FORMAL SECURITY ANALYSIS OF A SECURE ON-DEMAND ROUTING PROTOCOL FOR AD HOC NETWORKS USING MODEL CHECKING

by

Evren Önem

B.S. in Mathematics, Boğaziçi University, 2003

Submitted to the Institute for Graduate Studies in
Science and Engineering in partial fulfillment of
the requirements for the degree of
Master of Science

Graduate Program in Computer Engineering

Boğaziçi University

2007

ABSTRACT

FORMAL SECURITY ANALYSIS OF A SECURE ON-DEMAND ROUTING PROTOCOL FOR AD HOC NETWORKS USING MODEL CHECKING

An ad hoc network is a self-configuring network of mobile terminals, connected by wireless links and exhibiting nomadic behavior by freely moving within an area. Computing the routes between the terminals in the ad hoc environment and delivering a guarantee of communication have never been achieved by any protocol in its entirety. In this work, we model an ad hoc network to model-check ARIADNE in order to verify one of its powerful security properties. By a similar approach to Buttyán's *Active-1-2* attack on ARIADNE, we have used SPIN to flag a sequence of possible events in the protocol leading to a new *Active-2-2* attack, where two compromised nodes collaborate to remove all intermediate nodes from the route-discovery process.

ÖZET

KABLOSUZ TASARSIZ AĞLAR İÇİN GÜVENLİ BİR YÖNLENDİRME PROTOKOLÜNÜN MODEL KONTROL TEKNİĞİ İLE FORMAL GÜVENLİK İNCELEMESİ

Kablosuz tasarsız ağ dediğimiz kavram, belli bir alanda serbestçe hareket ederek gezgin bir davranış tarzı sergileyen, kablosuz olarak birbirine bağlı hareketli terminallerden oluşan bir bilgisayar ağıdır. Kablosuz tasarsız ağlardaki terminaller arasında yönlerin hesaplanması ve iletişim garantisinin sağlanabilmesi şu ana dek hiçbir protokol tarafından tam manasıyla sağlanamamıştır. Bu çalışma, bir tasarsız ağ yönlendirme protokolü olan ARIADNE'nin güçlü bir güvenlik özelliğinin doğrulanması amacıyla formal olarak modellenmesi ve model-kontrolünün yapılmasını içermektedir. Buttyán'in ARIADNE üzerinde sergilenebileceğini gösterdiği *Active-1-2* tipi saldırıya benzer bir yaklaşımla, SPIN yazılımı ARIADNE protokolünde *Active-2-2* tipinde yeni bir saldırıya yol açan olası bir haberleşme serisi bulması için kullanıldı. Bu saldırıda paketin gittiği yol üzerindeki iki anlaşmalı terminal, yol keşfetme işlemi sırasında aralarındaki tüm diğer terminalleri yokmuş gibi gösterebilmektedir.