Mechanism of Authentication Procedure between Ad Hoc Network and Sensor Network

Seungmin Kim, Jisoo Yang, Hankyu Kim, Jung Tae Kim
Mokwon University
E-mail: jtkim3050@mokwon.ac.kr

ABSTRACT

Extending mobile IP to ad hoc networks with the foreign agent acting as the bridge between the wired network and ad hoc networks can provide the global Internet connectivity for ad hoc hosts. The existing research in the area of the integrated wired and ad hoc network is carried out in a non-adversarial setting. This paper analysed an effective solution to solve the security related problems encountered in these integrated networks. This security protocol also excludes malicious nodes from performing the ad hoc network routing. This paper focuses on preventing ad hoc hosts from the attacks of anti-integrity

1. Introduction

Wireless networks, in general, are more vulnerable to security attacks than wired networks, due to the broadcast nature of the transmission medium. Furthermore, wireless sensor networks have an additional vulnerability because nodes are often placed in a hostile or dangerous environment where they are not physically protected. Ad hoc networks have faced huge security lacks. The major problem is providing security services in such infrastructure less networks is how to manage the cryptographic keys that are needs. There are several issues, such as routing, scalability, quality of service and security that need to be solved before implementing these networks in practice. Also each mobile node maintains a fresh certificate table to enforce authentication and integrity in the processing of ad hoc routing to prevent the attacks by using unauthenticated, modified, fabricated or duplicated message [1]. Security is an important issue for ad hoc networks, especially for security-sensitive applications. To secure ad hoc network, we take into consideration following
attributes such as availability, confidentiality, integrity, authentication, and non-repudiation. In Ad hoc Networks, cluster-based routing schemes are used to reduce channel contention in networks with a large number of nodes. Moreover, clustering is also used to form routing backbones to reduce network diameter. Clustering divides a physical network into various overlapping or disjoint virtual sub-networks with fewer nodes in each cluster. Panagiotis Papadimitratos and Zygmunt J. Haas analyzed the problem of secure and fault-tolerant communication in the presence of adversaries across a multi-hop wireless network with frequently changing topology. To effectively cope with arbitrary malicious disruption of data transmissions, they proposed and evaluated the secure message transmission (SMT) protocol and its alternative, the secure single-path (SSP) protocol. They demonstrated that highly reliable communication can be sustained with small delay and small delay variability, even when a substantial portion of the network nodes systematically or intermittently disrupt communication [2].

**III. Conclusion**

In any ad hoc network application, trustworthiness is a primary challenge that should be met in its open and distributed environment. Based on this access control mechanism, malicious nodes can be effectively excluded from ad hoc network so that the trust relationship between ad hoc nodes is enhanced for the security of route.

**References**


**Acknowledgement**

This research was supported by Basic Science Research Program through the National Research Foundation of Korea(NRF) funded by the Ministry of Education, Science and Technology(grant number: 2013-052980)