NOVEL METHODS FOR SECURITY PROTOCOLS AND KEY MANAGEMENT TECHNIQUES IN WIRELESS NETWORKS BASED ON SIGNCRYPTION AND HYBRID CRYPTOGRAPHY

by

Attila Altay Yavuz

B.S., Computer Engineering, Yildiz Technical University, 2004

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 FBE Program for which the Thesis is Submitted

Boğaziçi University

2006

ABSTRACT

NOVEL METHODS FOR SECURITY PROTOCOLS AND KEY MANAGEMENT TECHNIQUES IN WIRELESS NETWORKS BASED ON SIGNCRYPTION AND HYBRID CRYPTOGRAPHY

Providing security in wireless communication networks is one of the most challenging problems in security systems. Broadcast nature of wireless networks make them more vulnerable for eavesdropping and active attacks when compared to terrestrial fixed networks. Also, wireless networks are resource limited especially for power and bandwidth possibilities, which makes harder to provide security in these systems. In addition to these, novel mathematical analysis and rapid development of hardware systems cause an increasing threat over existing security protocols and key management techniques, which are used in wireless networks. These problems become much severe for wireless networks having very large number of members and high member join-leave characteristic.

In this thesis, in order to address aforementioned problems, we propose seven novel studies each of them provide efficient solutions for these problems in wireless networks. In these studies, we develop a generic design structure and design principles. Using these principles, in this thesis, we present our studies in integrated manner so that they propose different solutions for different architecture each of them providing various advantages. We especially focus on providing security in satellite networks and military Mobile Ad-hoc NETworks (MANET) in our studies. Notice that, these wireless networks are one of the most challenging communication networks for providing security since they have very large number of members and highly dynamic member join-leave profile. Also, military MANETs are specifically requires high security and performance together since they are mission critic wireless networks.

We bring novelties to wireless network security systems in three main points: Architectural design, integrated key management techniques and novel cryptographic approaches that have not been used in Secure Satellite Multicast Systems (SSMS) and military MANETs. Our architectural design principles, integrated with hybrid key management techniques, are based on "independency of layers". In this principle, modification in a layer does not affect all other layers in the network system. Our hybrid key management technique combines centralized logical tree based key management techniques and decentralized key management techniques in an efficient manner. Cryptographic methods, which are used in our security protocols, are specifically utilized and adapted to architectural design and hybrid key management approaches of our security protocols. Using these novelties, we propose studies which are briefly mentioned below.

We propose Two-Tier Pintsov-Vanstone Signature Scheme (TTPVSS) protocol, which introduces our independency of layers principle and a novel hybrid key management technique that are basis of our generic architectural design principles. These approaches significantly reduce rekeying workload of satellites and provide many advantages when compared to traditional methods. Also, as a novelty, TTPVSS uses Elliptic Curve Pintsov-Vanstone Scheme (ECPVSS) that provides high security and advantages. Then, utilizing some principles of TTPVSS, we propose a novel three-tier satellite multicast security protocol based on Elliptic Curve Menezes-Qu-Vanstone (ECMQV) and Improved Merkle Cryptosystem (IMC). In this protocol, we use three independent Logical Key Hierarchy (LKH) and decentralized type hybrid key distribution layer, which significantly reduce cryptographic workload of satellite networks. Also, batch keying mechanism is more actively used than TTPVSS. This protocol additionally use special properties of GEO, MEO and LEO satellites for better performance and security. ECMQV, different from classical key exchange and digital signature schemes, achieves major cryptographic goals and security against active attacks that can not be prevents using traditional methods. IMC is our novel cryptographic method that has not been used before in SSMS.

NAMEPS, N-tier sAtellite Multicast sEcurity Protocol based on Signcryption schemes, is our latest protocol for SSMS in this thesis. In NAMEPS, we use N-tiered architecture and Efficient Large Key management protocol (ELK) based hybrid key management technique, which further reduces rekeying and cryptographic workload of satellites and other components of wireless networks. NAMEPS also utilize batch keying mechanism and additionally use validation ticket mechanism that provides advantages. One of the most important property of NAMEPS is that, as a novel approach, we use a multi-recipient signcryption scheme which provides computational and storage advantages when compared to traditional cryptographic approaches. Signcryption is a relatively new concept in cryptography and adapting signcryption based methods to wireless network is a novel and promising approach.

Apart from SSMS, we propose HIMUTSIS; HIerarchical MUlti-Tier adaptive adhoc network security protocol based on SIgncryption type key exchange Schemes for military MANETs. In HIMUTSIS, we propose a novel multi-tier architecture for military MANETS, which reduces threshold cryptography requirement and single point of failure problems as well as minimizing rekeying workload of the components of the military communication network. Also, HIMUTSIS offers a multi-level security system that optimizes security and performance requirements according to needs of military units. As a novelty, we utilize signcryption based key exchange protocols in HIMUTSIS that provides high security and performance together.

In addition to designing network security protocols, we also studied on improving existing cryptosystem. In this sense, we propose IMC (Improved Merkle Cryptosystem), which has significant security advantages over both MC (Merkle Cryptosystem) and VMC (Variant of Merkle Cryptosystem). Security of IMC is compatible with today's modern public key cryptosystem.

Apart form these, we work on STAKE (Signcryption Type Authentic Key Establishment) which integrates signcryption based approaches with our IMC algorithm.

As a result, in this thesis, we present our major studies for wireless network security and cryptography in integrated manner providing many advantages when compared to traditional approaches.

ÖZET

KABLOSUZ AĞLARDA GÜVENLİK PROTOKOLLERİ VE ANAHTAR YÖNETİM TEKNİKLERİ İÇİN SIGNCRYPTION VE HİBRİD KRİPTOGRAFİ TEMELLİ YENİ YÖNTEMLER

Kablosuz iletişim ağlarında güvenliğin sağlanması, güvenlik sistemlerinin en zorlu problemlerinden biridir. Kablosuz ağların tümyayın doğası, onları yerel sabit ağlara nazaran gizli dinleme ve aktif saldırılara karşı daha korunmasız kılmaktadır. Ayrıca, kablosuz ağlar özellikle enerji ve bant genişliği olanakları bakımından sınırlıdır ve bu durum kablosuz ağlarda güvenliği temin etmeyi güçleştirmektedir. Bunlara ek olarak, yeni matematiksel analizler ve donanım alanındaki hızlı gelişmeler, kablosuz ağlarda kullanılan mevcut güvenlik protokolleri ve anahtar yönetim teknikleri üzerinde artan bir tehdit oluşturmaktadır. Bu problemler, özellikle üye sayısının çok fazla olduğu ve üyelerin sisteme giriş-çıkışlarının sık gerçekleştiği dinamik karakteristikteki kablosuz ağlarda daha şiddetli bir hal almaktadır.

Biz bu tezde, yukarıda belirttiğimiz problemleri hedef alarak, her biri kablosuz ağlarda değindiğimiz sorunlara etkin çözümler sağlayan yedi yeni çalışma öneriyoruz. Bu çalışmalarda, genel nitelik içeren tasarım mimarileri ve prensipleri geliştirilmiştir. Bu prensipleri kullanarak, bu tezde yer alan çalışmalar, her biri farklı mimariler için farklı çözümler öneren ve avantajlar sağlayan bütünleşik bir yaklaşımla sunulmaktadır. Bu çalışmaların ana konusunu, uydu ağlarında ve askeri tasarsız mobil ağlarda güvenliğin sağlanması oluşturmaktadır. Bu kablosuz ağlar, çok sayıda ve dinamik özelliğe sahip üyelerden oluştukları için, güvenliğin sağlanması bağlamında en zorlu kablosuz iletişim ağı türleri arasında yer almaktadır. Ayrıca, askeri tasarsız mobil ağlar, görev kritik kablosuz ağlar olmaları nedeniyle yüksek güvenlik ve performansa bir arada ihtiyaç duyar.

Biz bu çalışmalarımızda, kablosuz ağ güvenlik sistemlerine üç temel noktada yenilik getirdik: Mimari tasarım, bütünleşik anahtar yönetim teknikleri ve bildiğimiz kadarıyla daha önce güvenli uydu çoklu yayın sistemleri ve askeri tasarsız mobil ağlarda kullanılmamış yenilikçi kriptografik yaklaşımlar. Sistemlerimizde yer alan karma anahtar yönetim teknikleriyle birleştirilmiş mimari tasarım prensipleri "katmanların bağımsızlığı" prensibi üzerine kuruludur. Bu prensibe göre, katmanlarından herhangi birinde gerçekleşen değişiklik, diğer katmanlara sirayet etmemelidir. Karma anahtar yönetim tekniklerimiz, mantıksal ağaç temelli merkezi anahtar yönetim teknikleri ile dağıtık anahtar yönetim tekniklerinin etkin bir kombinasyonundan oluşmaktadır. Güvenlik protokollerimizde kullanılan kriptografik yöntemler, çalışmalarımızın mimari tasarım ve karma anahtar yöntemlerine uygun olacak şekilde kullanılmış ve adapte edilmiştir. Bu yenilikleri kullanarak, aşağıda belirtilen çalışmaları yaptık.

İlk çalışma olarak, genel mimari tasarım prensiplerimizin temelini teşkil eden, yeni karma anahtar yönetim tekniklerini ve katmanların bağımsızlığı prensibini ortaya atan İki Katmanlı Pintsov-Vanstone İmza Şeması (TTPVSS) protokolünü öneriyoruz. Bu yaklaşımlar, uydu üzerindeki yeniden anahtarlama yükünü önemli ölçüde azaltmakta ve geleneksel yöntemlere nazaran önemli avantajlar sağlamaktadır.Ayrıca, yenilik olarak, TTPVSS yüksek güvenlik ve avantajlar sağlayan Eliptik Eğri Pintsov-Vanstone İmza şemasını (ECPVSS) kullanmaktadır. Bu çalışmayı müteakiben, TTPVSS'nin bazı prensiplerini kullanmak suretiyle, yeni bir Elliptik Eğri Menezes-Qu-Vanstone (ECMQV) ve Geliştirilmiş Merkle Kriptosistemi (IMC) temelli üç katmanlı uydu güvenli çoklu yayın protokolü öneriyoruz. Bu protokolde, uydu üzerine binen yeniden anahtarlama yükünü önemli şekilde azaltan, mantıksal anahtar hiyerarşisi ve dağıtık nitelikli karma anahtar yönetim metotlarını kullanan, üç bağımsız anahtar dağıtım katmanı kullanılmaktadır. Ayrıca, grup halinde anahtarlama mekanizması TTPVSS'ye kıyasla daha aktif bir şekilde kullanılmaktadır. Bu protokol, daha yüksek bir güvenlik ve iyi bir performans sağlamak amacıyla, GEO, MEO ve LEO uydularının kendilerine özgü niteliklerinden de faydalanmaktadır. ECMQV, diğer klasik anahtar değişim ve sayısal imza algoritmalarından farklı olarak, temel kriptografik amaçlara ulaşmakta ve bunlara ek olarak,geleneksel yöntemlerin koruma sağlayamadığı aktif saldırılara karşı da güvenliği temin edebilmektedir. IMC, bizim tarafımızdan önerilen ve daha önce güvenli

uydu çoklu yayın sistemlerinde kullanılmamış olan bir algoritmadır.

NAMEPS, signcryption temelli ve çok katmanlı uydu çoklu yayın güvenlik protokolü, bu tezde güvenli uydu çoklu yayın sistemleri için önerdiğimiz son protokoldür. NAMEPS, uyduların ve kablosuz ağın diğer bileşenlerinin üzerindeki yeniden anahtarlama ve kriptografik yükü daha da azalmak amacıyla, çok katmanlı bir mimariyi ve Etkin Büyük Anahtar Yönetim Protokolü (ELK) temelli karma anahtar yönetimi tekniklerini bir arada kullanmaktadır. Ayrıca, NAMEPS grup anahtarlama mekanizması ve buna ek olarak avantajlar sağlayan bir onaylama bileti mekanizması da kullanmaktadır. NAMEPS'in en önemli özelliklerinden biri, yeni bir yaklaşım olarak, geleneksel kriptografik yöntemlere göre önemli hesaplamasal ve veri saklama yükü avantajı sağlayan, çoklu alıcılı signcryption şemasını kullanmasıdır. Signcryption kriptografide göreceli olarak yeni bir yöntemdir ve signcryption temelli yöntemleri kablosuz ağlara uyarlamak yenilikçi ve gelecek vaat eden bir yaklaşımdır.

Güvenli uydu çoklu yayın sistemleri dışında, askeri mobil tasarsız ağlarda güvenliği sağlamak üzere, HIMUTSIS (Signcryption tipi anahtar değişim şema temelli hiyerarşik çok katmanlı adaptif tasarsız ağ güvenlik protokolü)'i öneriyoruz. HIMUTSIS, askeri iletişim ağlarındaki tek noktaya bağımlılık problemini ve eşik değerli kriptografi gereksinimi azaltacak ve aynı zamanda ağın bileşenleri üzerindeki yeniden anahtarlama yükünü en aza indirecek yeni bir çok katmanlı mimari önermektedir. Ayrıca, HIMUTSIS, askeri birimlerin güvenlik ve performans gereksinimlerini, bu birimlerin ihtiyaçlarına göre optimize eden çok seviyeli bir güvenlik sistemi de önermektedir. Yeni bir yaklaşım olarak, HIMUTSIS, yüksek performans ve güvenlik sağlayan signcryption temelli anahtar değişim protokollerini kullanmaktadır.

Bu tez çalışmamızda, ağ güvenliği protokolü tasarımlarına ek olarak, mevcut bazı kriptosistemlerin iyileştirilmesi üzerinde de çalıştık. Bu bağlamda, orijinal Merkle kriptosistemi (MC) ve onun bir varyantı olan VMC üzerinde önemli güvenlik avantajları bulunan Geliştirilmiş Merkle Kriptosistemini (IMC) öneriyoruz. Buna ek olarak, signcryption temelli yaklaşımlarla IMC algoritmasını birleştiren STAKE (Signcryption tipinde kimlik onaylı anahtar oluşturma) protokolü üzerinde de çalışmaktayız.

Sonuç olarak, bu tez çalışmamızda, biz kablosuz ağlarda güvenlik ve kriptografi konularında geleneksel yaklaşımlara nazaran önemli avantajlar sağlayan temel çalışmalarımızı bütünleşik bir şekilde sunmaktayz.