Available online at www.sciencedirect.com

ScienceDirect

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

Computers & Security

Towards efficient certificate status validations with E-ADOPT in mobile ad hoc networks

Mohammad Masdari [a,*], *Sam Jabbehdari* [b], *Jamshid Bagherzadeh* [c], *Ahmad Khadem-Zadeh* [d]

[a] *Department of Computer Engineering, Urmia Branch, Islamic Azad University, Urmia, Iran*
[b] *Computer Engineering Department, Islamic Azad University, North Tehran Branch, Tehran, Iran*
[c] *Computer Engineering Department, Urmia University, Urmia, Iran*
[d] *Iran Telecommunication Research Center, ITRC, Tehran, Iran*

ARTICLE INFO

Article history:
Received 27 April 2014
Received in revised form
10 September 2014
Accepted 18 November 2014
Available online 28 November 2014

Keywords:
Security
PKI
ADOPT
Verification
Caching node
Overheads

ABSTRACT

Each public key infrastructure needs an efficient certificate status validation method to exclude the revoked certificates from network. In this paper, we present a novel certificate validation scheme called E-ADOPT or Enhanced-ADOPT which utilizes a new kind of certificate status information. In this solution, we modify the OCSP response messages to carry information about the accusations issued against the certificate and this additional security information helps the client nodes to tune the OCSP results refresh rate more intelligently. As a result, client node can mitigate the certificate status information inconsistency problem with lower overheads and conduct more effective certificate status validations in MANET. Simulation results demonstrate that by appending accusation-related information to the OCSP responses, our solution achieves better results.

1. Introduction

Mobile ad hoc networks or MANETs are prone to various passive and active security threats (Daza et al., 2007; Jawandhiya et al., 2010). Therefore, providing security in these networks is a challenging issue (Qazi et al., 2013).

By the success of PKI or Public Key Infrastructure in securing the conventional networks, many solutions have been presented to adapt PKI for MANETs. In Omar et al. (2012), Omara et al. studied the existing trust models based on the public-key certificates and classified them into authoritarian models and anarchic models. The simplest approach to implement PKI in authoritarian models is to assign Certificate Authority (CA) tasks to a single node. Also, another kind of CA called DCA or distributed CA can be utilized in mobile ad hoc networks in which CA's private key is distributed among the shareholding DCA nodes and many operations such as issuing or revoking certificates are performed by cooperation of at least k shareholding DCA nodes. These certificate management methods and their features are discussed in (Masdari et al., 2011; Masdari and Pashaei, 2012).

* *Corresponding author.*
E-mail addresses: M.Masdari@Iaurmia.ac.ir (M. Masdari), s_jabbehdari@iau-tnb.ac.ir (S. Jabbehdari), j.bagherzadeh@urmia.ac.ir (J. Bagherzadeh), zadeh@itrc.ac.ir (A. Khadem-Zadeh).

http://dx.doi.org/10.1016/j.cose.2014.11.004
0167-4048/© 2014 Elsevier Ltd. All rights reserved.

In anarchic models or fully distributed approach, each node manages its trusted nodes' certificates. But this method has low scalability and it can only be applied in small MANETs.

Regardless of certificate management method, certificates are revoked to isolate the malicious nodes from network (Liu et al., 2010; Wei et al., 2011; Zhang et al., 2013). As a result, to conduct secure communication, each node needs to verify the validation of its participants' certificates.

In conventional networks, client nodes can apply on-line certificate status protocol (OCSP) (Myers et al., 1999) to achieve CSI from OCSP responder nodes. The mentioned protocol sends short messages and it is more adaptable to applications of pervasive computing but it needs online connections to OCSP responder nodes which cannot be guaranteed in MANETs.

ADOPT or Ad hoc Distributed OCSP for Trust is one of the OCSP-based certificate validation schemes presented for hybrid MANETs by Papapanagiotou et al. in Daza et al. (2007). This scheme tries to adopt the OCSP protocol to dynamic environment of MANET and by the effective use of CSI caching it is able to deliver CSI even in the offline states to the MANET nodes.

Although, ADOPT and other certificate status validation schemes proposed for hybrid MANETs (Muñoz et al., 2009), suffer from high CSI inconsistency problem which is only solved by periodically refreshing the CSI. But this incurs high overheads to MANET and reduces the scalability of PKI system.

To mitigate these problems, in this paper we present an ADOPT-based certificate validation solution for hybrid MANETs that we call it Enhanced-ADOPT or E-ADOPT. This scheme utilizes a novel kind of CSI called Enhanced CSI (ECSI) which includes not only the OCSP response fields but also contains information about the accusations issued against the certificate. Utilizing security information of ECSI, client nodes participating in the certificate validation process can tune the CSI refresh rate more intelligently. As a result, in comparison with ADOPT, our solution alleviates the CSI inconsistency problem and reduces various overheads of certificate status validations in MANETs. Also, our solution provides better support for offline validations and revocation operations.

To the best of our knowledge, no previously proposed scheme in the literature has used this method and our scheme is the first one that tries to improve the certificate validation by incorporating revocation information in CSI.

The remainder of this paper is organized as follows: Section 2 discusses about the existing certificate status validation protocols for MANETs and Section 3 illustrates our proposed solution to optimize the certificate validation in MANETs and finally Section 4 presents the extensive simulation results and concluding remarks.

2. Related works

The OCSP or Online Certificate Status Protocol (Myers et al., 1999) which is first described in RFC 2560, is a request/reply protocol that enables users to achieve status information of some certificates. Fig. 1 shows the content of OCSP request and response messages. Upon the receiving a request, OCSP Responder returns an OCSP response that consists of a response type which may be good, revoked or unknown. In addition, these digitally signed responses can contain the following items:

- nextUpdate: The time at or before which newer status information will be available.
- producedAt: The time when the OCSP responder signed this OCSP response.

Also, lightweight OCSP is a variant form of basic OCSP protocol which was proposed in Deacon and Hurst (2007) to minimize the validation overheads.

2.1. OCSP-based certificate validation in MANET

Numerous solutions have been proposed to adapt OCSP protocol for MANETs (Berbecaru, 2004; Fongen and Winjum, 2009; Forné et al., 2009; Gañán et al., 2013; Muñoz-Tapia and Forné-Muñoz, 2002; Papapanagiotou et al., 2006, 2007). ADOPT or Ad hoc Distributed OCSP for Trust (Marias et al., 2005a, 2005b; Marias et al., 2006; Papapanagiotou et al., 2010; Masdari et al., 2013) is one the latest schemes that is proposed for hybrid MANET in the literature. This scheme uses server nodes, caching nodes and client nodes. When a client node wants to achieve the status of a certificate, it broadcasts an OCSP request. After a Server node receives this request, it issues the requested CSI. Then caching nodes cache this CSI and send it back to the client.

In Muñoz et al. (2009), Munoz et al. present a novel solution to check CSI in hybrid MANETs and propose a new risk based criterion to evaluate cached CSI. However, they do not specify how the client nodes receive information to compute the risk function.

Caching is one of the main techniques used by all proposed certificate validation solutions in MANET. In the offline states, caching increases the availability of CSI and decreases the overheads of certificate validation process. However, CSI caching produces the CSI inconsistency problem and as the Equation (1) shows, in online states CSI inconsistency is less than OCSP response's validity period:

$$CSI\_Inconsistency \leq ValidityPeriod \tag{1}$$

$$ValidityPeriod = nextUpdate - producedAt \tag{2}$$

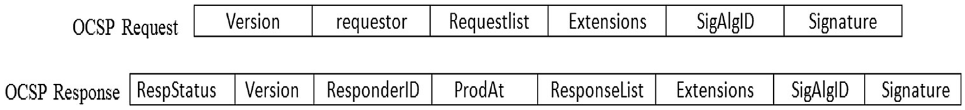

Fig. 1 – OCSP request and response messages.