Journal of Information Security and Applications 000 (2017) 1–10

Contents lists available at ScienceDirect

Journal of Information Security and Applications

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

An efficient provably-secure identity-based authentication scheme using bilinear pairings for Ad hoc network

Libing Wu[a], Jing Wang[a], Kim-Kwang Raymond Choo[b], Yuangang Li[c,d], Debiao He[a,*]

[a] State Key Lab of Software Engineering, Computer School, Wuhan University, Wuhan, China
[b] Department of Information Systems and Cyber Security and Department of Electrical and Computer Engineering, The University of Texas at San Antonio, San Antonio, TX 78249, USA
[c] School of Information Management & Engineering, Shanghai University of Finance and Economics, Shanghai, China
[d] Goldpac Limited, Goldpac Tech Park, Qianshan, Zhuhai, China

ARTICLE INFO

Article history:
Available online xxx

Keywords:
Ad hoc network
Mutual authentication
Non-repudiation
IBE
Bilinear pairings

ABSTRACT

Designing an efficient and secure authentication scheme to ensure secure communication between parties in an ad hoc network remains challenging. Recently in 2017, Shaghayegh and Mehdi proposed an identity-based authentication scheme using bilinear pairings for Ad hoc networks. The scheme is claimed to be secure against a number of known attacks and provides non-repudiation property not found in most other authentication protocols. However, we demonstrate that their scheme is vulnerable to man-in-the-middle and forgery attacks, two previously unknown flaws. We then propose an improved mutual authentication scheme based on identity-based encryption (IBE) for Ad hoc networks. Our security analysis and experimental results demonstrate that the proposed scheme is secure and highly efficient.

1. Introduction

An ad hoc network is a collection of a number of wireless mobile nodes that can communicate with each other directly to exchange messages over a wireless networking environment. Unlike traditional infrastructure networks, an ad hoc network is able to disseminate information without involving a hardware device or software application as a centralized information hub [1–3]. As shown in Fig. 1, when an ad-hoc node is connected to an external access point or a wired network, other nodes can also connect to the external network through that node. In other words, it is infrastructure less, continuously self-configuring and self-organizing. Ad hoc networks can be created on-the-fly and for a particular use, such as military applications (e.g. Internet-of-Military-Things), and natural disasters (e.g. Hurricane Harvey and Hurricane Irma) [4].

With constant advances and increasing popularity of wireless communication technology, ad hoc networks have been deployed in a wide range of applications, such as Internet of Things [5], body area networks (BANs) [6,7] and intelligent transportation [8]. However, due to the characteristics of open link and dynamic topology, ad hoc networks are prone to spoofing, eavesdropping, impersonation and denial-of-service(Dos) attacks [9,10]. Thus, there is a need to ensure that entities (e.g. devices and users) can share and disseminate information securely, such as through the use of (mutual) authentication and key agreement schemes [7,11–13]. Generally, authentication of identity and message resource is the first defense and security protection in most wireless network systems. Existing authentication and key agreement schemes are generally based on public key infrastructure (PKI), which necessitates the need for a certificate authority(CA) to store, issue and manage the digital certificates for each user. Such PKI-based schemes may not scale well, particularly when the number of users increases significantly [14]. Since an ad hoc network is a network formed by a set of wireless mobile hosts, and has no established infrastructure or centralized administration [1,15,16], traditional PKI does not work for ad hoc networks.

Identity-based encryption (IBE) scheme is a potential solution for ad hoc network security, although designing efficient, secure and lightweight schemes suitable for ad hoc network deployment remains challenging. This is the gap we seek to address in this paper.

Design of authentication scheme for ad hoc networks is an ongoing research area. For example, as recent as 2017, Shaghayegh and Mehdi [17] proposed one such authentication scheme. It is claimed that the scheme provides mutual authentication, is secure against known attacks, and achieves high efficiency. In this paper, we demonstrate that this scheme is vulnerable to both man-in-the-middle and forgery attacks (i.e. contribution 1). More importantly,

* Corresponding author.
E-mail addresses: wjuluck@163.com (J. Wang), raymond.choo@fulbrightmail.org (K.-K. Raymond Choo), hedebiao@whu.edu.cn (D. He).

https://doi.org/10.1016/j.jisa.2017.10.003
2214-2126/

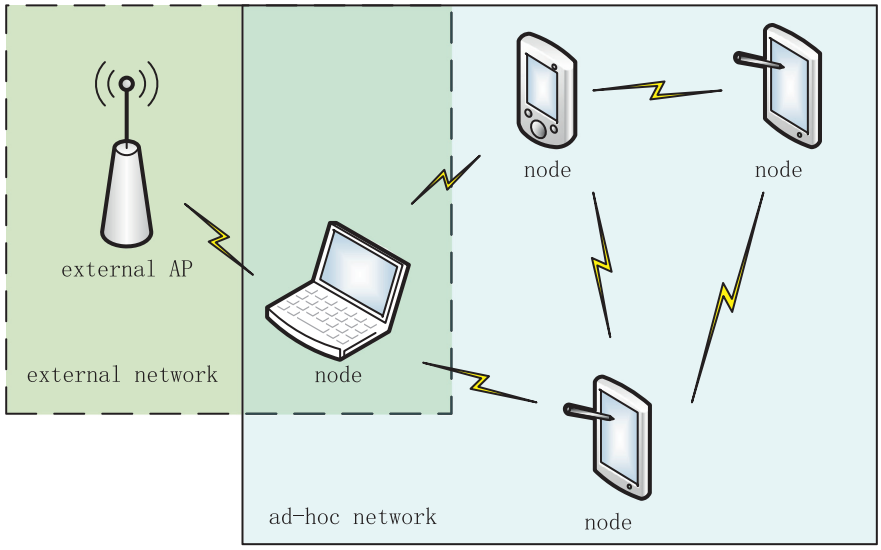

Fig. 1. Networking mode in Ad hoc networks.

we also propose an improved mutual authentication scheme for ad hoc networks, and prove it secure and evaluate its efficiency (i.e. contribution 2).

In the next section, we review related literature and background materials. In Section 3, we revisit and reveal previously unknown flaws in the scheme of Shaghayegh and Mehdi's scheme [17]. We then present an improved protocol, and analyze its security and performance in Sections 4–6. The last section concludes this paper.

2. Related literature and background materials

2.1. Related literature

Identity-based cryptosystem (IBC), first introduced by Shamir [18], is designed to simplify public key and certificate administration. In 2001, Boneh and Franklin presented an improved IBE cryptosystem using bilinear pairings, as well as demonstrating the security of the system [19]. In recent times, there has been a focus to design cryptosystems and schemes that are lightweight and suitable for deployment in settings comprising computationally-constrained devices, such as in Internet of Things and ad hoc networks [20–23], and consumer storage devices [24]. These schemes are generally built using elliptic curve cryptography (ECC) and bilinear pairings [14,25–27], due to their capability to offer short key size and achieve high performance [28,29].

Das et al.[30] presented a remote client authentication protocol using bilinear pairings for smart card application. However, the scheme was later shown to be insecure against forgery attack [31]. Yang and Chang proposed a mutual authentication with key agreement protocol for mobile devices, based on both identity-based cryptosystem and ECC [32]. However, Yoon and Yoo [33] demonstrated that the scheme of Yang and Chang [32] was insecure against a number of attacks (e.g. impersonation attack, replay attack and no perfect forward secrecy), and proposed an improved scheme to mitigate these attacks. A year later, Yoon and Yoo [34] proposed a more efficient authentication scheme for mobile wireless environment based on Wu et al.'s scheme [35]. However, He et al. [36] pointed out that Yoon and Yoo's scheme [33] is still vulnerable to the same attacks affecting the scheme of Yang and Chang. In [37], an identity-based authentication and key agreement scheme for mobile client-server environment is presented. It was also demonstrated that the scheme is more efficient than Yoon and Yoo's scheme [34].

Based on He's scheme [37], Tsai and Lo [38] proposed another authentication scheme for mobile devices. Other schemes include the pairing-based user authentication schemes of Hsu et al.[39] and Luo and Zhao [40]. Although these schemes are provably secure, they are not suitable for ad hoc networks since they are used for client-server environment.

More recently, the authors in [17] pointed out that most of the schemes discussed above neither provide non-repudiation nor digital signature properties. Hence, the authors presented a new authentication scheme for ad hoc networks. In the scheme, digital signature is used to achieve data integrity, non-repudiation and data original authentication. However, we will demonstrate that this scheme is not secure against several security attacks, contrary to the claims.

2.2. Background materials

We will now introduce the relevant background materials.

Let G and G_T respectively denote a cyclic additive group and multiplicative group with the same large prime order q, and P to be a generator of group G. Therefore, a bilinear pairing can be described as $e : G \times G \longrightarrow G_T$ with the following properties:

- **Bilinearity.** Given two arbitrary elements $P, Q \in G$, $e(aP, bQ) = e(abP, Q) = e(P, Q)^{ab}$ holds, where $a, b \in Z_p^*$.
- **Computability.** Given any two elements $P, Q \in G$, there always exists an efficient algorithm to compute the value of $e(P, Q)$.
- **Nondegeneracy.** Given at least one element in G, $e(P, P) \neq 1_{G_T}$ holds.

Next, the following mathematical assumptions that underpin the security of Shaghayegh and Mehdi's scheme [17] and our proposed scheme are introduced.

- **Discrete Logarithm (DL) Assumption.** Given two public elements $P, aP \in G$, there does not exist an efficient algorithm to obtain the value of a, where $a \in Z_p^*$.
- **Computational Diffie-Hellman (CDH) Assumption.** Given three public elements $P, aP, bP \in G$, it is challenging to calculate the value of abP, where $a, b \in Z_p^*$.
- **Bilinear Diffie-Hellman (BDH) Assumption.** Given four public elements $P, aP, bP, cP \in G$, it is challenging to calculate the value of $e(P, P)^{abc}$, where $a, b, c \in Z_p^*$.

Please cite this article as: L. Wu et al., An efficient provably-secure identity-based authentication scheme using bilinear pairings for Ad hoc network, Journal of Information Security and Applications (2017), https://doi.org/10.1016/j.jisa.2017.10.003