Secure Content Exchange in DelayTolerant Networks Using Attribute-Based Encryption

[1]Amang Sudarsono, [1]Sritrusta Sukaridhoto, [2]Toru Nakanishi, and [2]Nobuo Funabiki
[1]Electronic Engineering Polytechnic Institute of Surabaya (EEPIS), Surabaya, Indonesia.
EEPIS Campus, Jalan Raya ITS Sukolilo, Surabaya 60111.
[2]Dept. of Electrical and Communication Engineering, Okayama University.
3-1-1 Tsushimanaka, Okayama 700-8530, Japan.
Email : {amang, dhoto}@eepis-its.edu, {nakanisi, funabiki}@cne.okayama-u.ac.jp

Abstract

The advantage of Delay Tolerant Networks (DTNs) is providing protocols that take into consideration of communication needed for the under constraints of high delays, error rates, inconsistent link connections, and unreliable networks. It is more attractive in the era of ubiquitous connectivity even in the area with such constraints to carry packets from source to destination. As the consequence, there should be many adversaries who may involve themselves in the networks to illegally access the valuable data.In this paper, we propose a secure system in DTN by utilizing Ciphertext-Policy Attribute-Based Encryption (CP-ABE) for controlling access data stored in storage nodes and keeping secret message exchange during maintenance of the routing process. In our system, CP-ABE encrypts data or message so that able to be decrypted only by the authorized nodes whose have a match attribute policy specified in their secret key. Experimental results show that our system is sufficient practical where the time of encryption, decryption and HMAC is less than a second.

Keywords: delay tolerant network, attribute-based encryption, message authentication code, ciphertext-policy.

1. Introduction

Delay Tolerant Network (DTN) [7][8] was designed to provide ubiquitous connectivity even in the difficult accessibility environments whereasthe protocols and applications in widely use on the Internet are not able to applied to such kind of networks, due to long latency/delay and inconsistent or intermittent link connection including in the wireless networks.In case of mobile nodes in some challenging network scenarios, they usually face inconsistent connectivity such as battlefield and disaster network recovery situations. Then, DTN technology is arisefor enabling nodes in such critical situations to establish communication among them with a good feature to allow data destined to be resolved toward until the data is delivered successfully to a or several destination node(s). Moreover, the connection between nodes to carry packets from source to destination in the under constrains of high delays, losses, intermittent link connections and unreliable communications can be established properly by store-and-forward approach in the DTNs [8]. Store-and-forward property enables continuous connectivity whereas packet is moved and stored in the intermediate nodes through the network in order to reach destination nodes ultimately. Hence, many researchers have been taking in account DTNs research topics as one of alternative network connections such as in military operations [9] and mobile environment [11].

In addition, Zhu et. al. [16] summarized the social properties in DTNs through a survey of the recent social-based DTN routing methods. These methods assisted packet forwarding to provide advantages of positive social characteristics such as community and friendship. However, this network also provided negative social characteristics such as selfishness. Commonly, social selfishness in DTNs is involvingmobile communication devices (e.g., smartphones, GPS, etc) [17]. This social property is socially selfish to anybody else but unselfish to friends. This property is very important in the current situation of mobile access and communication, because it provides an access to the network at anytime, anywhere and by everyone even in the condition of inconsistent link connections. Chen et. al. [18] addressed the selfishness by considering trust-based DTN routing to perform trust-related attacks to disrupt DTN operations.

Recently, the use of DTN in the era of ubiquitous connectivity is more attractive to carry packets from source to destination even in the high losses, latency and inconsistent link connectivity. In addition, some applications such as information transfer can be applied in the DTN through storage in the intermediate nodes. In