ABSTRACT—The threat analysis for routing protocol is a significant issue in the ad-hoc network security. In this paper we propose a framework in which the vulnerabilities from the Sybil attack for ad-hoc routing protocol can be modeled in a mathematical approach, and the formal analysis is carried out with a specific proof system under the extended strand space model in order to further verify the validity of the threats from the Sybil attack. As an example, a security route protocol, called endairA, is analyzed in our framework, and the result shows that endairA has the flaw of creating false routes in present of the Sybil attack by utilizing some specific topology leak.

Key Words: the Sybil attack, ad-hoc routing protocol, security formal analysis, strand space