要 旨

センサネットワークにおける
ワンタイムパスワードを用いた鍵管理方式

藤原 蓮

近年, IoT(Internet of Things) の実現に向けて無線センサネットワークが注目されている．この無線センサネットワークにおいて効率的に鍵管理を行う手法として LEAP がある．しかし, LEAP は暗号化やネットワーク鍵, クラスタ鍵の配布に使用するペアワイズ鍵の更新処理がない．そこで本稿では, LEAP における鍵確立時の効率性を維持したまま, 暗号鍵の更新をワンタイムパスワード認証を用いて安全に行える手法を提案する．また, 提案方式のベースとなるワンタイムパスワード認証方式 SAS-X(Simple And Secure password authentication protocol version X) をセンサネットワーク向けに拡張する．センサネットワーク向けの拡張として, ノード盗取時における後方秘匿性を保護する仕組みを導入する．性能評価として提案方式のシミュレーションを行い, 鍵更新処理の有無によるノードの平均消費電力量を示した．また, 提案方式についてシステム要件, セキュリティ要件の観点から評価を行った．その結果, 提案方式は一部条件下のもと, システム要件, セキュリティ要件を満たすことを示した．

キーワード　センサネットワーク, ワンタイムパスワード認証

Abstract

Key Management Scheme using a One-Time Password Method for Sensor Networks

Ren FUJIWARA

In recent years, a wireless sensor network attracts attention to realize IoT (Internet of Things). In this wireless sensor network, LEAP is a method for efficient key management. However, LEAP does not update the pairwise key used for encryption, network key, and cluster key distribution. In this paper, we propose a method to securely perform encryption key update using one - time password authentication while maintaining the efficiency of LEAP. In addition, we extend the one-time password authentication system SAS-X (Simple And Secure password authentication protocol version X), which is the base of the proposed scheme, for sensor networks. As an extension for sensor networks, we introduce a mechanism to protect backward confidentiality even when nodes are stolen. We performed simulation of the proposed method for performance evaluation and showed average power consumption of the node due to the presence / absence of key update processing. We also evaluated the proposed method from the viewpoint of system requirements and security requirements. As a result, the proposed method satisfies the system requirements and security requirements under some conditions.

key words Wireless sensor networks, One-time password authentication