

Security within Ad hoc Networks

Position Paper, PAMPAS Workshop, Sept. 16/17 2002, London

Author: Preetida Vinayakray-Jani

preetida.vinayakray-jani@nokia.com

Nokia Research Center, Helsinki, Finland

1. WHAT IS AD HOC NETWORK?

With the advancement in radio technologies like Bluetooth, IEEE 802.11 or Hiperlan, a new concept of networking has emerged. This is known as ad hoc networking where potential mobile users arrive within the common perimeter of radio link and participate in setting up the network topology for communication. Nodes within ad hoc are mobile and they communicate with each other within radio range through direct wireless links or multihop routing.

2. LACK OF SECURITY WITHIN AD HOC NETWORK

The build up of ad hoc network can be envisaged where support of wireless access or wired backbone is not feasible. Ad hoc wireless network does not have any predefined infrastructure and all network services are configured and created on the fly. Thus it is obvious that with lack of infrastructural support and susceptible wireless link attacks, security in ad hoc network becomes inherent weakness. Achieving security within ad hoc networking is challenging due to following reasons [2]:

- Dynamic Topologies and Membership
 - A network topology of ad hoc network is very dynamic as mobility of nodes or membership of nodes is very random and rapid. This emphasizes the need for secure solutions to be dynamic
- Vulnerable wireless link
 - Passive/Active link attacks like eavesdropping, spoofing, denial of service, masquerading, impersonation are possible
- Roaming in dangerous environment
 - Any malicious node or misbehaving node can create hostile attack or deprive all other nodes from providing any service

Nodes within nomadic environment with access to common radio link can easily participate to set up ad hoc infrastructure. But the secure communication among nodes requires the secure communication link to communicate. Before establishing secure communication link the node should be capable enough to identify another node. As a result node needs to provide his/her identity as well as associated credentials to another node. However delivered identity and credentials need to be authenticated and protected so that authenticity and integrity of delivered identity and credentials cannot be questioned by receiver node. Every node wants to be sure that delivered identity and credentials to recipient nodes are not compromised. Therefore it is essential to provide *security architecture* to secure ad hoc networking.

The above mentioned *identification* problem simultaneously leads to *privacy* problem. In general mobile node uses various types of identities and that varies from link level to user/application level. Also in mobile environment very frequent mobile node is not ready to reveal his/her identity or credentials to another mobile node from privacy point of view. Any compromised identity leads attacker to create privacy threat to user device. Unfortunately the current mobile standards [3] do not provide any location privacy and in many cases revealing identity is inevitable to generate communication link. Hence a seamless privacy protection is required to harness the usage of ad hoc networking.

3. KEY ISSUES AND CHALLENGES

3.1 Link Level Security

In wireless environment the links are susceptible to attacks where eavesdropper can easily spoof the on going communication. As there is no protection like firewalls or access control in ad hoc network any node can become vulnerable to attacks coming from any direction or from any node. The results of such attacks include spoofing of the node's identity, tampering with node's credentials, leaking of confidential information or impersonating node. These types of attacks can easily compromise the basic security aspects like confidentiality, integrity, and availability and privacy of the node.

3.2 Secure Routing

The supported routing protocols within ad hoc network are more vulnerable to attacks as each device acts as a relay [1]. Any tampering with routing information can compromise whole network. An attacker can insert rogue information within routing information or introduce denial of service type attack by replaying old logged or stored information. Also compromised node can route malicious information to other nodes, which can cause serious damage. However proposed routing solutions are capable to operate with dynamic topology but in terms of security measure they provide partial or no solution [2]. Thus implementation of secure routing protocol is one of the challenges within ad hoc network.

3.3 Key Management

In general, security goals in ad hoc networks are achieved through cryptographic mechanisms such as public key encryption or digital signature. These mechanisms are supported through centralized key management where trusted Certificate Authority (CA) provides public key certificate to mobile nodes so nodes can develop mutual trust between one another. Any tampering with CA can easily compromise the security of the entire network.

The proposed mechanisms used for identification such as shared secret, public key cryptography, third party authentication provide partial solution, as they are vulnerable or unable to scale. All proposed solutions require that the mobile users make proper usage of cryptographic keys. However goal of proper management and safekeeping of small number of cryptographic keys is difficult to achieve in ad hoc network due to random mobility of nodes where continuous connectivity is not maintained [1].

3.4 Privacy

Spoofing of identity or any confidential information leads to privacy threats and later on that can be engineered to create DoS attacks. Thus privacy is one of the key issues within ad hoc networking.

4. CONCLUSION

In this paper, security relevant issues within ad hoc networks are identified. A brief introduction about key issues and challenges provides the decomposition of whole security issue within ad hoc networking. Significant usages of ad hoc network leverage on the well-defined security architecture, where security aspects like confidentiality, Integrity and availability, privacy are addressed properly.

REFERENCES

- [1] Jean-Pierre Hubaux, Levente Buttyan and Srdan Capkun, "The Quest for Security in Mobile Ad hoc Networks", Proceedings of the ACM Symposium on Mobile Ad hoc Networking and Computing, MobiHOC 2001
- [2] L. Zhou and Z.J. Haas, "Securing Ad hoc Networks", IEEE Networks, 13(6): 24-30, Nov/Dec 1999
- [3] 3GPP, "3G Security: Security Architecture", 3GPP TS 33.102, V3.6.0, Oct. 2000