Ad Hoc Networks 9 (2011) 767–787

Contents lists available at ScienceDirect

Ad Hoc Networks

journal homepage: www.elsevier.com/locate/adhoc

Provably secure hybrid key agreement protocols in cluster-based wireless ad hoc networks

Ratna Dutta *, Tom Dowling

Computer Science Department, National University of Ireland, Maynooth, Co. Kildare, Ireland

ARTICLE INFO

Article history:
Received 13 March 2009
Received in revised form 22 April 2010
Accepted 30 August 2010
Available online 1 October 2010

Keywords:
Clustering
Provable security
Wireless ad hoc networks
Group key agreement
Key distribution

ABSTRACT

Wireless ad hoc networks support rapid on-demand and adaptive communication among the nodes due to their self-configurable and autonomous nature and lack of fixed infrastructure. Security is a crucial factor for such systems. Since ad hoc networks rely on the collaboration principle, the issue of key distribution and efficient group key management in such networks represents two of the most important problems. We describe hybrid solutions to the problem of key distribution and key management by reflecting ad hoc networks in a topology composed of a set of clusters. To date no security proofs exist for these types of protocols. We present two dynamically efficient schemes. We show that both our hybrid schemes are provably secure in the standard model under Decision Diffie–Hellman (DDH) assumption. The proposed protocols avoid the use of a trusted third party (TTP) or a central authority, eliminating a single point of attack. We analyse the complexity of the schemes and differentiate between the two approaches based on performance in a wireless setting. In comparison with the existing cluster-based hybrid key agreement protocols, our proposed approaches individually provide better performance in terms of both communication and computation, handle dynamic events efficiently, and are supported by sound security analysis in formal security models under standard cryptographic assumptions.

1. Introduction

Ad hoc wireless networks offer anytime-anywhere networking services for infrastructure-free communication over the shared wireless medium. In this setting, secure group key agreement and efficient group key management are considered challenging tasks from both an algorithmic and computational point of view due to resource constraint in wireless networks. There are a wide variety of applications of wireless ad hoc networks in many areas ranging from military applications, emergency, law enforcement, rescue missions and other collaborative applications for commercial uses. Security is one of the most crucial factors for such systems. Designing communication efficient secure group key agreement protocols in wireless ad hoc networks has attracted significant attention due to popularity and increased security concerns of wireless ad hoc networks. There are quite a number of group key agreement protocols described in the literature [6,7,10,13,14,16,17,24,28,34]. However, traditional group key agreement protocols are not applicable in ad hoc networks. The major challenges in providing secure authenticated communication for wireless ad hoc networks come from the following unique features of such networks:

(i) lack of a fixed reliable public key infrastructure,
(ii) dynamic network topology due to high mobility and joining/leaving devices,
(iii) energy and resource constrained nodes with limited storage, communication and computation power,

* Corresponding author. Tel.: +353 1 708 4595; fax: +353 1 708 3848.
E-mail addresses: ratna.dutta@gmail.com, rdutta@cs.nuim.ie (R. Dutta), tdowling@cs.nuim.ie (T. Dowling).

1570-8705/$ - see front matter © 2010 Elsevier B.V. All rights reserved.
doi:10.1016/j.adhoc.2010.08.021

(iv) lack pre-distributed symmetric keys shared between nodes,
(v) high-level of self-organization,
(*vi*) vulnerable multi-hop wireless links, etc.

One possible solution to achieve ubiquitous computing in such wireless networks is to enable wireless nodes to operate in an ad hoc mode and self-organize themselves into a cluster-based network architecture. An application of such an architecture is the creation of Virtual Research Clusters in a multidisciplinary geographical setting. Researchers from different backgrounds (*e.g.* Mathematics, Computer Science, Engineering, etc.) can come together and cluster around an idea such as wireless ad hoc network security. Each cluster is lead by a designated professor, called sponsor, who is an expert in the research area associated with that cluster and is able to communicate with sponsors of other clusters. Researcher within a cluster can communicate with each other and also with the sponsor of that cluster. As the cluster develop, new researchers may enter or existing ones leave. At some stage, the idea will become sensitive, so security will be implemented and future enter/leave will be subject to our protocols. This concept has obvious applications in the business world where projects are created and cancelled at great speed. Privacy, authenticity, integrity and availability are four fundamental security issues which must be addressed depending on application specific requirements.

Clustering is a method that enables nodes to be organized based on their relative proximity to one another. Mobile nodes that are within the communication range of each other can communicate directly, whereas the nodes that are far apart have to rely on intermediate nodes to relay messages. This dynamic and multi-hop nature of ad hoc network makes the security one of the most important implementation issue apart from efficiency. A general approach to build up a cluster-based network architecture is to design efficient algorithms to organize wireless nodes into set of clusters. Many clustering algorithms have been proposed to minimize the cluster maintenance overhead, thereby reduce the waste of the precious bandwidth and also saves the consumption of the limited battery power. A detail survey of the clustering algorithms can be found in [40]. We assume ad hoc networks consist of nodes which have no prior contact, trust or authority relation and which may move freely and communicate with other nodes via wireless links. While all nodes are identical in their capabilities, certain nodes are elected to form the sponsors which are vested with the responsibility for the resource assignments, cluster maintenance, and of routing messages for all the nodes within their clusters. Sponsors typically communicate with sponsors of other clusters. The election of sponsors has been a topic of many papers as documented in [3,4,18]. The general idea among the related literature is to select sponsors based on some attributes of the networks, such as node degree, link delay, transmission power, and mobility. There are several mission critical applications (such as in military, emergency, rescue missions), scientific explorations (such as in environmental monitoring and disaster response), civilians (such as in law enforcement, building automation) and other collaborative applications for commercial uses where sponsors have a powerful radio which other nodes in the cluster do not have so that sponsors can communicate among themselves. For example, military networks consist of mobile devices carried by soldiers, automatic weapons, sensing devices, etc. In this setup, a platoon commander may play the role of sponsor and may be able to communicate with platoon commanders of (all/some) other clusters. On the other hand, soldiers are cluster mobile nodes which are able to communicate with the soldiers (and platoon commanders) within their own clusters and may move from one cluster to another.

Group key agreement and key management are easier to handle inside each cluster compared to the entire ad hoc network. This is because of the fact that clusters have more stable internal connections due to the larger amount of links between nodes within the same cluster. Besides, inter-cluster key agreement is more sensible as clusters are assumed to stay together longer than the nodes do in average for wireless ad hoc networks. Clustering may thus bring the necessary scalability into key establishment in very large networks.

1.1. Our contribution

The main contribution in this paper is to obtain two provably secure dynamically efficient authenticated hybrid key agreement protocols, namely AHP-1 and AHP-2 for cluster based wireless ad hoc networks, which are proven to be secure under Decision Diffie–Hellman (DDH) assumption. In a mobile ad hoc environment, the number of nodes could be very large. We divide all the nodes into clusters based on their relative proximity to one another. We differentiate between two types of keys. By cluster key we mean the key generated among all the nodes within a cluster and by session key we mean a common network key among all the nodes in the system. The aim is to generate a session key common to all the nodes in the network. This shared session key can later be used by all the nodes in the network to perform efficient symmetric encryption such as DES [31] and AES [30] for secure and faster communication among themselves.

The basic idea of our constructions are the followings: All nodes within a cluster dynamically generate their cluster keys *using a scalable constant round dynamic group key agreement protocol*. We choose the constant round multiparty dynamic key agreement protocol of Dutta–Barua DB [15] for this purpose, which is a variant of Burmester–Desmedt protocol BD-I [9] and handles dynamic operations very efficiently. Each cluster selects a sponsor using a sponsor selection mechanism. In our first protocol AHP-1, the sponsors form nodes in a spanning tree. Adjacent nodes in this tree will generate a secret key among themselves using 2-party Diffie–Hellman (DH) key agreement. This key used with an appropriate symmetric encryption scheme will be used to distribute the root session key (generated by the root sponsor in the tree) between them. In this way, each sponsor node of each cluster will obtain the root session key. On obtaining the root session key each sponsor will distribute it to the other cluster nodes in its own cluster using the cluster key and an appropriate