Bluetooth Access Control with Revolving Security Keys

George Mason University
{ahtoo,snorth2,wshaw,csmitn}@gmu.edu

Abstract

This paper presents a design for the purpose of increasing security in multi-hop ad hoc wireless networks, specifically in Bluetooth devices. This design incorporates the concept of using revolving security keys to increase the difficulty for intruders to gain access to end-points in the ad hoc wireless network. This paper discusses the network topology for managing the network when using revolving keys. Additionally, this paper analyzes existing solutions for improving network security and the problems with their implementation.

1. Introduction

2. Background

2.1. An example of eavesdropping on a Bluetooth network to steal user data

2.3. Bluebugging

2.4. Bluesnarfing

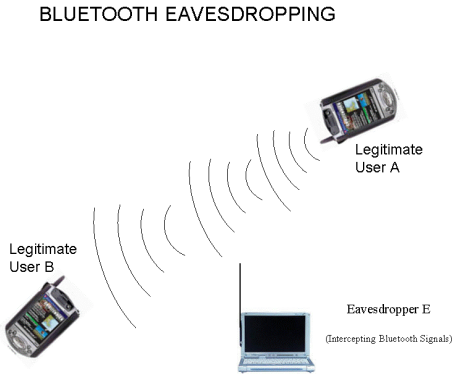


Fig 1a

2.5. Bluetooth Wardriving

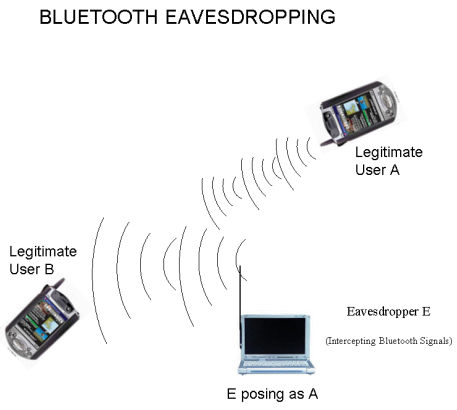


Fig 1b

2.6. Backdoor attack

2.2. Bluejacking

2.7. Car Whisperer

3. Existing Solutions

3.1. Bluetooth Capabilities and Security Threats

3.3. Authentication and Authorization

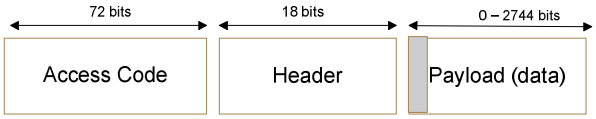
3.2. Ad Hoc Networks and Confidentiality

3.4. Nokia's Bluetooth Solution

3.6. PIN Code Usage in Bluetooth

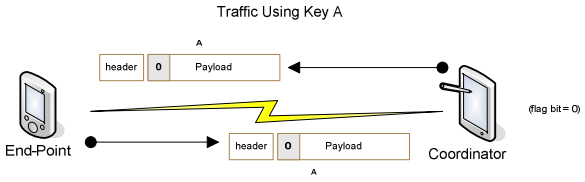
3.5. Security Key Enforcement

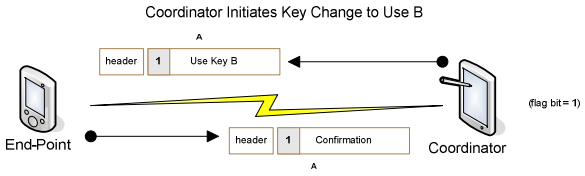
3.7. Level of Security

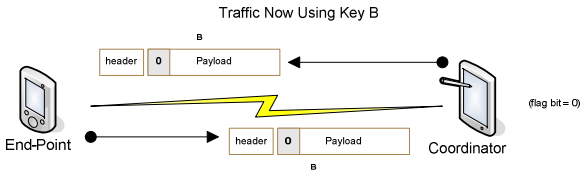


5. Network Topology

5.1. Overview

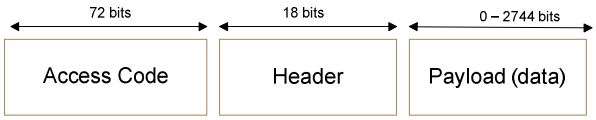






5.1.1. Hierarchy Algorithm

N



5.2. Point-to-Point

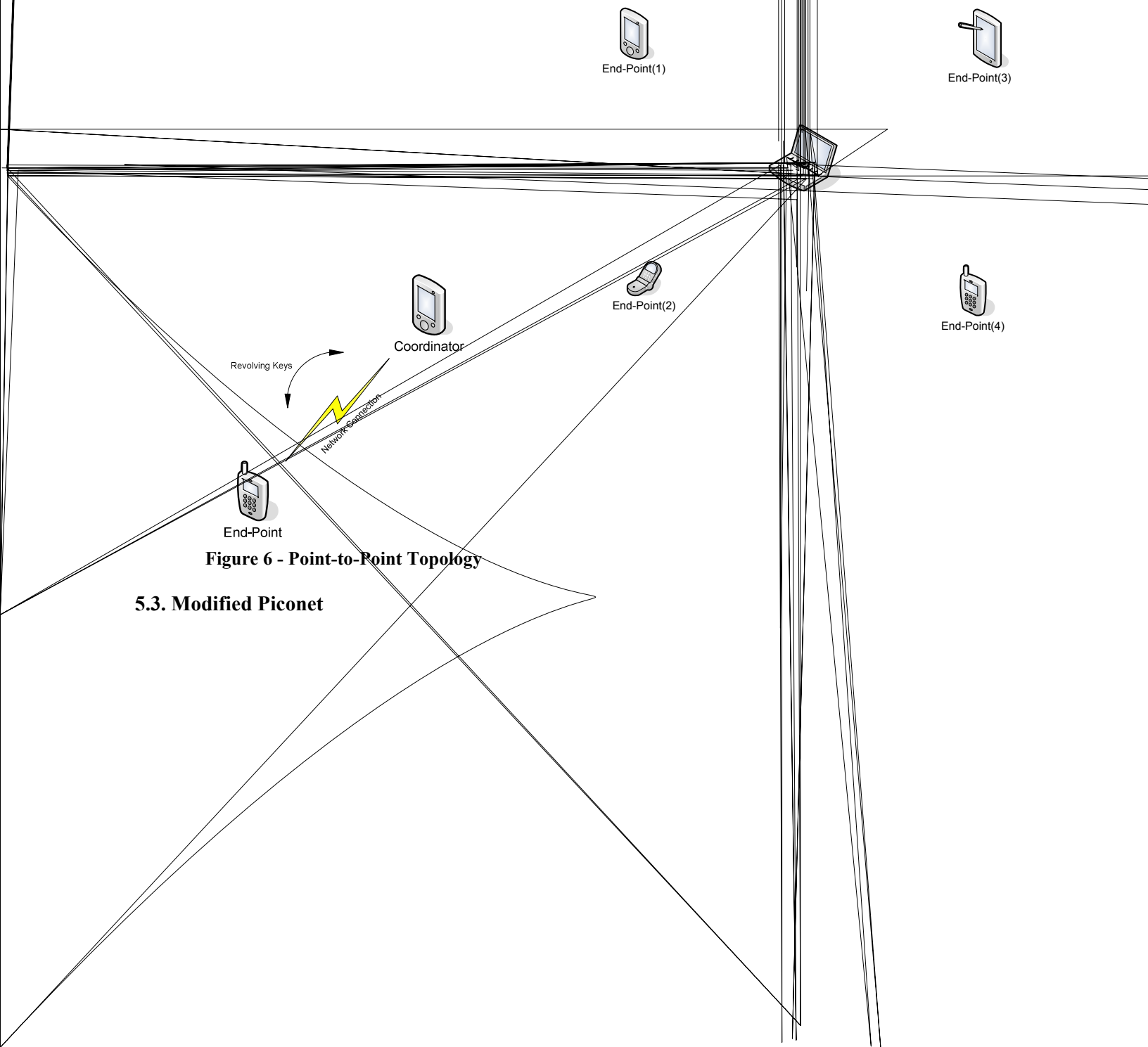


Figure 6 - Point-to-Point Topology

5.3. Modified Piconet

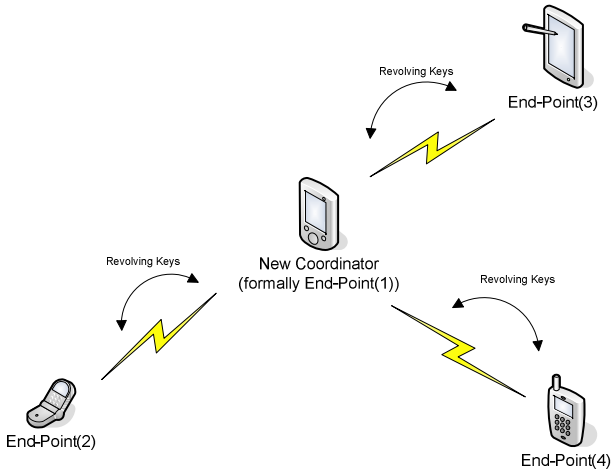


Figure 8 - Piconet after Failure

5.4. Advanced Piconet with Multiple Coordinators

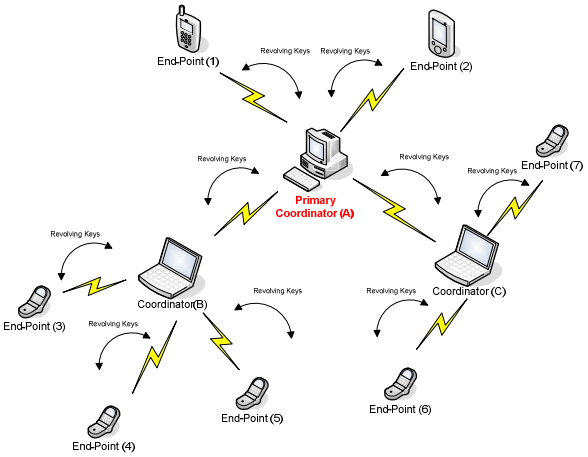
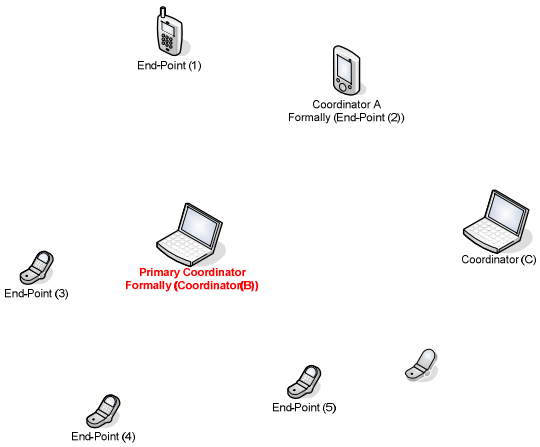


Figure 9- Advanced Piconet w/ Multiple Coordinators

5.4.1. Failover Mode


End-Point (1)
Coordinator A
Formally (End-Point (2))
Primary Coordinator
Formally (Coordinator(B))
Coordinator (C)
End-Point (3)
End-Point (4)
End-Point (5)

MobiHoc, 2002

Bluetooth

Security

7. References

Mobisys 2005 proceedings

Sensys '04,

ISSS '02,

Proceedings of the 1st ACM Workshop Security of Ad Hoc and Sensor Networks,