JOURNAL OF TELECOMMUNICATIONS, VOL. 27, ISSUE 2, 2014, PP. 43-49; ISSN: 2042-8839

Multi-Service Group Key Establishment for Secure Wireless Mobile Multicast Networks

Trust T. Mapoka, Yousef. A.S. Dama, Haider M. AlSabbagh, Simon J. Shepherd, Raed A. Abd-Alhameed

Abstract—Recently there is high demand in distributing multimedia services over the internet to ubiquitous and computational intelligent mobile subscribers by the service providers (SPs). In this instance, provision of those services must be restricted to authorized subscribers via integration of authentication and group key management (GKM). GKM with diverse group services subscribed dynamically by moving subscribers in wireless networks has been omitted in conventional approaches. However it is expected that significant key management overhead will arise in them due to multi-services co-existing in the same network. In this paper, we propose a scalable decentralized multi-service GKM scheme considering host mobility in wireless environment. In the scheme, authentication of mobile subscribers and key management phases are delegated from the trusted domain key distributor (DKD) to the subgroup controllers known as area key distributors (AKD). The trusted intermediate AKDs can then establish and distribute the service group keys to valid subscribers in a distributed manner using identity-based encryption without involving the domain key distributor (DKD). This alleviates unnecessary delays and possible bottlenecks at the DKD. We show by simulation that the proposed scheme has some unique scalability properties over known schemes in terms of optimized rekeying communication and storage overheads. The security performance studies have shown resilience to various attacks.

Index Terms—Multicast communication; multi-service group key management, wireless mobile multicast networks

- Trust T. Mapoka, Simon J. Shepherd and Raed A. Abd-Alhameed, School of Engineering and Informatics, Bradford University, Bradford, BD7 1DP, UK
- Yousef A.S. Dama; An-Najah National University, Nablus, Palestinian
- Haider M. AlSabbagh; Department of Electrical Engineering, University of Basra, Basra, Iraq

1 INTRODUCTION

The existing GKM protocols for wired approach as in [1] focus on generating keys and rekeying with dynamic group members. They are divided into centralized, decentralized and contributory [1]. Centralized schemes rely on the centralized server known as the DKD which is a single point of failure for key generation and distribution. Contributory scheme allow group members to cooperate for group key establishment without the DKD involvement. Decentralized schemes partition the group into subgroups each controlled by subgroup controllers to equally distribute the key management tasks hence scalability. Work in [2] further categorizes the GKM as common TEK and independent TEK per subgroup approaches depending on the TEK distribution in the framework. Common TEK approaches such as in [3-5] utilize one TEK for all group members and commonly suffer from 1-affect-n phenomenon; thus rekeying of the new TEK disturbs members in the entire network whenever a membership change occurs. Independent TEK per subgroup alleviate the 1-affect-n phenomenon caused by common TEK approaches such as in [6], by enabling each subgroup to manage its own TEK, thus rekeying of the new TEK is localized within the affected subgroup during membership change. However the GKM protocols do not consider rekeying on host mobility on their implementation which is the focus of this paper.

On the other hand, the existing GKM protocols for wireless mobile approach such as [7-10] focus on generating keys and rekeying with dynamic movements of subscribers. The protocols adopt decentralized framework for scalability. Work in [11] also categorized them according to common TEK [7-9] and independent TEK per subgroup [10] approaches as described in [2] to address similar rekeying issues. However, both the GKM approaches address access control in a single service. In these approaches, all the subscribers have same level of access privilege which enables them full access to the subscribed service if the decryption key is valid or deny access for an invalid decryption key. However, multi-service oriented GKM schemes may focus on multilevel access privileges which could complicate key management. Thus mobile subscribers may subscribe to various multiple services while moving and decrypt them with their keys. Several group oriented applications such as video conferencing, pay-per-view sports channels, and multi-stream mobile TV events may co-exist in the same evolving wireless networks. This would require an efficient GKM scheme for securing those service streams.

In this paper, we introduce a new scalable session key distribution list (SKDL) concept to our earlier multi-service GKM scheme for wireless mobile networks introduced in [12]. The new concept offers the following benefits over the previously proposed schemes;

- Move the authentication of individual mobile receivers from the DKD to the area intermediate trusted key distributor AKD. This alleviates un-