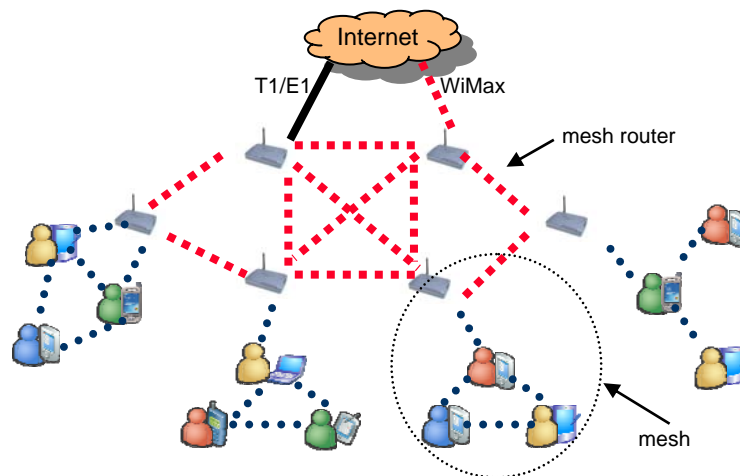


Final Report: Privacy-aware Secure User Communication for Metropolitan Wireless Mesh Networks

Kui Ren

ECE, IIT

Wireless mesh networks (WMNs) as shown in the below picture have recently attracted increasing attention and deployment as a promising low-cost approach to provide last-mile high-speed Internet access at metropolitan scale [1, 2]. Security and privacy issues are of most concern in pushing the success of WMNs for their wide deployment and for supporting service-oriented applications. Due to the intrinsically open and distributed nature of WMNs, it is essential to enforce network access control to cope with both free riders and malicious attackers. Dynamic access to WMNs should be subject to successful user authentication based on the properly preestablished trust between users and the network operator; otherwise, network access should be prohibited. On the other hand, it is also critical to provide adequate provisioning over user privacy as WMN communications usually contain a vast amount of sensitive user information. The wireless medium, open network architecture, and lack of physical protection over mesh routers render WMNs highly vulnerable to various privacy-oriented attacks. These attacks range from passive eavesdropping to active message phishing, interception, and alteration, and easily lead to the leakage of user information. Obviously, the wide deployment of WMNs can succeed only after users are assured for their ability to manage privacy risks and maintain their desired level of anonymity. Our long-term goal is to establish a novel user security and privacy framework for metropolitan WMNs. This lightweight framework is aimed at providing the following capabilities in a single protocol suite:



- **Network Access Security and Anonymity:** It achieves explicit mutual authentication and key establishment between users and mesh routers and between users themselves. It thus prohibits both illegal network access from free riders and malicious users and phishing attacks due to rogue mesh routers. It simultaneously enables unilateral anonymous authentication between users and

mesh routers and bilateral anonymous authentication between any two users in a single protocol suite. It thus ensures user anonymity and privacy.

- **User Accountability:** It enables user accountability, aimed at regulating user behaviors and protecting WMNs from being abused and attacked. It can always audit network communications in the cases of disputes and frauds. It further allows dynamic user revocation so that malicious users can be evicted.
- **Sophisticated User Privacy:** It allows users to disclose minimum information possible while maintaining accountability. It allows privacy-aware secure user communication, while satisfying the above two capabilities simultaneously.

In this project, we specifically focused on privacy-aware secure user communication research in the context of the above long-term security framework for metropolitan WMNs. Particularly, we are successful to establish a lightweight privacy-aware secure user communication protocol for metropolitan WMNs, which contains the following components:

- An efficient anonymous routing protocol, which avoids network-wide flooding when establishing the routes, while ensuring both sender and receiver anonymity. We note that all existing anonymous routing protocols targeted for general multi-hop wireless networks require network-wide flooding whenever a route needs to be established.
- An anonymous network access control protocol, which seamlessly integrated with the above anonymous routing protocol. This protocol prevents the WMNs from being abused by outsider attackers.
- A forward-secrecy converter, which can efficiently convert the above two protocols into the ones with forward-secrecy property. Forward-secrecy guarantees that compromising user long-term secret keys will not harm the secrecy and privacy of his past communications. We note that no existing work for WMNs could offer forward-secrecy property.

Research Results:

Publications: So far, our research has generated a number of related publications including one in the most prestigious conferences such as IEEE ICDCS. We list them below:

Zhiguo Wan, Kui Ren, Bo Zhu, Bart Preneel, and Min Gu, "Anonymous User Communication for Privacy Protection in Wireless Metropolitan Mesh Networks," AsiaCCS 2009, 10-12 March 2009, Sydney, Australia, 2009

Yanchao Zhang and Kui Ren, "Towards Address Privacy in Mobile Ad Hoc Networks," To Appear, ACM Mobile Networks and Applications (MONET), 2009

Yong Hao, Yu Cheng, and Kui Ren, "Distributed Key Management with Protection against RSU Compromise in VANETs," Globecom, Nov. 30-Dec. 4, New Orleans, LA, 2008

Kai Zeng, Shucheng Yu, Kui Ren, and Wenjing Lou, "Towards Secure Link Quality Measurement in Multihop Wireless Networks," Globecom, Nov. 30-Dec. 4, New Orleans, LA, 2008

Wei Ren, Kui Ren, Wenjing Lou, and Yanchao Zhang, "Efficient User Revocation in Privacy-aware PKI," ICST QShine, Jul. 28-31, HongKong, 2008

Yanchao Zhang and Kui Ren, "Towards Address Privacy in Mobile Ad Hoc Networks," ICST QShine, Jul. 28-31, HongKong, 2008

Zhiguo Wan, Kui Ren, and Bart Preneel, "A Secure Privacy-Preserving Roaming Protocol Based on Hierarchical Identity-Based Encryption for Mobile Networks," ACM WISEC, Mar. 31-Apr. 2, VA, 2008

Kui Ren and Wenjing Lou, "A Sophisticated Privacy-enhanced Yet Accountable Security Framework for Wireless Mesh Networks," **IEEE ICDCS 2008**, Beijing, China, June 17-20, 2008 (acceptance rate = 102/638 < 16%)

Bo Zhu, Kui Ren, and Lingyu Wang, "Anonymous Misbehavior Detection in Mobile Ad Hoc Networks," The 1st Workshop on Wireless Security and Privacy, Jun. 17-20, Beijing, China, 2008

Wei Ren, Kui Ren, and Wenjing Lou, "Optimized User Revocation for Group Signature Based Privacy-aware PKI," The 1st Workshop on Wireless Security and Privacy, Jun. 17-20, Beijing, China, 2008

Zhiguo Wan, Kui Ren, Wenjing Lou, and Bart Preneel, "Anonymous ID-based Group Key Agreement for Wireless Networks," IEEE WCNC, Network Track, 2008

External Funding:

The research result from this proposal also contributes partly to three NSF proposals that the PI current have as listed below:

PI, CT-ISG: Collaborative Research: Privacy-Preserving Secure Communications in Wireless Mesh Networks

Single PI, NeTS-NECO: COLLABORATIVE RESEARCH: New Approaches for Secure and Dependable Distributed Data Storage and Access Control in Mission-critical Wireless Sensor Networks

Co-PI, NeTS - NECO: A Paradigm for a Healthy Nested Data Network in Medical Environments

The above second proposal has been awarded by NSF as a three-year grant. (CNS-0831963, \$273,680)