Available online at www.sciencedirect.com

ScienceDirect

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

Computers & Security

Automated key exchange protocol evaluation in delay tolerant networks

Sofia Anna Menesidou [a], *Dimitrios Vardalis* [a], *Vasilios Katos* [b,*]

[a] *Information Security and Incident Response Unit, Department of Electrical and Computer Engineering, Democritus University of Thrace, University Campus, Xanthi 67100, Greece*

[b] *Department of Computing and Informatics, Bournemouth University, Poole House, Fern Barrow, BH12 5BB, UK*

ARTICLE INFO

Article history:
Received 9 April 2015
Received in revised form 23 October 2015
Accepted 8 February 2016
Available online 17 February 2016

Keywords:
Delay tolerant networks
Protocol evaluation
Opportunistic key management
Protocol injection
ns-2

ABSTRACT

Cryptographic key exchange is considered to be a challenging problem in Delay Tolerant Networks (DTNs) operating in deep space environments. The difficulties and challenges are attributed to the peculiarities and constraints of the harsh communication conditions that DTNs typically operate in, rather than the actual features of the underlying key management cryptographic protocols and solutions. In this paper we propose a framework for evaluation of key exchange protocols in a DTN setting. Our contribution is twofold as the proposed framework can be used as a decision making tool for automated evaluation of various communication scenarios with regards to routing decisions and as part of a method for protocol evaluation in DTNs.

© 2016 Elsevier Ltd. All rights reserved.

1. Introduction

Delay or disruption tolerant networks (DTNs) have increasingly become popular due to certain advantages over traditional protocols such as TCP/IP. DTNs are store-and-forward networks and can be applied in various connectivity-"challenged" networks such as deep space networks, under-water networks, vehicular networks, sensor networks, mobile ad-hoc networks and so forth, where bandwidth is limited and an end-to-end path from source to destination is not always available. Although DTNs by nature may support high availability (which in DTN terminology is referred to as reliability), they are not short of security issues.

Over the past few years, cyber attacks have grown constantly emphasising the need and importance of information security within a network. Security is one of the major issues in deep space networks not only for military, governmental, and commercial missions but also for scientific projects. Cryptographic key exchange and cryptographic key management in general is considered to be a challenging problem in DTN environments. Although there is a wealth of key management protocols in the literature, there is no practical mechanism to evaluate which protocol is more efficient in an environment with limited connectivity and bandwidth. Throughout the literature the emphasis and priorities in cryptographic protocol analysis were placed on the security goals rather than the quality of service and the applicability and feasibility of such protocols. Albeit the evolution, maturity and existence of rigorous and formal tools for assessing the security properties of the plethora of security protocols, many of them may be impractical in a DTN environment. As such, the purpose of this

* *Corresponding author.* Tel.: +4401202966736.
E-mail address: vkatos@bournemouth.ac.uk (V. Katos).
http://dx.doi.org/10.1016/j.cose.2016.02.006
0167-4048/© 2016 Elsevier Ltd. All rights reserved.

paper is to propose a framework for evaluating key agreement protocols in terms of delay and bandwidth constraints. From our simulation results we will also show the impact of the missing credentials (e.g. certificate or session key) on the end-to-end delay of space DTNs. The novelty of this work lies on the area of cryptographic key management in DTNs which is an open and challenging task.

The remainder of this paper is structured as follows. Section 2 provides the literature review and the current state of the art for key management in DTNs. In Section 3 a framework to evaluate cryptographic protocols in such networks is proposed and in Section 4 simulation results are presented. In Section 5 a discussion on opportunistic key management as an idea to minimise end-to-end delay is introduced. Finally, we conclude the paper in Section 6 where open issues, research challenges and future work directions are summarised.

2. Related work and current state of the art

The literature has a relatively long lasting and mature domain of key management. A significant amount of work is published on key management protocols, most of which have been extensively analysed, with well recognised security properties and acknowledged weaknesses. However, when it comes to integrating such protocols in a DTN infrastructure, it seems that the requirements and constraints of a DTN environment render such protocols unsuitable. As such, the prohibiting factors relate to the practical communication, performance and efficiency aspects rather than the security capabilities of the key management protocols. Most of the work done until now is based on the assumption of shared key material (Wood et al., 2009). In Farrell et al. (2009), the author states a series of requirements for key management in DTNs without proposing a solution. Up to date a limited number of approaches for key management in DTN environments can be found in the literature, yet no method for automated practical evaluation of key establishment has been proposed. In fact in RFC6257 (Symington et al., 2011) and in the Internet draft (Birrane, 2013) key management is recognised as a difficult topic and the authors explicitly state that such exclusion is a result of an informed decision. Last but not the least, the relatively new Internet draft proposes and outlines a design for security key management in DTNs (Burleigh, 2015). Specifically, the core requirements and design criteria for DTN security key management are described.

2.1. *Key management in DTNs*

Identity-Based Cryptography (IBC) has been examined as a potential solution for security within DTNs. IBC is a cryptographic method that enables message encryption and signature verification using the public identifier of an entity. The authors in Seth and Keshav (2005) propose an Hierarchical Identity Based Cryptography (HIBC) that provides efficient and practical solutions to secure channels, mutual authentication and revocations in DTNs. In addition, the authors in Asokan et al. (2007) evaluate IBC cryptography in the context of a DTN. In Kate et al. (2007) an anonymous authentication protocol is presented and a secure communication solution based on the non-interactive Sakai–Ohgishi–Kasahara (SOK) key agreement scheme is proposed. This scheme is based on Boneh–Franklin hierarchical identity based encryption (IBC) and signature schemes. However, such IBC solutions appeared to superficially solve the problem (Farrell et al., 2009). Specifically, IBC solutions are undesirable due to intractability of some problems such as Private Key Generation (PKG) parameter distribution, private key revocation, identity name space management and so forth (Lv et al., 2014).

In Edelman et al. (2010) a group-oriented security solution for DTN that provides access control and secure group communications is proposed. The authors suggest a centralised group key management mechanism of the logical key hierarchy (LKH). Group key management in DTN has been studied in Xu et al. (2012). The proposed protocol is based on the Chinese Remainder Theorem. The key lifetime concept is also introduced in order to alleviate the forward security problem in many-to-many DTN communication scenarios. Another work on group key management is found in Zhou et al. (2013), where an automatic group key management scheme based on one-encryption-key multi-decryption-key (OMPK) key protocol for DTNs is proposed. In this work the authors also prove forward and backward security of their protocol.

The author in Van Besien (2010) presents a key distribution scheme for infrastructureless networks, which is based on the Bundle Protocol (BP) and more specifically on the Bundle Security Protocol (BSP). With this dynamic and non-interactive scheme, cryptographic keys for all the BSP mechanisms can be established. The derived keys will be used by the BSP supported algorithms such as HMAC-SHA1 for authentication, RSA for digital signatures, and AES for encryption. However, this work is also based on IBC, which has proved to be impractical for DTNs. The authors in Jia et al. (2012) propose a dynamic virtual digraph (DVD) model for public key distribution. They heuristically define the DVD model by extending traditional graph theory. A public key distribution for pocket DTN based on two-channel cryptography is also presented. The authors in Menesidou and Katos (2012) propose a one-pass key establishment protocol based on an adoption of the Horsters–Michels–Petersen (HMP) protocol. In their method they inject protocol messages in the payload of the BP as part of the message. In addition, an encryption decision making workflow diagram of a custodian node is developed.

More recently, the work in Shikfa et al. (2012) focuses on the problem of key management in the framework of content-based forwarding and opportunistic networks. A specific key management scheme that enables the bootstrapping of local topology is also proposed. In Ding et al. (2013) the authors propose an authentication and key agreement protocol with anonymity based on combined public keys for DTNs. In their solution an on-line third trusted party is not required. In Lv et al. (2014) the authors propose a non-interactive key establishment scheme for BSP. Their work focuses on space DTNs. They utilise a time-evolving mode based on the periodic and predetermined behaviour patterns of space DTNs. From the model, they can schedule when and to whom a node should send his public key.

Download English Version:

https://daneshyari.com/en/article/456412

Download Persian Version:

https://daneshyari.com/article/456412

Daneshyari.com