Name : Vinod Kumar
Supervisor : Prof (Dr.) Rajendra Kumar & Dr. S.K. Pandey
Department : Computer Science, Faculty of Natural Sciences
Title of Thesis : Analysis and Design of Cryptographic Algorithms for Secure Group Communication

Abstract

In today's Internet era, group communications have become more and more essential for many emerging applications. Given the openness of today's networks, efficient and secure distribution of common key is an essential issue for secure communications in the group. To maintain confidentiality during communication, all authorized members require a common key called the group key in advance. In the secure multimedia multicast communication, data is transmitted in such a manner that only authorized group members are able to receive the media data. In order to provide secure delivery of multimedia contents in digital pay-TV systems, a large number of keying messages are exchanged for updating the group key/scrambling key in the traditional key distribution schemes. The issues of controlling illegal access to multimedia contents require efficient and secure mechanisms for distribution of common key called scrambling key or group key.

Smart Grid (SG) is a modernized power grid. Nowadays changing the power grid system into a smart grid is revolution and evolution. Owing to the widespread use of wireless communication technologies in AMI of SG, security is one of the most significant and challenging problem. A specific feature of AMI systems is that it requires hybrid transmission modes of data which includes unicast, multicast and broadcast communication modes. Moreover, SMs and smart home appliances may have limited computing and storage capability and only authorized HAN appliances may communicate with SMs. To meet these distinctive requirements and ensure confidentiality during communications in HAN of AMI, secure and robust key management scheme is also required. The main challenging issue in dynamic and secure multicast communication is to design centralized, decentralized and distributed group key management protocols with minimum computation and storages complexity. The designing of secure and efficient key management protocols for pay-TV systems and protocol for AMI of SG which minimizes the computation, communication and storage overheads are also challenging issues.

In this thesis, we aim to study in the area of key management for secure group communication and application in digital pay-TV system and AMI in SG. In the first study, we propose an enhanced and secured RSA public key cryptosystem algorithm using Chinese remainder theorem and based on this enhanced RSA cryptosystem a more efficient centralized group key distribution protocol that minimizes

the computation cost of key server during key updating. Moreover, the storage complexity of KS is also minimized. Further we also propose an extended CGKD protocol based on clustered tree which is scalable and efficient to deal with enormous membership changes.

In the second study, we propose a group key distribution and authentication protocol for dynamic access control in secure group communication using Chinese Remainder Theorem (CRT), which is highly secure and computationally efficient. The protocol, 1) has drastically reduced the computation cost of group controller and members, 2) has provide intense security, 3) has minimized storage and communication overheads, 4) has been decentralized for higher scalability, and 5) is suitable for many practical applications due to intense security along with low computation and storage overheads.

In the third study, we propose an efficient distributed key management scheme using ternary tree for establishing secure communication in large and dynamically updating groups. The computational overhead is reduced drastically since it requires only one key to transmit and only one encryption at member join. Similarly, at member leave, it requires only one key to transmit and $\mathcal{O}(log_3 n)$ encryptions. The storage and communication costs are also minimized. A polynomial based non-interactive session key computation protocol for secure communication in dynamic groups is also proposed. In the proposed protocol, the polynomial is constructed in such a way that it may be used as a generalized polynomial for 'n' members and may be reformed every time by the server whenever there is any change in the group membership.

In the fourth study, we propose key distribution protocol for digital pay-TV systems by which only legal members can access the multimedia contents correctly and the illegal access can be prevented. The protocol is applicable in Conditional Access System (CAS) of digital pay-TV systems without increasing storage and communication overheads on GM and members. An effective key management protocol for access control in Pay-TV system using theory of numbers is also proposed. It drastically reduces the computation time required for key updating. The protocol is also extended to handle the multiple access control.

In the fifth study, we propose a key management scheme tailored for HAN with significantly lower rekeying overhead and enhanced robustness which allows the SM and HAN devices to share a session key between them. As a whole, this thesis focuses on designing the key management schemes for secure group communication and for different category of applications. The first three studies concentrate on designing the key management schemes for centralized, decentralized and distributed environments. The remaining two studies concentrate on designing the key distribution protocols for digital pay-TV system and Advanced Metering Infrastructure of smart grid.