Computer Networks 87 (2015) 78–88

Contents lists available at ScienceDirect

Computer Networks

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

A-CACHE: An anchor-based public key caching scheme in large wireless networks☆

Lin Yao[a], Jing Deng[b,*], Jie Wang[a], Guowei Wu[a]

[a] School of Software, Dalian University of Technology, Dalian 116023, China
[b] Department of Computer Science, University of North Carolina at Greensboro, Greensboro, NC 27412, U.S.A

ARTICLE INFO

Article history:
Received 4 March 2015
Revised 7 May 2015
Accepted 1 June 2015
Available online 10 June 2015

Keywords:
Asymmetric encryption
Public key
Caching
Large wireless networks

ABSTRACT

When asymmetric cryptography is used in wireless networks, public keys of the nodes need to be made available securely. In other networks, these public keys would have been certified by a certificate authority (CA). However, the existence of a single CA in large wireless networks such as mobile ad hoc networks and wireless sensor networks can lead to a communication hotspot problem and become an easy target for attacks. In this work, we propose a distributed technique, termed A-CACHE, to cache the public keys on regular nodes. One salient feature of our scheme is that some anchor nodes with larger cache memories are exploited. Due to the limited memory size that each node is allowed to dedicate for key caching, only a limited number of keys will be cached. Access to the public keys of other nodes is possible based on a chain of trust. In addition, multiple copies of public keys from different chains of trusted nodes provide fault-tolerant protections and guard against malicious attacks. We explain our technique in detail and investigate its prominent features in this work. Through analysis and evaluations, we observe the existence of an optimum ratio to cache the keys of local nodes.

© 2015 Elsevier B.V. All rights reserved.

1. Introduction

The importance of wireless networks with large number of nodes can never be overestimated. In mobile Ad hoc networks (MANETs), networked nodes form multi-hop topologies instantaneously in order to exchange information among themselves. In wireless sensor networks (WSNs), micro-sized sensor nodes are placed on different fields to detect anomaly and to deliver such results to data sinks. In internet of things (IOT), RFID devices help to link almost every piece of hardware together to form a large wireless network. While many research on large wireless networks have focused on network performance such as throughput, energy conservation, and network lifetime [2–5], many other recent research works investigated the security issues of such networks [5,6].

For instance, passive and active security attacks could be launched from outside by malicious nodes or from inside by compromised/misbehaving nodes. Without appropriate security protections, critical information of the networks can be leaked to adversaries.

Asymmetric cryptography techniques can be used to support information security. Using an asymmetric key scheme, each node in the network has a pair of keys: public key and private key. The public key should be known by all nodes in the network; the private key should only be held by the node itself. In order to achieve information confidentiality, a node uses the public key (of a receiver) to encrypt the message and sends it to the receiver through the wireless network. The encrypted message can only be decrypted by the intended receiver that holds the matching private key. In

☆ An early version of the proposed technique [1] was published and presented in IEEE GLOBECOM '10, CISS symposium, Miami, FL, U.S.A., December 2010.

* Corresponding author. Tel.: +1 3362561112.
E-mail addresses: yaolin@dlut.edu.cn (L. Yao), jing.deng@uncg.edu (J. Deng), andrew340621@163.com (J. Wang), wgwdut@dlut.edu.cn (G. Wu).

http://dx.doi.org/10.1016/j.comnet.2015.06.001
1389-1286/© 2015 Elsevier B.V. All rights reserved.

order to achieve information/message authenticity, a node can use its own private key to sign the message. The receiver then authenticates the message by trying to decrypt the received message using the sender's public key.

However, such public keys may not be readily available or certifiable. Usually, there exists a certificate authority (CA) that will issue certificates for every node. Each certificate, signed by the CA, contains a public key and the identifier of a node. Unfortunately, such a CA is not suitable for large wireless networks. On the one hand, a CA can become an easy target for attackers. For example, the traffic toward the CA can be mis-routed with the use of worm-hole attacks or black-hole attacks. Jamming attacks can be launched by the adversary to blackout all wireless communications in the CA's neighborhood, effectively crippling the security of the entire network. On the other hand, large wireless networks are usually formed by nodes joining and leaving, without any pre-existing infrastructure; therefore, it is unlikely that such a CA exists in large wireless networks.

It is possible to store such public keys on the nodes themselves. A straightforward solution is to store the public keys of all nodes on every node so that every public key is easily accessible. However, there are two difficulties of doing so: the limited resource (such as memory space that can be dedicated to key storage) of such wireless network devices and the network dynamic (e.g., joining nodes, leaving nodes, as well as sleeping/awaking nodes). The limited memory space forbids nodes to store many public keys as they wish. The possibility of having newly joined nodes, nodes that have left, or nodes that might have been sleeping points to methods of storing public keys of only some nodes.

In this work, we propose an anchor-based caching scheme, A-CACHE. We deploy or recruit some nodes to serve as the anchor nodes, which dedicate more memory storage to key caching. These anchor nodes serve their neighborhood for queries for different nodes. We demonstrate that the inclusion of such anchors significantly improve the chance of success in finding the queried keys as well as reduce the query cost.

In addition, in order to increase the chance of query success, nodes should cache a good mixture of the keys of local nodes as well as the remote nodes, where the local nodes are defined as those in the neighborhood of the caching node and the remote nodes are outside of the neighborhood. The cache for local nodes ensures that nodes can be securely connected or trusted based on the cached public keys; the cache for remote nodes ensures that it is possible to find public keys for remote nodes from the queried neighborhood.

Our technique has the following salient features:

- Anchor nodes are used in the network to support the efficient key storage/query process. These anchor nodes are expected to dedicate more memory space for key caching.
- Every node stores two categories of public keys, the keys of local nodes (those in the node's neighborhood) and those of remote nodes. For example, node A can cache one key from m different nodes. Some of these m nodes are local nodes, while the other nodes are referred to as remote nodes since they are located outside of node A's neighborhood. A local caching ratio is assigned to balance the number of these two categories of public keys. We observe that there exists an optimal local ratio to maximize the overall public key availability in different network settings.
- We also design a key update strategy that allows nodes to update their public key caches according to the optimum local ratio. The update process balances the cache for local/remote nodes dynamically and will ensure the high availability of node public keys.

The paper is organized as follows: Section 2 describes recent related works. In Section 3, our public key caching scheme is explained in detail. We analyze the chance of key query success and optimize the local ratio in Section 4. Simulations are performed to evaluate our scheme in Section 5. In Section 6, we summarize our work and discuss future works.

2. Related work

Solutions to the problem of public key management in wireless networks have already been proposed. Key management schemes can be classified into two categories: certificate authority (CA) schemes and distributed schemes. In CA schemes, a trusted central authority has to stay on-line to cope with the changes of public key such as revoking or generating public keys periodically. Because the CA is responsible for the security of the entire network, it is a vulnerable point of the network. To solve this problem, the responsibility of a CA can be distributed [7]. We mainly discuss distributed public key management schemes below.

In distributed schemes, no CA is assumed or established. Instead, trust is usually propagated through a trust graph. Often times, it can be established with the help of the so-called web-of-trust [8]. The trusted nodes share the responsibility of collectively providing the CA functionality for the network to manage and distribute certificate keys. In the credential distribution scheme for key updates [9], users can issue public key certificates and authentication can be performed via the path generated by most trustworthy nodes. In [10], a trust-based threshold cryptography scheme for MANETs is proposed, allowing private keys to be generated by key shares obtained from a set of trustworthy 1-hop neighbors. In the novel certificate-less on-demand public key management (CLPKM) protocol [11,12], end-to-end trust value is used to select the most trusted route to verify public keys. There are other works exploiting the web-of-trust techniques, for example, cluster-based [13,14], binary-tree based [15], composite keys [16], and stable keys [17].

In distributed schemes, it is non-trivial to discover or query the certificate chain. In [18], Mohri et al. proposed a new distributed algorithm to find the certificate-chain and get the public keys. In the technique based on trust graph and threshold cryptography [19], users can issue public key certificates, authenticate each other via certificate chains. In [20], every node generates its own public-private key pair, issues certificates to neighboring nodes, and provides on-demand authentication services by means of gathering certificate chains towards a target node. This model is able to authenticate public keys by selecting the most trustworthy path in certificate chains.

Threshold cryptography scheme is also used in public key management. In [21], mobile certificate authorities

دریافت فوری ← متن کامل مقاله

ISIArticles
مرجع مقالات تخصصی ایران

✓ امکان دانلود نسخه تمام متن مقالات انگلیسی
✓ امکان دانلود نسخه ترجمه شده مقالات
✓ پذیرش سفارش ترجمه تخصصی
✓ امکان جستجو در آرشیو جامعی از صدها موضوع و هزاران مقاله
✓ امکان دانلود رایگان ۲ صفحه اول هر مقاله
✓ امکان پرداخت اینترنتی با کلیه کارت های عضو شتاب
✓ دانلود فوری مقاله پس از پرداخت آنلاین
✓ پشتیبانی کامل خرید با بهره مندی از سیستم هوشمند رهگیری سفارشات