Ad Hoc Networks 20 (2014) 163–181

Contents lists available at ScienceDirect

Ad Hoc Networks

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

SKAIT: A parameterized key assignment scheme for confidential communication in resource constrained ad hoc wireless networks ☆

Ramon L. Novales [1], Neeraj Mittal *,[2], Kamil Sarac

Department of Computer Science, The University of Texas at Dallas, Richardson, TX 75080, USA

ARTICLE INFO

Article history:
Received 23 July 2013
Received in revised form 18 March 2014
Accepted 16 April 2014
Available online 24 April 2014

Keywords:
Collusion resistance
Confidential communication
Key predistribution
Symmetric key assignment

ABSTRACT

Predistribution of cryptographic keys is a widely used approach for establishing secure communication between severely resource-constrained nodes with limited or no access to network infrastructure. Many existing key predistribution schemes make the implicit assumption that the contents of the communication messages need not be kept private from nodes other than the intended recipient. Messages in such schemes are not guaranteed to be confidential—they may be read by nodes within the network other than the intended recipient. In this paper, we propose SKAIT, a *parameterized* symmetric key predistribution scheme that guarantees a secure and confidential channel between every pair of nodes in a wireless network. Specifically, our scheme guarantees that the contents of messages exchanged between two nodes in the network cannot be read even by other nodes within the network. But, like many other key assignment schemes, our scheme is also vulnerable to collusion-based attacks in which several nodes can pool their keys together to eavesdrop on communications between other nodes. Parameterization enables control over the number of keys assigned to a node, and allows users to trade increased key space complexity for improved resistance against collusion-based attacks. We also present an extension to SKAIT, referred to as SKAIT-MI, that reduces the minimum number of keys that a node is required to store by replacing the single large key assignment instance with several smaller key assignment instances. We show via simulation that SKAIT and its extension SKAIT-MI provide significantly better resistance against collusion than other proposed schemes that support internal confidentiality—by as much as a factor of two—for a large range of key storage capacities. Finally, we describe an extension to our key assignment schemes to add support for node additions and revocations.

1. Introduction

Due to the open nature of the wireless medium, communication between nodes in wireless networks is vulnerable to eavesdropping by unauthorized nodes or users. In certain classes of networks, such as wireless sensor networks [15,33,29], ad hoc networks [18], mobile networks [21,36], and body sensor networks [39], individual nodes may be resource-constrained. Due to relatively low computational and storage requirements, predistribution of

☆ Parts of this work have appeared earlier in the Proceedings of the 9th International Symposium on Parallel and Distributed Computing (ISPDC), 2010.

* Corresponding author. Address: Department of Computer Science, The University of Texas at Dallas, 800 W Campbell Rd, MS EC 31, Richardson, TX 75080, USA. Tel.: +1 972 883 2347; fax: +1 972 883 2349.
E-mail address: neerajm@utdallas.edu (N. Mittal).
[1] The author is currently working at Symantec in San Francisco, California, USA.

[2] This work was supported, in part, by the National Science Foundation (NSF) under Grant Number CNS-1115733.

http://dx.doi.org/10.1016/j.adhoc.2014.04.006
1570-8705/

symmetric keys has emerged as an attractive solution for securing communication channels between nodes in the absence of any infrastructure. Each node in the network is assigned a set of symmetric keys, and if two nodes share one or more keys in common, they can use those keys to establish a secure channel between them. Such channels are secure against outside eavesdroppers, as only nodes within the network possess the keys necessary to decrypt messages sent along them. Certain key predistribution schemes [15,12,27] make the implicit assumption that the contents of communication messages need not be kept private from nodes within the network other than the intended recipient. Under such schemes, there is no guarantee that other nodes in the network do not possess the keys used to secure a channel; in fact, the same key or keys may be used to secure multiple channels. Further, two nodes with no keys in common choose a shared key and exchange it by using other nodes as intermediaries. Consider, for example, a network secured by such a scheme; nodes x and y wish to communicate with each other, and create a secure channel between them using a common key k_1. There may exist some node z that possesses k_1 and lies within radio range of node x or y (or within radio range of some node on a multi-hop path from x to y). Or, consider the case where nodes x and y wish to create a secure channel between them, but do not share a common key. Nodes x and y find a multi-hop path (say, p_2) between them that consists of secured channels, and then establish a shared key (say, k_2) between themselves using this secure multi-hop path. While k_2 is kept private from eavesdroppers outside of the network, every node in p_2 knows k_2. Further, a node within radio range of p_2 could potentially possess the key used to secure one of the hops, giving them access to k_2 as well. Clearly, these schemes do not guarantee *confidentiality*, as nodes other than the intended recipient may possess the key or keys required to decrypt a message. Although all network nodes may be keyed, deployed, and owned by the same entity, there may be scenarios, such as the handling of sensitive medical data [35], that require the confidentiality property. Further, as discussed in [10,11], these schemes are also vulnerable to impersonation attacks. Key predistribution schemes have been proposed which guarantee confidentiality [17,22,1,14,28,6,37,32,11], and it is to this class of predistribution schemes that this work contributes.

Key predistribution schemes must also address the issues of space complexity (the number of keys that a node is required to store) and collusion resistance (the resilience of the network against pooled-key attacks). As nodes may be resource-constrained and networks may be large, a scheme that scales well in terms of space complexity is desirable. Also, even if a key predistribution scheme satisfies the confidentiality property, it may be possible for nodes to pool their keys, either through collusion or capture by an adversary, and thereby gain the collective ability to decrypt messages that they could not individually. Collusion resistance, which was first defined in [22], measures the ability of a scheme to keep the communication between two nodes confidential in the presence of colluding (or compromised) nodes. Specifically, the r-collusion resistance of a key predistribution scheme is defined as the minimum fraction of channels in the network that remain confidential and cannot be eavesdropped upon by the colluding nodes given that r nodes are colluding to pool their keys.

1.1. Our contributions

We first propose SKAIT (Symmetric Key Assignment by Identifier-Triplet), a novel *parameterized* symmetric key predistribution scheme that guarantees a secure and confidential channel between every pair of nodes in a network. Each node is assigned $w + 2\lceil \frac{n}{w} \rceil$ keys, where n is the number of nodes in the network and w is an adjustable parameter ranging from 5 to $\sqrt{n}$; SKAIT is focused on making use of key storage capacities between $3\sqrt{n}$ and $\frac{2n}{5} + 5$ (for a network of 4096 nodes, this range is from 192 to 1645). SKAIT is suitable for use when network nodes face computational or storage constraints, such as in ad hoc, mobile, or sensor networks. The parameterization of SKAIT allows a user to control the number of keys assigned to a node, making a trade-off between collusion resistance and key space complexity.

SKAIT cannot be used if nodes are severely space-constrained and are able to store fewer then $3\sqrt{n}$ keys only. To address this limitation, we describe an extension to SKAIT, referred to as SKAIT-MI (Multi-Instance SKAIT) that can work with smaller key storage capacities. To that end, we reduce the key assignment problem to $\frac{k(k-1)}{2}$ smaller subproblems, where k is an adjustable parameter ranging from 2 to $\log n$. Each subproblem is then solved using a separate instance of SKAIT. SKAIT-MI can be used for key storage capacities as low as $\frac{4}{3}\log^2 n - 4\log n$.

Using simulation experiments, we show that both SKAIT and SKAIT-MI provide significantly better resistance against collusion than existing key predistribution schemes that support internal confidentiality—by as much as a factor of two—for a large range of key storage capacities.

Finally, we describe an extension to our key assignment schemes to add support for node additions and revocations.

1.2. Roadmap

The remainder of the paper is organized as follows. We summarize the related work in Section 2. The system model is presented in Section 3. We describe SKAIT in Section 4, and present a mathematical analysis of its space complexity, time complexity, and collusion resistance in Section 5. We describe SKAIT-MI—an extension of SKAIT—to work for smaller key storage capacities in Section 6, and also present a mathematical analysis of its space complexity, time complexity, and collusion resistance in Section 7. Section 8 presents a comparison of SKAIT and SKAIT-MI with other comparable key predistribution schemes via simulation experiments. We present extensions to our scheme to allow node addition and revocation in Section 9. Finally, Section 10 concludes the paper.