Trust Establishment in Ad Hoc and Sensor Networks

Efthimia Aivaloglou, Stefanos Gritzalis, and Charalabos Skianis

Information and Communication Systems Security Laboratory,
Department of Information and Communication Systems Engineering,
University of the Aegean, Samos, Greece
{eaiv,sgritz,cskianis}@aegean.gr

Abstract. Ad hoc and sensor networks highly depend on the distributed cooperation among network nodes. Trust establishment frameworks provide the means for representing, evaluating, maintaining and distributing trust within the network, and serve as the basis for higher level security services. This paper provides a state-of-the-art review of trust establishment frameworks for ad hoc and sensor networks. Certain types of frameworks are identified, such as behavior-based and certificate-based, according to their scope, purpose and admissible types of evidence. Moreover, hierarchical and distributed frameworks are discussed, based on the type of ad hoc and sensor networks they are designed for. The review is complemented by a comparative study built both on criteria specific to each category and on common criteria, grouped into three distinct classes: supported trust characteristics, complexity and requirements, and deployment complexity and flexibility.

Keywords: Trust establishment, trust evaluation, ad hoc networks, sensor networks.

1 Introduction

Mobile ad hoc networks are temporary wireless networks, formed dynamically by a set of mobile nodes without relying on any central infrastructure. Ad hoc networks are characterised by randomly changing topologies, distributed control and cooperative behaviour. Sensor networks, as a special case of ad hoc networks, are composed of inexpensive, small and resource constrained sensor nodes, densely spread over sensing fields. The distributed and dynamic nature of these types of networks are highly desirable properties when considering the design of security solutions for Critical Information Infrastructures (CIIs). CIIs, offering information and communication services which are significantly affecting quality of life, safety, and economic activities, may thus include ad hoc and sensor network technologies not only for the provision of context-rich services, but also for their protection in crisis situations.

The design of secure ad hoc and sensor networks is an active research area. Securing ad hoc and sensor networks generally entails ensuring the confidentiality

J. Lopez (Ed.): CRITIS 2006, LNCS 4347, pp. 179–194, 2006.

and integrity of the data communicated, providing the means for node authentication and access control, along with lower level security issues like secure routing and node grouping. However, several works (e.g., [1,2,3,4]) argue that the conventional view of security does not suffice provided the unique characteristics of ad hoc networks, that are susceptible to a variety of node misbehaviours. From compromised nodes acting as internal attackers to legitimate nodes that act selfishly or maliciously, internal misbehaving nodes are a vulnerability that can not be tackled using authentication and cryptography alone. This vulnerability, along with the cooperative nature of ad hoc and sensor networks, rise the necessity for assessing the trust relationships among the network nodes. The trust relationships established between network nodes could be used for the provision of higher level security solutions, such as trusted key exchange or secure routing. However, the trust evaluation requirements and challenges posed by ad hoc networks are substantially different from the case of traditional wired networks. The existence of trusted third parties used as intermediaries for establishing trust relationships cannot be taken for granted, trust relationships change frequently due to the dynamic topology, while trust evaluation may be based on uncertain and incomplete evidence due to connectivity problems. To tackle the aforementioned new challenges, trust establishment frameworks have been proposed for representing, evaluating, maintaining and distributing trust among ad hoc network nodes.

The rest of the paper is organised as follows: Section 2 discusses the notion of trust in ad hoc and sensor networks and the challenges and requirements related to trust establishment. Section 3 presents a selection of the trust establishment frameworks, separated into two categories according to their scope and purpose, and compared according to criteria specific to each category. Section 4 contains the comparative evaluation on issues that are common for all frameworks presented, and discusses issues related to the applicability on sensor networks. Finally, Section 5 concludes the paper and suggests future directions.

2 The Notion of Trust in Ad Hoc Networks

The notion of trust, as used in different research areas like trusted computing, trusted platforms, trusted code and trust management, has received various interpretations [5]. Throughout this work, we study the in-network trust relationships that can exist between network entities. We use the notion of trust as "The quantified belief by a trustor with respect to the competence, honesty, security and dependability of a trustee within a specified context" [6]. A trust relationship is established by two parties, the trustor and the trustee, also referred to in this work as the trust issuer and the target. The *trust establishment* process includes the specification of valid types of evidence, and its generation, distribution, collection and evaluation [7].

Trust evidence, which form the basis for establishing trust relations, may be uncertain, incomplete, stable and long-term [8]. *Trust evaluation* is performed by applying context-specific rules, metrics and policies on the trust evidence. The