要 旨

ワンタイムパスワード認証方式 SAS-2 を適用したネットワーク機器開発

中 原　知 也

インターネットやモバイル通信のブロードバンド化が進み，これらの通信網上で個人が金額情報や個人情報などを扱う機会が増加している．このような通信を安全に行う方法として，SAS-2 等の処理負荷の小さいワンタイムパスワード認証技術を暗号鍵交換に応用した方式が考案されている．SAS-2 を用いた暗号鍵交換方式においては，サーバ-クライアント間の通信経路が遮断されることにより，SAS-2 が保存する認証情報が不一致となる問題が生じる．さらに，提案されている鍵交換方式を次世代ネットワークとして期待されているアドホックネットワークへ適用する際に，簡易かつ安全に新たな通信経路を確立できない問題が指摘されている．

本論文では，この SAS-2 の同期問題を解決し，安全に鍵交換を行える認証方式について提案し，評価を示す．さらに，アドホックネットワークにおいて簡易かつ安全に新規通信経路を確立可能とする認証情報譲渡方式について提案し，評価を示す．最後に，提案方式を適用した機器の開発について述べ，提案方式の適用性を示す．

キーワード　認証，ワンタイムパスワード，SAS-2，同期，鍵交換

Abstract

Development of Network Equipments with One-time Password Authentication Method SAS-2

NAKAHARA, Tomoya

Internet and mobile communications have been developing, and services with personal data and electronic commerce systems have been increasing. An encrypted communication method using a cryptographic-key exchange with one-time password authentication protocol SAS-2 (Simple And Secure password authentication protocol, Ver.2) has been proposed to keep the confidentiality of those data. The method has a problem which authentication information stored in the server and the client is not corresponding when a communication route between the server and the client is broken by unexpected reasons. Another problem with the method is that cannot create a new connection in security on the next generation network, the ad-hoc network.

In this paper, an improved algorithm of the SAS-2 that solves the asynchronous problem and exchanges the cryptographic key safely is proposed. Moreover, an authentication information delivery method that solves the new connection problem on the ad-hoc network is proposed. Finally, I have shown that the high convenient network devices with the proposed method.

key words Authentication, One-time password, SAS-2, Synchronous, Key exchange