에드 홉 네트워크와 개별 센서 네트워크 간의 인증 절차 메카니즘

김승민, 양지수, 김한규, 김정태
목원대학교

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

요 약

최근에는 이동형 IP로 부터 Ad hoc 통신망으로의 통신 환경의 변화로 말미암아 기존의 유선망과 통합하여 글로벌한 인터넷망을 연결 가능하게 만든다. 기존의 유선망과의 통합 과정은 보안에 취약한 면을 보이고 있다. 따라서 본 논문에서는 통합 통신망에서 발생할 수 있는 보안의 문제점 및 이를 해결하기 위한 방법에 대해서 분석하였다. 이러한 보안적인 요소는 외부의 악의적인 비인가 노드를 배제한다. 따라서 외부로 공격되는 공격이라던지 무결성에서 오는 위협 요소를 방어할 수 있다.

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

키워드

Ad Hoc, Security Protocol, Network Routing, WSN

Ⅰ. 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 analysed 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].

II. Security Requirement in Ad Hoc Networks

The fundamental aspects of network security: confidentiality, integrity, availability, authentication, and non-repudiation are valid for protection of the communication in an ad hoc network. Confidentiality is a security service that provides resistance to the security. Since the mobile nodes within each other's transmission range communicate directly via wireless link, and each node acts as a router to relay the messages, so the confidentiality of routing information is very important for both of the payload data and the routing message headers. Encrypting the transmission messages and the identities of the two communicating nodes in the MANET are the popular methods of providing confidentiality. Integrity guarantees that a transmission message is never corrupted. A message could be corrupted because of being failures, such as radio propagation error, or because of the malicious attacks during the transmission time. Availability ensures that resources or communications are not prevented from each node in the MANET(Mobile ad-hoc networking) needs the routing function or transmission bandwidth by malicious entities. Authentication guarantees all of the routing information and payload data that can be verified the sender who he or she claims to be (sender authentication). Hence, authentication enables each node to verify the identity of the relaying node with which it is communicating. Non-repudiation corresponds to a security method against denial by the origin sender of a message. This method is similar in nature to a signature by the origin writer of a document. Although the security services are the most prominent ones, it should be noted that authorization is sufficient in the application layer instead of a sender authentication that is implemented in the network layer [3].

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

[1] Joydeep Chandra and Lisham Lekhendro Singh, "A Cluster Based Security Model for Mobile Ad Hoc Networks," ICPWC'2005, pp.413-416

[2] Panagiotis Papadimitratos and Zygmunt J. Haas, "Secure Data Communication in Mobile Ad Hoc Networks," IEEE Journal On Selected Areas In Communication, Vol. 24, No. 2, 2006, pp.343-356

[3] Tzu-Chiang Chiang and Yueh-Min Huang, "Group Keys and the Multicast Security in Ad Hoc Networks," Proceedings of the 2003 International Conference on Parallel Processing Workshops (ICPPW'03), pp1530-1536

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)