet and starts scanning.
- On receiving the UPDATE message each PH starts scanning and becomes a potential attachment point.
- New user take an action like “joining” the meeting and enters the *scatternet PIN*, PH starts inquiring. On successful inquiry, the PH connects to the discovered PH after proper authentication.
- Once the scatternet updates all devices stop scanning.

Secure Scatternet Topology Update Protocol contd…



USER B

Update Meeting…

Meeting Name: project

Password : PIN

DONE

USERS D-E

Joining Meeting…

Meeting Name: project

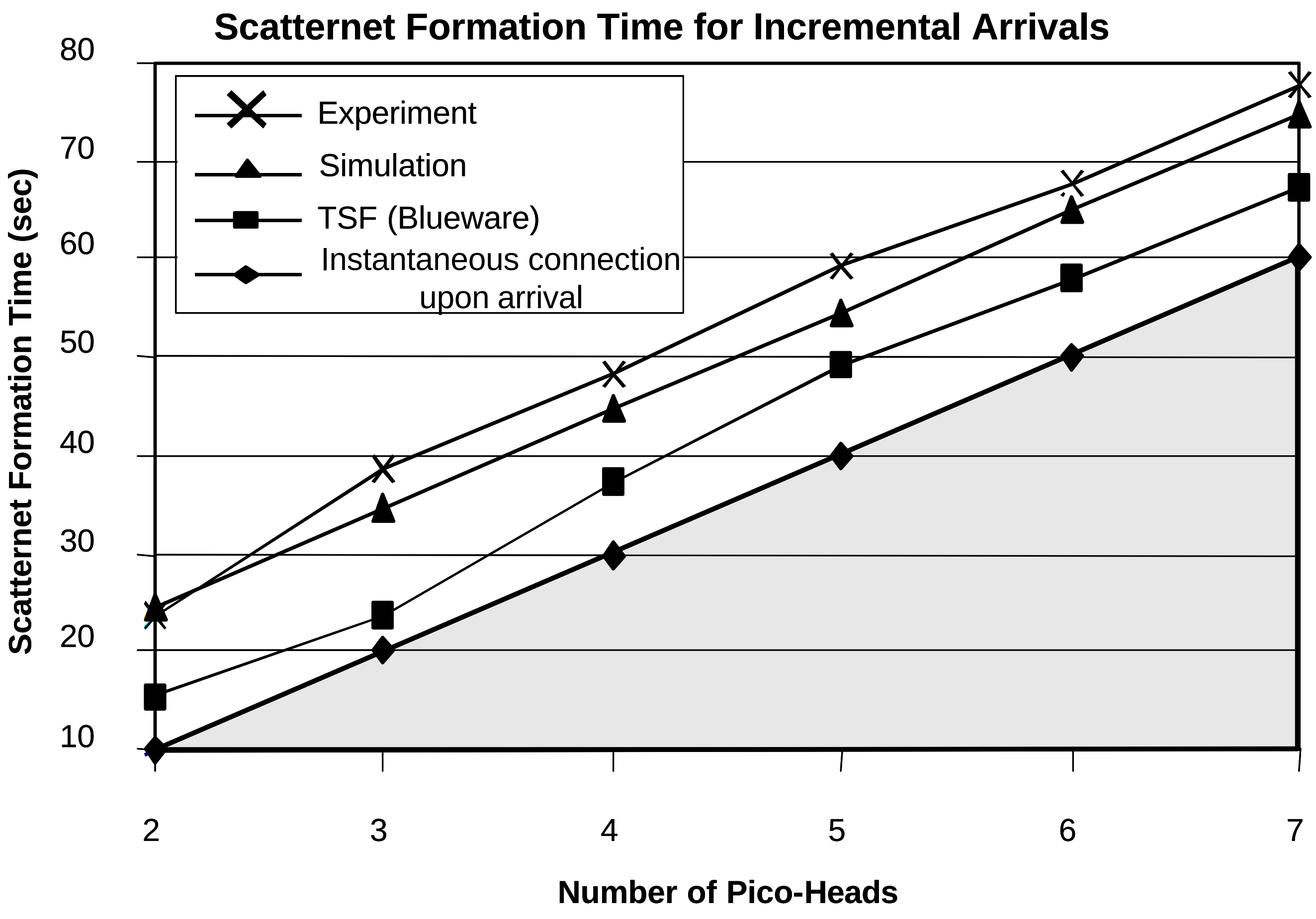
Password : PIN

DONE

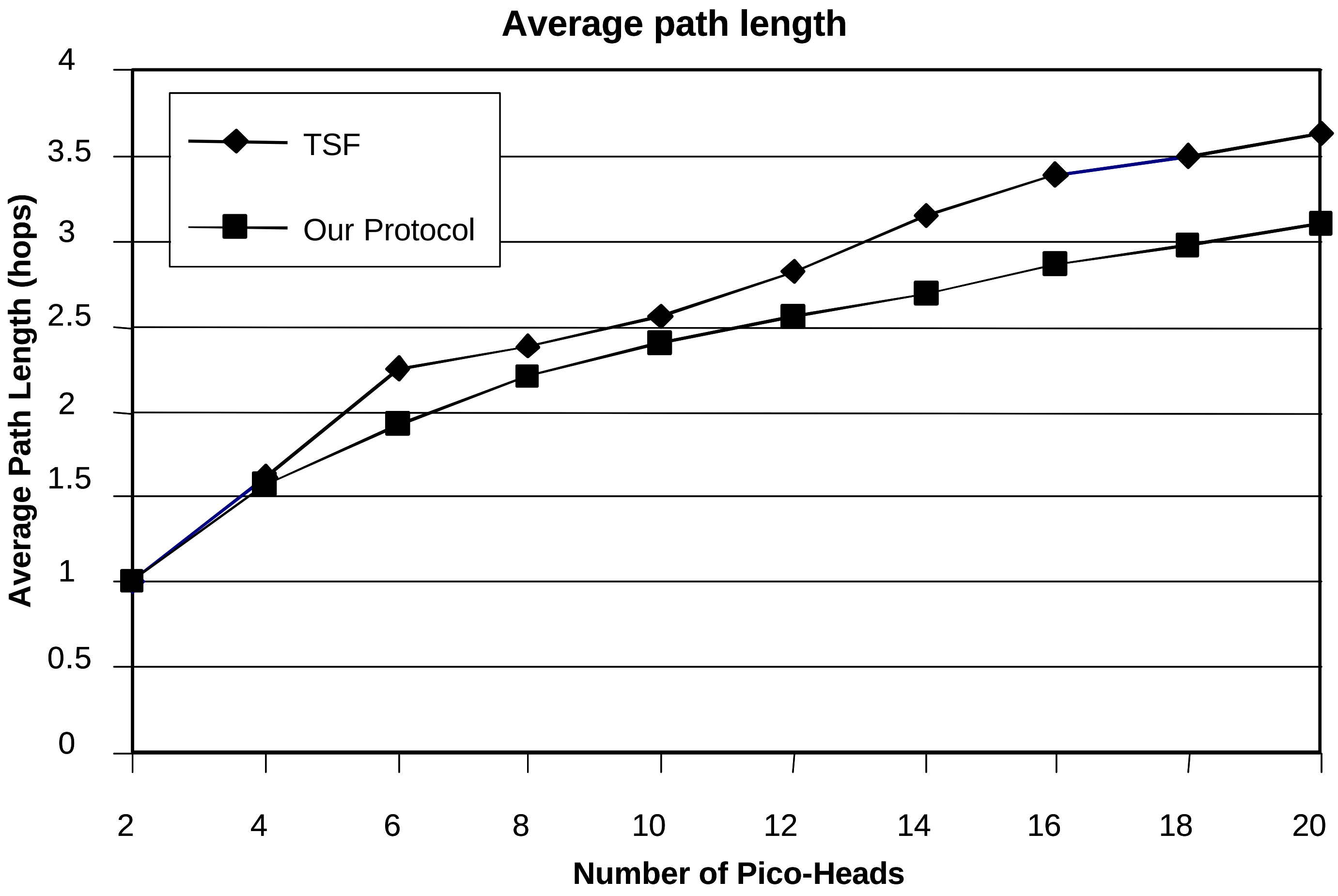
Experimental Setup

- Prototyped our scatternet formation protocol using BTH v1.1 compliant hardware, running Linux kernel 2.4.18 with Bluez stack v2.2.
- We equipped nodes with dual-radios, since no off-the-self BTH hardware supported master/slave (or slave/slave) scatternet operation at that time.
- Simulated our protocol over modified Blueware ns-simulator.
- Modified Blueware by introducing important features like periodic page scan mode, randomized inquiry/paging start time and fine tuned BTH parameters like page-timeout value, randomized selection of Inquiry Train.

Performance Results



Performance Results (contd…)



Conclusions

- Simple scatternet formation protocol to enable secure group collaboration using Bluetooth.
- Our protocol requires BTH authentication before allowing devices to join the scatternet.
- Our protocol allows encryption of the inter-(private) piconet and intra-(private) piconet with separate keys.
- Once scatternet formation completes no device is scanning making scatternet undiscoverable and unconnectable to the intruders.

Future Work

- Future work will include solving problem where the intruder compromise the network by discovering the *scatternet PIN* and joining the scatternet.
- Another challenge is dealing with dynamic environment enhancing existing protocol to provide secure healing protocol.
- Finally developing access control framework to provide selective and dynamic access to specific scatternet devices.

Thank You