# Security Model for Ad Hoc Networks

Y.R.Venturini; C.M.Schweitzer;L.A.Martucci; F.F.Redigolo; A.W.Mittelsdorf; W.V.Ruggiero and T.C.M.B.Carvalho

Computer Engineering and Digital Systems Department
Universidade de São Paulo
São Paulo - SP - Brazil

*Abstract: several new applications and the new emerging technologies that make ad hoc networking possible are pushing the development of ad hoc networks. Securing the ad hoc environment is essential for the success of these new applications as well as for the entire future of ad hoc networking. Several ad hoc security aspects, like trust management and routing concerns were approached in the last few years, but no comprehensive security models for ad hoc environments discussed. This paper presents a security model for wireless service-based ad hoc networks.*

*Keywords*: security, wireless; ad hoc networks

## 1 Ad Hoc Networks and Security

An ad hoc network is defined as a set of mobile nodes or platforms that can move arbitrarily in a temporary infrastructure and establish an ephemera network without the presence of a central entity, using a wireless interface to switch packets. The nodes in this network type can acts like a host (running users applications) or like a router (switching packets to another nodes, extending the network reach) [4][6][7].

The same reasons that allow us to create, almost instantaneously, a wireless ad hoc network, also bring the challenge of controlling and insuring the system security required for the applications and services using such communication infrastructure [5]. The main contribution of this paper is a security model with all the basic requirements to develop secure applications and services in ad hoc network environments.

The rest of this paper is organized as follows. Section 2 is related to the ad hoc environment assumptions where the security aspects for the ad hoc network are presented. The security model for ad hoc networks based in services is defined and discussed in section 3. The conclusion, in section 4, summarizes the work.

## 2 Ad Hoc Security Aspects

Wireless communication has several characteristics that differ from traditional wired environments; most of them are related to the nature of the communication itself. Wireless communication signals spread through the environment in contrast to wired communication, where signal is confined in copper or optical fiber. Besides, one of the greatest advantages of wireless systems, the node mobility, can lead to severe security issues [9].

It's important to understand that wireless communication can cause impact not only to the physical, data link and network layers of the OSI model. Although the methods of cryptography deployed in wired network can also be applied in wireless network, sometimes they are not appropriated. For example, the wireless networks has upper error rate and blocs cryptography mechanisms can be more appropriate than stream cryptography mechanisms, for this problem

### 2.1 Physical Transmission

In wired networks precautions to avoid that unauthorized users have access to the network are usually taken:

- The devices are physically protected from unauthorized access and the cabling is protected against eavesdropping.
- Firewalls are installed to avoid unauthorized hosts to access controlled services.
- Network access points can be security strongholds.

It is not possible to avoid unauthorized devices to reach the wireless network area. Any device within reach of radio-frequency signals can get access to data being transmitted, as well as to transmit data to devices. Interruption and interception attacks are easier to perform in wireless networks than on traditional, wired

networks. To avoid this kind of attacks, implementation of services capable of assuring the availability of connection and confidentiality of information are required.

The physical mechanism usually deployed is the spread spectrum technique with low power transmission [1][2][3]. This technique increases the difficulty for signal interruption (e.g., a jamming attack) as well as signal interception (avoiding eavesdropping attacks).[8]

### 2.2 Unauthorized Access

Some characteristics in ad hoc networks may require different security solutions. Private or public network require different levels of security and the solutions can also be different.

#### 2.2.1 Private Network

In a private network, the devices with authorized connection are known and controlled. These networks are usually created to serve a limited group of users and devices, such as business networks, domestic networks, domestic automation networks, network created for conferences or meetings outside the business networking environment or even wireless access provider to the Internet.

In these networks just authorized devices should have access to network, but in wireless network this control is not so simple. In order to controls the communication and avoid intruders, the devices first need to authenticate each other. Device authentication may not be enough to control access to the network.

Other usual question in these networks is the confidentiality of data being transmitted. The use of cryptography is necessary to critical data transmission because it is not possible to avoid an intruder to capture the signal being transmitted on the air.

#### 2.2.2 Public Network

The public access network provides services that can be accessed by unknown devices. This network is usually created to itinerant users. Some examples: Information services offered, for example, in an airport; or a temporary network with access point to Internet created in events.

This kind of network may or may not require device and users authentication. Equally, the data transmitted can be confidential or not. Usually the need of authentication and cryptography depends on the service.

In this case, users and devices are unknown, which makes encryption and authentication mechanisms harder to be deployed, if not impossible. The use of public and private key scheme can offer authentication in the application level.

## 3 Security Model for a Service-based Ad Hoc Networks

In a service network, services offers and requests interact through the communication infrastructure. The wireless ad hoc network communication infrastructure is composed by wireless devices, which communicate among themselves in a dynamic fashion and without any fixed infrastructure.

The security model, of this work, has the purpose of build a services based ad hoc network, which the services interactions can run in a secure way.

### 3.1 Services Networks

A services network is formed by communication infrastructure and by entities set that participate in the process of service offer and request.

#### 3.1.1 Entities

The entities can also be classified accordingly to their physical or logical nature, which interact each other in the services request and running process. *Physical entities* are equipment with the most diverse complexities. The simplest devices may have only one function, such as air-conditioners, microwaves, etc. The more sophisticated ones offer multiple services, such as wireless phones with PBX functions, answering machines and Internet access; computers that communicate with wireless devices, among others.

*Logical entities* must be hosted by physical entities to exist. Logical entities are the processes that run in servers or access devices, including the processes that interact with users.

The entities that compose this network can be classified in *users, service providers* (also called services) and *devices*. All entities can be engaged in an identification process; this is an important issue when it is crucial to protect the network against non-legitimate entities.

- *Users*: The users are logical entities that request services to the network services providers. Users are the entities that use the network services and are capable of identification.
- *Services Providers*: The service providers are logical entities with capacity,

functionality and availability to answer the service requests presented to them. The service capacity corresponds to the intensity that a service can be provided. The amplitude of this capacity is related to the amount of resources allocated or associated to the service. The functionality is related to the ability to provide, supply or perform a set of functions and the service availability is related to the periods of time that the device is able to perform its functionality services. A service provider may request services to another entities and may also be identified

- *Devices*: The devices are physical entities capable of supporting (hosting) services and users. The devices commonly offer user interfaces, such as displays, keyboards, microphones and touch screens. These devices have physical addresses and may be identified.

Considering the dynamic behavior of the entities, they may be *present* or *absent*, depending of the position in the network reach-radius and their power status (on/off).

Devices can also be classified as *permanent* or *guest*. Permanent devices are those who have durable privileges in the ad hoc network context. An initial configuration process defines those privileges. Guest devices are those who come in the network radius, are capable of communicating with it and do not have durable privileges. The guests can be classified as unidentified, until they are not submitted to an identification process, and identified when they gone through a positive identification process. The guests that gone through an identification process can assume generic identities (anonymous) or specific ones (identified guests).

### 3.1.2 Communication Infrastructure

The communication infrastructure provides the data exchange between entities in a transparent manner. No particular technology is required for the service network; however, ad hoc networks will be assumed in this document.

## 3.2 Authentication and Authorization

Before a service or function can be used by an entity, a verification of proper permissions for this access may be performed. In the first place, the entity is identified, to check if it is who it claims to be. This process is called *authentication* (or identification). Later, there is a service use permission verification. This process is called *authorization.*

The entities are classified in the network as a result of an initial authentication process called registration. This classification depends on pre-established configurations and can trigger the emission of one or more certificates that indirectly define the entity's rights.

*Actions* are entities' individual initiatives, taking the form of requests or responses. Generally, access devices perform service requests and receive responses. Devices that host service providers perform actions that process service requests, returning responses (and/or results).

*Permissions* are the rights to perform actions. Permissions can have different granularities. Service permissions define the rights to use a service as a whole, while function (or operation) permissions define rights to act on specific functions of the service.

An efficient mapping between services and entities is necessary for permission control and verification. A direct mapping between services and entities may become unpractical in networks with more than a few users or with complex services. The current proposed model use groups and profiles.

*Groups* are sets of entities. Groups are created based on common entity characteristics or purposes.

*Profiles* define a set of permissions, which can be relative to devices, services or functions. The profiles form a convenient way to group permissions, and later be mapped to groups of entities.

*Access rights* are defined as the relationship that establishes the right of an entity to perform a given action. In a practical way, access rights are defined and may be verified through the mapping between users, groups, profiles and actions.

$$\text{Entity} \Leftrightarrow \text{Group} \Leftrightarrow \text{Profile} \Leftrightarrow \text{Action}$$

The *action-radius* of an entity is defined by all the actions it has rights to execute, thus it is derived from the union of all the actions which it has access rights.

The access rights that a service network assigns to an entity are proportional to the trust level that this network has about the entity. The trust level indicates how much the service network trusts a particular entity. The trust level can be changed as result of administrator

intervention (new device introduction into the network), promotion, demotion, suspect behavior or banishment. Finally, the trust level can be automatically changed through authentication, as when an entity passes from the non-identified to identified state.

The authentication of an entity go through several steps. The public services network may not require authentication, while critical services, such as document signing or commercial transactions being executed through home devices may require multiple identification levels. The service may require the appropriate identifications by its own criteria, and in the order and quantity desired, allowing great flexibility and increasing security. Several types of identification may be supported, such as passwords, tokens, certificates and biometrics.

After session establishment, where mutual device identification is required, extra identification requests may be optionally exchanged. The mutual initial identification exchanges the minimal amount of necessary information, to not compromise entities' privacy. Depending of the response, new requests may be generated as well as messages granting or denying the identification presented to execute an appropriate action.

### 3.3 Registration Service

The registration service objective is register new entities on the service-based network (i.e., initially authenticating them on the network), issuing signed digital certificates to them. These certificates should be presented by user entities on each service request with authentication purpose; if the certificate is authentic and valid, the service provider uses it to verify the access rights related to the identified end user.

In order to use the lookup service (which belongs to the basic infrastructure of a service-based network, and contains a list of the available services) as well as the general services, an entity must identify itself using the certificates issued by the device hosting the registration service, called the registration authority.

The registration service and the lookup service could be associated, but they do not necessarily coexist in the same device. Both services are essential to the network, but they do not need to be available at all times.

The registration service is mandatory to the security model, and like all services in an ad hoc network it is not fixed on a device and can exist in any capable, permanent and previously identified (or announced) network device. These devices could be in a list of the possible registration authorities.

The registration authorities control a mobile database of registered entities, called the registry. It should be distributed and shared among the permanent devices capable of being a registration authority. Service providers have to accept certificates signed from any registration authority.

An entry in the registry is indexed through a unique identifier associated to each entity (e.g., a combination of the physical device address and a PIN, for devices). It includes entities' certification information (e.g., an entity's public key) and, for devices, information regarding the class they belong to (permanent or identified guest).

When devices register in the registration service, they are classified as anonymous guests, identified guests or permanents. The registration service classifies the devices based on pre-configured list of devices that should belong to a specific class (e.g., the list of permanent devices) as well as on rules for automatic classification (i.e., if a device fulfills some requirements, it may be automatically classified and registered).

After a period of time away from its permanent (home) network, a device should be capable of recognizing its home network through its registry's logical id. This logical id should be changed periodically, following a pseudo-random sequence generated from a seed distributed to permanent devices. If the seed's secrecy is compromised, the same could be changed by the active registration service and propagated through the ad hoc network. Devices out of the permanent network range will have to be submitted to a new registry. This method guarantees the user privacy, avoiding device tracing, and the service network privacy, avoiding identification to a non-authorized user.

The registration service also has a certification revocation list. This list contains the revoked certificates, and each revoked certificate should be at this list until the certification expiration.

A service provider may also issue special signed digital certificates, independently from a central registration authority. In this case, these certificates authenticate the entities only to the services hosted by the issuer service provider, which becomes a special instance of a registration authority restricted to specific services. When combined with trust distribution mechanisms, a set of such special registration authorities may take the role of a central registration authority.

### 3.4 Application Security

Many devices, such as notebooks or handheld computers, support the installation, configuration and execution of applications. These activities have a potential security risk; since they may allow execution of malicious code, permit virus proliferation and compromise privacy, among others.

In order to protect against potentially unsafe activities, a security model similar to the Java security model version 2 is proposed, which should:

- Be safe against malicious applications: it is necessary to prevent programs from damaging its computational environment. Viruses and Trojan horses are examples of such programs;
- Protect against intrusive programs: it is necessary to avoid that private information in the host device are accessed or disclosed by the programs;
- Support authentication: the author and user identity of the program should be verified;
- Use cryptography: all data in transit, i.e., sent or received to/from the network or storage devices (e.g., hard disks and databases), should be encrypted;
- Support audits: all potentially sensitive operations should be logged;
- Be capable of verification: rules of operation should be established and adherence to them must be verifiable;

A virus is not a device's recognized application, since it does not own a valid digital signature (unless the system is configured to do so), and it is prevented from executing. When an application needs more privileges, it must be a proper member of a higher privileged group, or an authorized user must modify the system permissions.

### 3.5 Dynamic Behavior

When the dynamic process of inserting a device in an ad hoc network environment is treated, It is necessary to consider the device behavor in this environment. As previously seen, when devices register in the network, they are classified as anonymous guests, identified guests or permanents entities. Figure 1 shows the finite state machine related to the device behavior.

When a device accesses the network, it enters in an initial state (Init), under an unidentified guest status. If it successfully registers with the registration service, it becomes a network member, and moves to an active state dependant on the classification it receives from the registration service (Permanent, Identified Guest or Anonymous Guest). It remains on the initial state while it does not successfully register and if it is powered off or leaves the network environment, it leaves the initial state and goes to an inactive state.

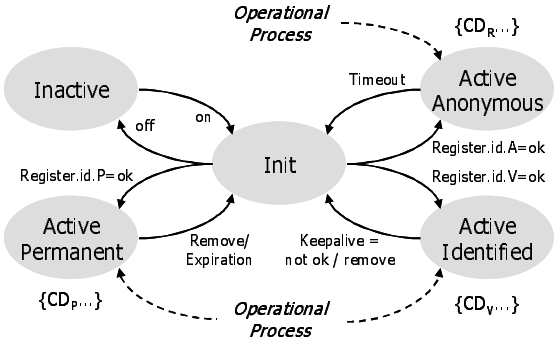


Figure 1 - Device Access State Machine

If the device is registered as a permanent device (Register.id.P=ok), it means it has enduring privileges on the network. It leaves the permanent state when its certificate expires (expiration) or is revoked (i.e., it is removed from the list of permanent devices). When a short-lived is granted an anonymous guest certificate (Register.id.A=ok), the device has pre-defined time to access network public services (those which do not need an identification), returning to the to initial state when it times out. And last, if the device is an identified guest, it can access any network public service and guest specific services (Register.id.V=ok. It returns to the initial state when it is removed, its certificate expires or it is no longer active (keepalive=not ok). When a device is in one of the active states, it is

necessary to consider its behavior when a service is requested, as shown in Figure 2.

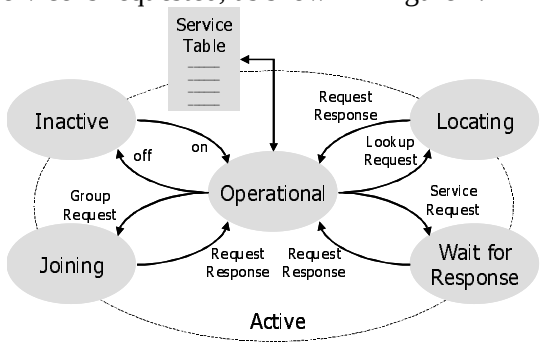


Figure 2 - Finite-state machine of service access

In the moment that the device is in an active state (operational), it can request a service location (locating), a service itself (wait for response) or request a group registration to join additional groups and gain additional privileges. A request response indicates whether or not the request was successful.

Before using a service, a device needs to find it. Through the service location protocol, it requests a service location, going to the "Locating" state. It returns to the active state after receiving the answer. When a device is in the active state as an anonymous guest, it can only locate public services

When it requests a service, it enters the "Wait for Response" state and exits this state when it receives the response of the service provider.

### 3.6 Security Mechanisms

The security model encompasses several security mechanisms, which are used by the entities to interact among themselves in a secure way.

*Network Discovery*: An entity may belong to different networks (e.g. a home network and a corporate network). Before accessing a service, the entity must discover in which network it is presently in (by the registry id, for example), and select the appropriate certificates and credentials for the network services. This task is under responsibility of the network discovery mechanism.

*Individual Registration***:** In order to access a service in a network, an entity needs to go through an individual registration process: any new entity in the network should register itself in the registration service. The registration service, according to its configuration, provides a special certificate, called an individual certificate, to the registering entity. The individual certificate is valid for that specific network and it correctly identifies the entity to the services in the network.

*Group Registration*: As previously seen, the entities may belong to one or more groups and, depending on which groups it belongs, the request of service operations may be allowed or denied. In order to join a group, the entity must execute a group registration process: it registers itself to specific groups in the registration service. As a result of the group registration, the entity receives group membership credentials, which shall be used to prove to services which groups it belongs to.

*Registration Service Configuration*: In order for entities to successfully register and receive individual and group certificates, the registration service must be configured. The registration service configuration mechanism is responsible for defining the rules that should be used in the registration process in order to issue permanent, identified guest or anonymous guest individual certificates.

*Service Setup*: Each service must be configured in order to securely communicate. This mechanism is responsible for the configuration of security parameters in a service, such as the access rights related to groups, individual entities and operation profiles as well as the security requirements for the service. All configurations must be signed, for auditing purposes. It is possible that services issue special certificates, to identify entities that are allowed access to its functions independently from the registration authority. These certificates are managed through the service setup.

*Authentication***:** A key mechanism in the security infrastructure is the identification of entities, such as users, devices or services. This identification is possible with the individual certificates, which are issued and signed by the registration authority. To identify itself in a network, an entity presents its individual certificate, issued by the registration authority of that network, to another entity.

*Session Setup*: When an entity wants to communicate with a service provider, it must setup a session between them. A session must provide an encrypted tunnel for communication in the wireless medium, in order to assure the confidentiality and integrity needed for the secure communication. During the session

establishment, there is the authentication phase, where the entity proves its identity to the service provider and vice-versa (if necessary). Once the session is established, the entity may request the service operations desired and, depending on the service configuration, the entity may need to provide additional group membership credentials to have a specific operation allowed.

*Logging*: The network may provide a logging service for non-repudiation and auditing. There must be logging for key security operations, such as individual and group registration and service registration configuration.

*Certificate and Credential Revocation*: When groups or entities are removed from the network, the individual certificates and group credentials must be revoked. The revocation mechanism is responsible for maintaining and advertising the list of certificates and credentials revoked. It allows to security-tight services a way of instantly verifying if credentials and certificates are still valid as well as allows that services periodically receive this list.

*Content Filtering*: The content filtering mechanism is responsible for checking that viruses and other malicious code do not enter a device and corrupt services.

*Runtime Checking*: The processes that implement the services must be executed in a restricted environment, with signed and unsigned code having different restrictions. If malicious code bypass the content filtering mechanism, the runtime checking mechanism must detect new, non-registered services that may appear as a consequence, as well as detecting that a running process has been tampered. Also, if a service tries to interact with other services or the underlying device in a disallowed or unexpected way, the runtime checking must detect and interfere, to avoid potentially dangerous situation.

# 4 Conclusions

This article presented an overview of a network security model for a service-based ad hoc network. The necessary minimal services in this model are the locating and registration services. The former is necessary for the existence of a services network and the latter second for it is security. These services can be replicated in many devices and, despite being necessary, do not need to be present at all times, fulfilling ad hoc network requirements.

The model guarantees the security of network resources through certificates issue by the registration service. The individual certificates ensure the authenticity of entities involved in the communication, while the groups' certificates (credentials), guarantee the services access rights. The presence of the registration service is not essential after the entity receives its certificates: after receiving them the entity is capable of identifying itself and the groups it belongs to without depending on other entities.

Through proposed solutions in the model it is possible to guarantee ad hoc services network security without central elements dependency, which are usually presents at all times in traditional networks.

This security model targets services networks based in Bluetooth and IEEE 802.11b technologies. Futures works will describe the architecture of security model shown in this paper.

# 5 References


[1] IEEE Std. 802.11 - *Wireless LAN Media Access Control (MAC) and Physical Layer (PHY) specifications*, 1999.

[2] Bluetooth SIG – *Specification of the Bluetooth – Core, version 1.1* – specification volume 1, February 2001.

[3] Bray, J.; Sturman, C.F. – *Bluetooth: Connect without Cables* – Prentice Hall, 2000

[4] Bruno, R.; Conti, M.; Gregori, E. – *WLAN Technologies for Mobile ad hoc Network* – IEEE Proceeding of the 34th Hawaii International Conference on System Sciences, 2001.

[5] Feeney, L.M.; Ahlgren, B. – *Spontaneous Networking: An application-Oriented Approach to Ad hoc Networking* – IEEE Communications Magazine, june 2001.

[6] Kärpijoki, V. - *Signaling and Routing Security in Mobile and Ad hoc Networks* - http://hut.fi/~vkarpijo/iwork00/, 2000.

[7] Perkins, C.E. - *Ad Hoc Networking* – Addison-Wesley, 2001.

[8] Träskbäck, M. - *Security of Bluetooth: An overview of Bluetooth Security* – 2000.

[9] Zhou, L.; Haas, Z. – *Securing Ad hoc Network* – IEEE Network, Nov/Dec 1999.