Chapter 30
Security in Ad Hoc Network and Computing Paradigms

Poonam Saini
PEC University of Technology, India

Awadhesh Kumar Singh
National Institute of Technology Kurukshetra, India

ABSTRACT

Resource sharing is the most attractive feature of distributed computing. Information is also a kind of resource. The portable computing devices and wireless networks are playing a dominant role in enhancing the information sharing and thus in the advent of many new variants of distributed computing viz. ubiquitous, grid, cloud, pervasive and mobile. However, the open and distributed nature of Mobile Ad Hoc Networks (MANETs), Vehicular Ad Hoc Networks (VANETs) and cloud computing systems, pose a threat to information that may be coupled from one user (or program) to another. The chapter illustrates the general characteristics of ad hoc networks and computing models that make obligatory to design secure protocols in such environments. Further, we present a generic classification of various threats and attacks. In the end, we describe the security in MANETs, VANETs and cloud computing. The chapter concludes with a description of tools that are popularly used to analyze and access the performance of various security protocols.

INTRODUCTION

The ad hoc network is a collection of wireless mobile nodes that dynamically self-organize in arbitrary and transient network topologies (Macker & Corsen, 1998; Weiser, 1999; Prasant, 2005). The nodes[1] can thus be internetworked in areas without a pre-existing communication infrastructure or when the use of such infrastructure requires wireless extension. The ad hoc networks and computing models have the following typical features (Chlamtac, Conti & Liu, 2003; Basagni, Conti, Giordano & Stojmenovic, 2003; Macker & Corson, 2003; Corson, Maker & Cernicione 1999):

DOI: 10.4018/978-1-5225-8176-5.ch030

Copyright © 2019, IGI Global. Copying or distributing in print or electronic forms without written permission of IGI Global is prohibited.

- **Continually Changing Topology and Membership:** Nodes continuously move in and out of the radio range of other nodes in the network, thereby, frequently reconfiguring the membership information to update the nodes.
- **Unreliable Wireless Links:** Due to high mobility and dynamic nature of ad hoc protocols, the links between nodes in such networks are inconsistent. Therefore, the susceptibility to active/passive link attacks increase.
- **Lack of Security Features and Poor Scalability of Security Mechanisms:** The security features implemented in statically configured protocols are not sufficient to take care of the requirements of an ad hoc environment. Moreover, with the growth of scalable networks, the security mechanism must be scalable too. Also, the physical protection of mobile hosts is generally poor.
- **Aggregation of Data on Cloud:** Clouds have the capability to aggregate private and sensitive information about users in diverse data centers. Hence, the isolation and protection of customer data is an important concern.
- **Browser Security Failures:** As the cloud users and administrators rely heavily on Web browsers, the browser security failures can lead to cloud security breaches.
- **Transparency:** Customers need confidence and transparency about the performance of the cloud system and its management strategy.

Because of features listed above, ad hoc networks and computing paradigms are more vulnerable to security attacks as compared to traditional networks. Hence, security and privacy becomes necessary to safeguard the leakage of information in such hostile environment.

SECURITY ATTACKS: A BACKGROUND

There are many types of security attacks in an ad hoc and computing environment (Karpijoki, 2000; Lundberg, 2000; Hubaux, Buttyan & Capkun, 2001; Buttyan & Hubaux, 2002; Deng, Li & Agrawal, 2002; Ilyas, 2003). Primarily, the attacks can be categorized as following:

1. **Internal vs. External:** Internal attacks initiated by the authorized nodes into the network. The network itself may contain compromised or arbitrary behaving nodes. On the other hand, external attacks are initiated by the adversaries, initially not a part of network, to cause delay in network services, congestion and disrupt other network related operations.
2. **Passive vs. Active:** Passive attacks include eavesdropping on or monitoring packets exchanged within an ad hoc network whereas active attacks involve some modifications of the data steam or the creation of a false stream.
3. **Malicious vs. Rational:** Usually, a malicious attacker aims to harm the users or network. Hence, a malicious attacker may employ any means of forging without considering loss and consequences involved. On the other hand, a rational attacker looks for personal benefit and hence is more predictable.
4. **Local vs. Extended:** Though, an attacker may control several entities, it can be limited in scope and hence its affect remains local. An extended attacker controls several entities that are scattered across the network, thus extending the scope. This distinction is especially important in privacy-violating and wormhole attacks that will be described shortly.

27 more pages are available in the full version of this document, which may be purchased using the "Add to Cart" button on the publisher's webpage:
www.igi-global.com/chapter/security-in-ad-hoc-network-and-computing-paradigms/224596

Related Content

Designing Instruction and Professional Development to Support Augmented Reality Activities
Kelly M. Torresand Aubrey Statti (2021). *International Journal of Fog Computing (pp. 18-36).*
www.irma-international.org/article/designing-instruction-and-professional-development-to-support-augmented-reality-activities/284862

Predictive Modeling for Imbalanced Big Data in SAS Enterprise Miner and R
Son Nguyen, Alan Olinsky, John Quinnand Phyllis Schumacher (2018). *International Journal of Fog Computing (pp. 83-108).*
www.irma-international.org/article/predictive-modeling-for-imbalanced-big-data-in-sas-enterprise-miner-and-r/210567

Data Recovery Strategies for Cloud Environments
Theodoros Spyridopoulosand Vasilios Katos (2015). *Cloud Technology: Concepts, Methodologies, Tools, and Applications (pp. 377-391).*
www.irma-international.org/chapter/data-recovery-strategies-for-cloud-environments/119863

An Evolutionary Approach for Load Balancing in Cloud Computing
Subashis Mohapatraand Banshidhar Majhi (2015). *Handbook of Research on Securing Cloud-Based Databases with Biometric Applications (pp. 433-463).*
www.irma-international.org/chapter/an-evolutionary-approach-for-load-balancing-in-cloud-computing/119355

Chemometrics: From Data Preprocessing to Fog Computing
Gerard G. Dumancas, Ghalib Bello, Jeff Hughes, Renita Murimi, Lakshmi Viswanath, Casey O. Orndorff, Glenda Fe G. Dumancas, Jacy O'Dell, Prakash Ghimireand Catherine Setijadi (2019). *International Journal of Fog Computing (pp. 1-42).*
www.irma-international.org/article/chemometrics/219359