International Journal of Electronics and Communication Engineering (IJECE)
ISSN(P): 2278-9901; ISSN(E): 2278-991X
Vol. 3, Issue 2, Mar 2014, 49-58
© IASET

DYNAMIC CERTIFICATION AUTHORITY BASED MANETs

VIJENDER SINGH HOODA[1] & AMNINDER KAUR[2]

[1]Research Scholar, Associate Professor, Department of Information & Technology, Dronacharya College of Engineering, Gurgaon, Haryana, India

[2]Associate Professor, Department of Electronics & Communication Engineering, Dronacharya College of Engineering, Gurgaon, Haryana, India

ABSTRACT

Ad hoc network security has been considered as most significant research topic in recent time. Authentication and trust management in an ad hoc network is a challenging task now days. In order to provide security mechanisms that are based on public key technology, it is necessary to create the supporting key management infrastructure, which is commonly uses the concept of a certificate authority (CA). For public key based security services, establishing a CA can be cause of great difficulty without a trusted authority and global centralized and. The exclusive characteristics of mobile ad hoc networks causes a number of nontrivial challenges to design a security architecture such as open network architecture, shared wireless medium, stringent resource constraints and highly dynamic topology in distributes systems. In MANET any node may compromise the packet routing functionality by disrupting the route discovery process. A Distributed Certificate Authority (DCA) is realized through the distribution of the CA’s private key to a number of special shareholding DCA nodes. When CA- related operations are required, such as issuing or signing a certificate, checking public keys, or revoking certificates, a threshold of available shareholding DCA nodes should participate in the operation. There has been relatively slight work to date on designing distributed CA services. This paper proposes a new model for a distributed certificate authority in NTDR (Near-Term Digital Radio cluster-based ad hoc networks. The DCA’s private key is never known by any single node, either during setup or during certificate authority-related operations.

KEYWORDS: Ad-hoc Network, Certificate Authority CA, Distributed Certificate Authority (DCA), Security