CRYPTOGRAPHIC SECURITY IN WIRELESS NETWORKS VIA PHYSICAL LAYER PROPERTIES

By

Matthew Edman

A Thesis Submitted to the Graduate

Faculty of Rensselaer Polytechnic Institute

in Partial Fulfillment of the

Requirements for the Degree of

DOCTOR OF PHILOSOPHY

Major Subject: COMPUTER SCIENCE

Approved by the
Examining Committee:

_____
Dr. Bülent Yener, Thesis Adviser

_____
Dr. Biplab Sikdar, Member

_____
Dr. David Spooner, Member

_____
Dr. Paul Syverson, Member

_____
Dr. Boleslaw Szymanski, Member

Rensselaer Polytechnic Institute
Troy, New York

May 2011
(For Graduation August 2011)

ABSTRACT

Secure cryptographic authentication and key exchange is a difficult problem in general. The problem becomes even more challenging in wireless ad hoc and sensor networks due to the often limited storage and computational capabilities of network nodes and the unstructured deployment environment. Network devices deployed in a hostile environment are subject to potential seizure, compromise and modification by an adversary.

Standard authentication and key exchange protocols that rely on network devices to store persistent secret keying material in their non-volatile memory, such as is common for traditional PKI-based approaches, are thus unsuitable for deployment in hostile environments due to the possibility that their stored secret keying material may be compromised. The adversary would then be able to eavesdrop on encrypted messages sent by one or more nodes in the network, or even impersonate a legitimate network device in a traditional authentication protocol.

To solve these challenges, we consider novel approaches to key establishment and authentication proposed for use in wireless networks that leverage physical layer properties to enhance cryptographic protocols. First, we evaluate techniques for symmetric cryptographic key generation and renewal that enable two nodes to derive shared secret keying material based on the physical property of channel reciprocity of the wireless channel between them. By using a physical layer approach to shared key extraction, a pair of wireless devices can derive a symmetric key without relying on pre-shared keying material or post-deployment topology constraints.

While physical layer key extraction provides confidentiality without key predistribution, it does not, however, provide device authentication. To that end, we further evaluate techniques that leverage unique physical properties of network devices that result from natural manufacturing and environmental processes that enable us to relate the identity of each node in the network to their individual hardware fingerprints. Since physical-layer identification and authentication is based on properties inherent in the wireless devices themselves rather than stored secrets,

physically compromising a wireless device after deployment should not allow an adversary to impersonate that device.

While some prior work has been done in the area of developing physical layer security protocols, no rigorous analysis of the potential threats posed by both passive and active adversaries attempting to subvert physical layer key extraction and authentication has been conducted within real-world environments. Our work shows that, contrary to previous assumptions, a passive adversary within transmission range of a legitimate wireless transceiver has a non-trivial advantage in deducing portions of a symmetric key extracted by that device. We further analyze the additional advantage gained by multiple coordinating passive adversaries who collude to more accurately infer the symmetric key extracted between two devices.

In addition to strictly passive attacks, we propose and evaluate active attacks executed by an adversary attempting to influence the physical-layer key extraction protocol via targeted RF interference in order to induce predictable patterns in the derived secret keys. We find that an adversary can significantly reduce the effort necessary to reconstruct a shared symmetric key by intentionally delaying the key extraction protocol executed between two nodes, which additionally has important ramifications for physical-layer security in heavily congested networks.

Finally, we consider physical device identification techniques based on observed clock skew and modulation error characteristics. We introduce a distributed approach to physical device authentication in wireless sensor networks, based on the clock skew unique to each node in the network and also consider active man-in-the-middle and other impersonation attacks against related schemes. We also successfully demonstrated that an active adversary equipped with a software-defined radio device can, with reasonable probability, impersonate the modulation error characteristics of another device in order to subvert radiometric identification schemes.