Wireless/Mobile Network Security
Y. Xiao, X. Shen, and D.-Z. Du (Eds.) pp. – - –
©2006 Springer

Chapter 6

Pre-Authentication and Authentication Models in Ad Hoc Networks

Katrin Hoeper
Department of Electrical and Computer Engineering
University of Waterloo,
200 University Avenue West, Waterloo, Ontario, N2L 3G1, Canada
E-mail: khoeper@engmail.uwaterloo.ca

Guang Gong
Department of Electrical and Computer Engineering
University of Waterloo,
200 University Avenue West, Waterloo, Ontario, N2L 3G1, Canada
E-mail: ggong@calliope.uwaterloo.ca

1 Abstract

Providing entity authentication and authenticated key exchange among nodes are both target objectives in securing ad hoc networks. In this chapter, a security framework for authentication and authenticated key exchange in ad hoc networks is introduced. The framework is applicable to general ad hoc networks and formalizes network phases, protocol stages, and design goals. To cope with the diversity of ad hoc networks, many configuration parameters that are crucial to the security of ad hoc networks are discussed. Special attention is paid to the initial exchange of keys between pairs of nodes (pre-authentication) and the availability of a trusted third party in the network. Next, several pre-authentication and authentication models for ad hoc networks are discussed. The models can be implemented as a part of the proposed security framework and correspond to the wide range of ad hoc network applications. Advantages and disadvantages of the models are

analyzed and suitable existing authentication and key exchange protocols are identified for each model.

2 Introduction

The number of applications that involve wireless communications among mobile devices is rapidly growing. Many of these applications require the wireless network to be spontaneously formed by the participating mobile devices themselves. We call such networks *ad hoc networks*. The idea of ad hoc networks is to enable connectivity among any arbitrary group of mobile devices everywhere, at any time. We distinguish two categories of ad hoc networks, *mobile ad hoc networks (MANETs)* and *smart sensor networks*. Typical devices of MANETs are PDAs, laptops, cell phones, etc., and the devices of smart sensor networks are sensors. MANETs are used at business meetings and conferences to confidentially exchange data, at the library to access the Internet with a laptop, and at hospitals to transfer confidential data from a medical device to a doctor's PDA. Sensor networks can be used for data collection, rescue missions, law enforcement and emergency scenarios. Many more applications exist already or are imaginable in the near future. Caused by the widespread applications, a general security model and protocol framework for authentication and authenticated key establishment in ad hoc networks have not been defined yet.

2.1 Ad Hoc Network Properties

To achieve the ambitious goal of providing ubiquitous connectivity, ad hoc networks have special properties that distinguish them from other networks. We briefly discuss those properties in the following.

Ad hoc networks are *temporary* networks because they are formed to fulfill a special purpose and cease to exist after fulfilling this purpose. Mobile devices might arbitrarily join or leave the network at any time, thus ad hoc networks have a *dynamic infrastructure*. Most mobile devices use radio or infrared frequencies for their communications which leads to a very *limited transmission range*. Usually the transmission range is increased by using *multi-hop* routing paths. In that case a device sends its packets to its neighbor devices, i.e. devices that are in transmission range. Those neighbor nodes then forward the packets to their neighbors until the packets reach their destination. The most distinguishing property of ad hoc networks is that the networks are *self-organized*. All network interactions have to be executable in absence of a trusted third party (TTP), such as the establishment of a secure channel between nodes and the initialization of newly joining nodes. Hence, in contrast to wireless networks, ad hoc networks do not rely on a fixed infrastructure and the accessibility of a TTP. The self-organizing property is unique to ad hoc networks and makes implementing security protocols a very challenging task. Another characteristics of ad hoc networks are the *constrained network devices.* The constraints of ad hoc network devices are a small CPU, small memory, small bandwidth, weak physical protection and limited battery power, as first summarized in [23]. In most ad hoc networks all *devices have similar constraints.* This property distinguishes the architecture of an ad hoc network from a client-sever structure.

2.2 Security Challenges

The special properties of ad hoc networks enable all the neat features such networks have to offer, but at the same time, those properties make implementing security protocols a very challenging task. There are four main security problems that need to be dealt with in ad hoc networks: (1) the *authentication* of devices that wish to talk to each other; (2) the *secure key establishment* of a session key among authenticated devices; (3) the *secure routing* in multi-hop networks; and (4) the *secure storage of (key) data* in the devices. Note, that once (1) and (2) are achieved, providing confidentiality is easy. In the remainder of this article, we will focus on entity authentication and authenticated key establishment (AAKE) protocols and their implementation issues in ad hoc networks. Note that most security problems related to such protocols occur in the bootstrapping phase, i.e. at the time nodes wish to securely communicate for the very first time. We refer to this phase as the *pre-authentication phase*, and we define and discuss this stage in great detail later in this chapter.

2.3 Outline

As said earlier, due to the wide range of ad hoc network applications, no general security framework has been introduced yet. In this chapter, we introduce a security framework for authentication and authenticated key exchange in ad hoc networks. The framework is applicable to general ad hoc networks and formalizes network phases, protocol stages, and design goals. To cope with the diversity of ad hoc networks, we discuss many configuration parameters that are crucial to the security of ad hoc networks. We pay special attention to the initial key exchange between pairs of nodes (pre-authentication) and the availability of a TTP in the network. We then categorize several pre-authentication and authentication models that can be implemented as a part of the proposed security framework. The models correspond to the wide range of ad hoc network applications and we analyze their advantages and disadvantages and identify suitable existing authentication and key exchange protocols for each model.

The rest of this chapter is organized as follows. In Section 3, we introduce a security framework for ad hoc networks, including network and authentication phases, protocol stages and design goals. In Section 4, we identify some security related configuration problems that are crucial for protocol implementations in many ad hoc network applications. Taking all previous results into account, we categorize and analyze a number of pre-authentication and authentication models in Section 5 and 6, respectively. Finally, in Section 7, conclusions are drawn.

3 Security Framework

In this section, we first discuss the different network phases that occur in the lifecycle of an ad hoc network. Then, we introduce the two authentication phases of communicating nodes in such networks. Next, we define the protocol stages of general AAKE protocols in ad hoc networks. At the end of this section, we summarize the design goals all protocols that are designed for ad hoc networks should meet. All these definitions combined form a security framework for general ad hoc networks. The framework helps designing security solutions for ad hoc networks. In particular, when proposing protocols for ad hoc networks, all network and authentication phases, protocol stages and design goals as defined in this security framework need to be addressed.

3.1 Network Phases

We distinguish two network phases in ad hoc networks, namely the *network initialization phase* and the *running system phase*. In the first phase, the network is set up. All nodes that are present at the network initialization phase, i.e. during the time the network is formed, are initialized. The self-organization property of the network is sometimes not required in this phase. For instance, a TTP might be available in the initialization phase in order to initialize all present nodes with required data, such as system parameters and cryptographic keys. After the initialization phase, nodes can freely join or leave the network at any time. We refer to this as running system phase. Ad hoc networks are generally self-organized in this phase. This follows that no TTP or other fixed infrastructure is longer available. Consequently, current network nodes are responsible to initialize newly joining nodes with required key material, cope with leaving nodes and execute all other necessary administrative tasks in a self-organized manner.

3.2 Authentication Phases

We distinguish two authentication phases for authentications among network nodes. The first phase consist of the initial exchange of data and cryptographic key material among a group of two or more nodes. The data can include secret or public keys, for example. The same data is used to identify each other in all later authentications among the same nodes. The described initial authentication phase is called *imprinting* in the resurrecting duckling model [23], and *initialization* in the Bluetooth protocol [4]. Henceforth, we will adopt the term *pre-authentication* from [2]. The data that is exchanged in the pre-authentication phase needs to be sent over a secure channel, where secure refers to an authentic and confidential channel for exchanging symmetric key data, and to an authentic channel for exchanging public keys in asymmetric schemes. Pre-authentication is not limited to the devices present at the time of the network initialization phase, it also needs to be provided to subsequently joining nodes in the running system phase. All nodes that subsequently join the ad hoc network need to be able to securely obtain shared data and required key material from all potential communication partners. The main challenge is to provide pre-authentication in the running system phase, even though the network environment might have changed and a TTP is not accessible any longer. During the second phase, the *authentication phase*, the nodes identify each other by using the authentic data that was exchanged in the pre-authentication phase. These authentications are executed over an insecure channel and need to be secured by the key material exchanged during pre-authentication.

3.3 Protocol Stages

We now consider the protocol stages of a two party AAKE protocol. The desired AAKE protocol should first provide pairwise pre-authentication, then mutual authentication between the same two nodes, and lastly, a secure establishment of a session key shared between the nodes. All AAKE protocols can be executed in the *running system* in an ad hoc network, i.e. after the network initialization phase. A suitable AAKE protocol should take all ad hoc network properties and constraints into account. Note, that the protocol design goals are defined in the next section.

A typical AAKE protocol in our security framework for ad hoc networks consists of the following three stages:

1. Pre-Authentication

The first stage is the pre-authentication between two devices that wish to communicate with each other at this or a later time. In this phase either a secret key or an authentic copy of a public key are securely shared between the devices. Keys can be shared during pre-authentication using one of the pre-authentication models that we will introduce in Section 5. The best suited model needs to be chosen according to the particular application.

The key data that has been exchanged or established during pre-authentication is used in all subsequent authentications between the same nodes. Hence, the next time the same nodes wish to securely communicate, i.e. to execute an AAKE protocol, the nodes can skip the pre-authentication stage and directly start with the authentication. Pre-authentication needs only to be repeated if keys are revoked or expired.

2. Authentication

In the second stage, the authentication stage, the participants mutually authenticate each other using the key data from the pre-authentication phase. A suited authentication protocol can be chosen out of the authentication models introduced in Section 6. The best suited protocol needs to be chosen according to the respective application. If the authentication of one node fails, the protocol stops and further countermeasures might be taken, for example revoking the key of the rejected node.

3. Session Key Establishment

Upon successful mutual authentication, the nodes start establishing a session key in the third protocol stage. Note that all session keys need to be established over an authentic channel. Otherwise, Oscar could take over Alice's role after her successful authentication to Bob. To overcome this attack, the session key establishment stage can be combined with the previous authentication stage. Again, for suitable AAKE protocols please refer to Section 6.

3.4 Design Goals

After discussing the special properties and needs of ad hoc networks and several of the issues that occur when implementing protocols in such networks, we now derive the design goals that all ad hoc network protocols should meet in order to be suitable.

All protocols should only require *few computational steps* due to the limited battery power of all ad hoc devices. Too many computational steps would drain the battery. For the same reason protocols should only require *few message flows.* Caused by the nature of wireless networks, the communication bandwidth is very small. If messages are too large, they will be split into several packets. Sending many packets contradicts with the previous design goal, therefore *small data packages* are desirable. Due to the limited computational power of ad hoc devices, preferable protocols should mainly require *cheap computations.* As a general trend, the processors of most ad hoc devices, such as PDAs, are becoming more and more powerful, and therefore heavy computations, such as modular exponentiations, are becoming feasible. However, heavy computations require more battery power, and thus, it is important to restrict the number of heavier computations. Based on the assumption that all ad hoc network devices have similar constraints, suited protocol should be *balanced*, i.e. all devices need to perform approximately the same number of equally heavy computations. Considering the very limited memory space of all devices, protocols should neither require much memory space for the protocol code itself nor for the storage of parameters and key material. As a consequence, *short code, short keys and short system parameters* are desirable. When designing protocols the *consequences of data disclosure should be very restricted* because ad hoc network devices and especially sensors provide only a low level of physical protection. Once an attacker gains access to the device, he/she is usually able to obtain the stored data, including the key material. Note that this attack is quite reasonable since such devices cannot be protected as some servers that are locked away in secure rooms, for instance. The protocol should be designed in a way that the disclosure of the stored data does not compromise the entire system. Also the delectability of such disclosures within the system needs to be examined when designing a protocol.

In addition to the previous design objectives, protocol designed for sensor networks should be *scalable* to cope with the large number of sensors in the network and be *fault tolerant* because sensors are very prone to failures.

4 System Configurations

In this section, we identify the problems that one might encounter when implementing AAKE protocols in ad hoc networks. Therefore, we consider several system settings that occur in different applications, such as the availability of a TTP, the security of the communication channels, the constraints of the devices, the number of participating domains, etc..

4.1 Availability of Trusted Third Party (TTP)

The availability of a TTP is crucial for a protocol implementation and one of the new challenges of ad hoc networks. A TTP can play several roles in a network, for instance, the TTP could be responsible to initialize devices with secret keys, issue and distribute public keys and certificates, distribute session keys to devices that wish to securely communicate, or help to verify the validity of certificates by providing certificate revocation lists (CRLs). We distinguish among four different settings for the availability of a TTP, described in the following paragraphs and illustrated in Figure 1. The four rows in the figure correspond to the four settings, where the first column describes the network initialization phase, the second column the event of a joining node in the running system phase and the third column the event of present nodes establishing a secure channel, i.e executing an AAKE protocol.

AV-1: TTP is always available
The case that a TTP is accessible by all network nodes at any time is generally not considered as an option in ad hoc networks, because ad hoc networks should be self-organized after their initialization phase. However, in the future it might be reasonable to assume an Internet connection in some as hoc network applications, for example via an access point. In that case, we could adopt WLAN solutions and modify them to cope with the resource constraints and mobility of ad hoc network devices.

AV-2: TTP is available at network initialization phase and every time a node joins
The second option comprises all scenarios where a TTP is available at the network initialization phase and, in addition, the TTP is accessible by all nodes that subsequently join the network. This assumption is not as restrictive as it might seem, because the TTP does not need to be accessible by all network nodes every time a new node joins a network. For instance, there could be applications in which nodes contact a TTP to receive the required

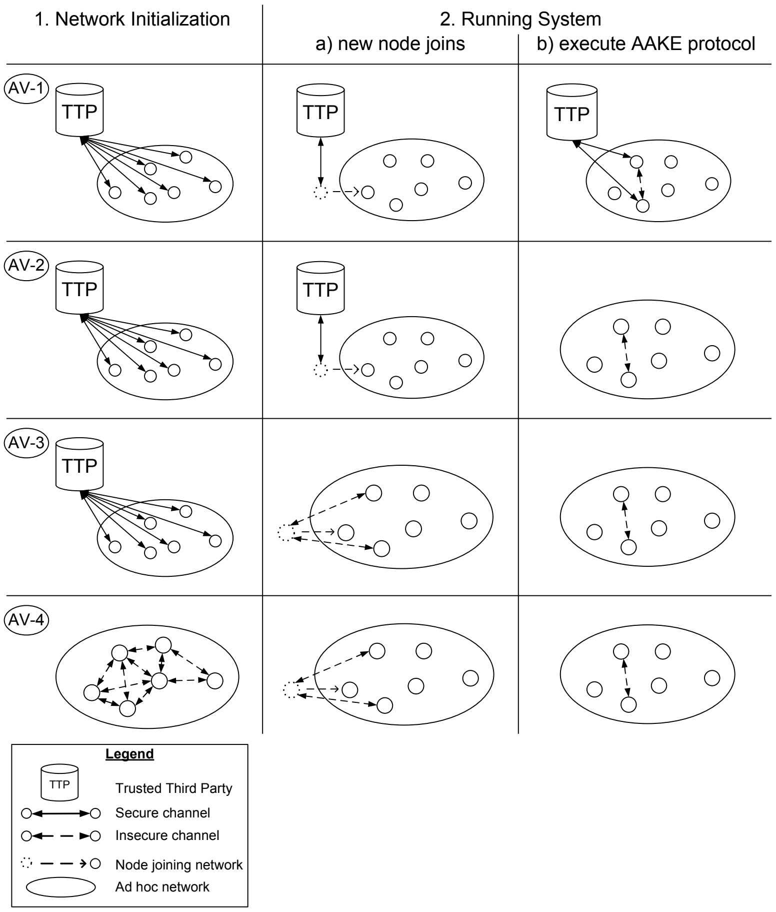

Figure 1: Four scenarios of TTP availabilities *AV-1* – *AV-4*, as described in Section 4.1: (1) during the network initialization; and (2) in the running system when (a) new nodes join or (b) present nodes establish a secure channel, i.e execute an AAKE protocol.

system parameters and keys before joining the network. The network itself is still self-organized and the present nodes have no access to a TTP.

AV-3: TTP is available at network initialization phase
In this scenario only the nodes that were present at the time of the network initialization phase are initialized by the TTP. Usually this is called self-organization property of the network. The present network nodes are responsible to take over the tasks of the TTP, such as issuing and distributing keys and/or certificates to subsequently joining nodes.

AV-4: No TTP is available at any network phase
In this scenario network nodes need to take over the tasks of the TTP during the network initialization phase and in the running system phase. If no TTP is available at any time, implementing security protocols such as AAKE protocols is very challenging. If we want to implement a symmetric scheme we would need to develop a security model in which devices can securely exchange their common keys. Whereas implementing a public key encryption schemes would require an authentic channel to exchange public keys without the aid of a TTP that issues keys or key credentials.

4.2 Other Configuration Parameter

There are many other implementation issues that depend on the particular ad hoc network application. We will discuss some of those issues that could affect the implementations of security protocols.

First of all, the *security of the communication channels* is a crucial parameter in ad hoc network applications. We distinguish two communication channels. One channel to exchange the data during the pre-authentication phase and another channel for the authentication and key establishment phases. As discussed earlier, pre-authentication requires a secure channel among the devices to securely exchange authentic public key data or authentic and confidential secret key data. Upon pre-authentication, all communications can be executed over an insecure channel where the communication is secured by the key material that was exchanged during pre-authentication. How a secure pre-authentication or authentication channels can be established is discussed in Section 5 and 6, respectively.

Another implementation issue is the *level of resource constraints.* Depending on the computational constraints of the network devices it might be feasible or infeasible to execute protocols requiring heavy or many computations, as required in most public key schemes. In addition to the computational constraints, we have to consider the communication and power constraints when designing or implementing a protocol. Generally sensors are too constrained for implementing public key protocols.

Hierarchical ad hoc networks haven been proposed as alternative to flat ad hoc topologies to overcome some limitations of the latter, as for instance described in [5]. Hierarchical ad hoc networks have several layers, where each layer consists of a set of similar devices. For instance, the lowest layer consists of the least powerful devices, e.g. sensors, and each higher level consists of some more powerful devices, where the top level could be the Internet. In this way, all heavy computations could be shifted from the very constrained devices to the more powerful ones and thus asymmetric schemes could become feasible. For this reason, the model is attractive for sensor networks. It needs to be analyzed for particular applications if it is reasonable to assume that higher layers can be accessed by all sensor networks at any time.

When Stajano and Anderson [23] were among the first to consider the special properties of ad hoc networks, they assumed a *controller* (mother duck) and several devices that are controlled (ducklings) in all ad hoc networks. In the proposed resurrecting duckling model, the mother duck imprints their ducklings, who, from then on, follow their mother. In another more recent paper Messerges et. al [21] described some applications that require a controller, e.g. sensor networks used for industrial control and building automation. In networks without a controller all nodes have similar roles and are assumed to have similar resource constraints. Whether we have an ad hoc network with or without controller depends on the application.

In some scenarios devices might be *aware of their location* and are able to provide information about their location, such as their geographical coordinates. A simple solution for providing the present location of mobile devices is to embed an additional integrated chip, such as a GPS chip, in all devices. For instance, some high-end PDAs are already equipped with GPS chips. However, there are many different systems that provide location coordinates depending on the network range and location. The most commonly known systems for tracking down devices are: (1) satellite navigation systems, such as GPS, or the European equivalent Galileo; (2) systems for locating devices inside a building using visual, ultra sonic, radio, or infrared channels; and (3) network based positioning system, such as GSM, and WLAN. If a user knows the location of its communication partner the data could be used to build an authentic channel, e.g. for authentication or public key exchange. However, special equipment for tracking devices is unnecessary if the location of devices is predictable. For instance, in some sensor networks, the sensors have an expected location. This knowledge is used in a location-based pairwise key establishment protocol [18], for instance.

The last system property we consider is the *number of domains* in our network. All devices in one domain share the same domain parameters, such as shared keys, that has been distributed during the network initialization, a certificate issued by the domain's certification authority (CA), or system parameters required for some computations. In most sensor networks, it is reasonable to assume one domain. However, in many MANETs, devices are from different domains. Providing authentication in those scenarios is harder to implement. Communicating parties need mechanisms to verify the trustworthiness of devices outside their own domain and to securely agree on some common system parameters. These compatibility issues have to be considered when implementing an AAKE protocol.

5 Pre-Authentication Models

In this section we discuss several symmetric and asymmetric pre-authentication models (PAMs) for providing pre-authentication in ad hoc networks. We summarize all models for better comparison in Table 1. We reference some papers that introduced protocols in the respective models in the second column and summarize the advantages and disadvantages of each model in the right column.

5.1 Symmetric Solutions

When using symmetric encryption a secret must be shared among the devices that wish to communicate. The secrets are established during the network initialization phase and the pre-authentication phase of the devices. Clearly, an authentic and confidential channel needs to be established to ensure secure pre-authentication. The following models describe how such a secure channel can be established.

PAM-S1. Secure Side Channel Model
In this model the secret information is exchanged over a secure side-channel during the network initialization phase and the pre-authentication phase of the devices. How this secure channel is established is not further specified in the model and left to be done by the users or the administrators that imple-

Model	Implementation	Comments*
PAM-S1. Secure Side-Channel	Keys exchanged over secure side-channel, e.g. IEEE 802.11 [14]	− secure channel not provided by system itself
PAM-S2. PIN	PIN manually entered in all devices, e.g. Bluetooth [4]	− does not scale well
PAM-S3. Physical Contact	Key exchanged by physical contact, e.g. resurrecting duckling protocol [23]	− requires proximity of the devices
PAM-S4. Pairwise Key Pre-Distribution	Sensors initialized with subset of key pool before deployed, e.g. [8]	− only one domain − requires TTP for every initialization
PAM-A1. Location-Limited	Public key directly exchanged, e.g. [2, 6]	− requires proximity of devices
PAM-A2. ID-Based	Identity used as self-authenticated public key, e.g. [15, 12]	+ implicit pre-authentication − KGC is key escrow
PAM-A3. Self-Certified Public Key	Certificate embedded in public key, e.g. [9]	+ implicit pre-authentication − no AAKE protocols
PAM-A4. Distributed CA	CA represented by n nodes using threshold scheme [27, 16, 19]	+ self-organized − not efficient[†] − requires many nodes
PAM-A5. Trusted Path	PGP-like; find trusted path between two nodes, e.g. [11, 7]	+ self-organized − not efficient − requires many nodes

Table 1: Pre-authentication models for ad hoc networks

[*] "+"/"−" denote advantages and disadvantages of the model, respectively.

[†] Efficiency with respect to computation and communication cost.

ment the protocol. For instance, the IEEE standard for wireless local area networks (WLAN) IEEE 802.11 [14] does not provide any recommendations and information of how pre-authentication can be achieved and assumes that pre-authentication has taken place before devices start communicating with each other. Hence, IEEE 802.11 is a protocol standard proposed in the discussed model.

PAM-S2. PIN Model

Protocols in this model require that passwords, PINs, or keys are manually entered in all devices that wish to securely communicate. This can be done by an administrator during the network initialization phase or by users as pre-authentication of their devices. Solutions in this model do not scale well because the secret needs to be entered manually in each device. An example for a protocol in this model is the Bluetooth protocol that was introduced by the Bluetooth Special Interest Group (SIG) [4]. The protocol is standardized as IEEE 802.15 [14] for wireless personal area networks (WPANs).

PAM-S3. Physical Contact Model

In this model the symmetric keys are exchanged by physical contact among the devices. Note that the physical contact provides an authentic and confidential channel. The requirement of physical contact among all communicating devices is be too restrictive in some applications. A protocol in this model is introduced in [23].

PAM-S4. Pairwise Key Pre-Distribution Model

Public key cryptography is not feasible in sensor networks and therefore only symmetric schemes are applicable. The approach that all sensors share the same secret key is not suited because once a single key is compromised the entire sensor network would be compromised as well. Due to the weak physical protection of sensors, compromising a single sensor and thus its stored key material is very likely. For this reason, sharing keys in a pairwise fashion seems to be a more reasonable approach. Since sensors have very constrained memory, they cannot store symmetric keys of every other sensor in the network. To overcome this constraint, the *pairwise key pre-distribution model* is introduced, in which each sensor is initialized with a subset of all network keys. Note that all sensors need to belong to the same domain. However, in most sensor network applications, it can be assumed that a trusted authority can set-up all sensors before they are deployed. An example of a protocol in this model is in [8].

5.2 Asymmetric Solutions

We describe several asymmetric pre-authentication models (PAM-As) in this section. Each model provides a method to obtain an authentic copy of the public key of a communication partner. The lack of a central CA is the main problem when implementing asymmetric protocols in ad hoc networks. We distinguish four categories of PAM-As: (1) with CA and use of certificates; (2) with CA and no use of certificates; (3) without CA and use of certificates; and (4) without CA and no use of certificates. The first category includes the distributed CA model; the second one includes the identity-based model and the self-certified public key; the third category contains the trusted path model; and the fourth contains the location-limited model.

PAM-A1. Location-Limited Model
If proximity of the ad hoc network devices is given, a secure pre-authentication channel can be established by visual or physical contact among the communicating devices. This secure pre-authentication channel enables the devices to directly exchange their public keys, i.e. without the necessity of a CA and public key certificates. This model is based on two assumptions, (1) all participants are located in the same room; and (2) all participants trust each other a priori. The model is well suited in all scenarios that meet those two assumptions and not applicable in any other scenario. Protocols in this model are introduced in [2, 6]. Note that in most cases where devices can perform physical contact implementing the physical contact model (PAM-S3) seems to be more reasonable.

PAM-A2. Identity-Based Model
Identity (ID)-based schemes, introduced in [22], do not require any key exchange prior to the actual authentication, because common information, such as names and email addresses, is used as public key. Since public keys are self-authenticating, certificates are redundant in this model. Pre-authentication is implicitly provided by the system because the (authentic) public keys of all network devices are known prior communicating. As a consequence, protocols in the *identity-based model* do not require any secure pre-authentication channel. This feature makes the ID-based model attractive for ad hoc networks. ID-based schemes require a TTP that serves as key generation center (KGC) in the network initialization phase in order to generate and distribute the personal secret keys to all users. Drawbacks of this model are: (1) the KGC knows the secret keys of all users; and (2) a confidential and authentic channel between the CA and each network de-

vice is required for the securely distribution of the secret keys. The latter problem can be eliminated by using a blinding technique as shown in [17] and the first drawback is shown to have low impact in ad hoc networks in [13]. The first protocol in this model is in [15], but the authors do not provide an actual AAKE protocol and many open questions for a protocol implementation remain. Some AAKE protocols in this model are in [12].

PAM-A3. Self-Certified Public Key Model
In this model the certificates are embedded in the public keys themselves. So-called self-certified public keys are introduced in [9] and, other than in ID-based schemes, the identity itself is not directly used as a key. In fact the identity is a part of the user's public key and signed by a CA and the users themselves. Hence, the public keys are unpredictable and need to be exchanged prior to the communication. The authenticity of the public keys is provided by the keys themselves, and thus we do not need a secure pre-authentication channel. In addition, this approach helps to save some bandwidth and memory space, because certificates do not need to be transmitted and stored. A CA is required to generate the self-certified public keys using the devices' public keys, identifiers, and the CA's master secret key as input. Protocols in this model are an authentication protocol without key agreement and a static DH-like key agreement [9].

PAM-A4. Distributed CA Model
In the distributed CA model the power and the tasks of a CA are distributed to t network nodes by implementing a (t, n)-threshold scheme. The idea is based on the fact that a CA should not be represented by a single node, because nodes can be relatively easily compromised by an adversary. In this model a group of t nodes can jointly issue and distribute certificates. Protocols in this model might support certificate renewing and revocation. We distinguish two cases, (1) a *distributed CA with special nodes* and (2) a *distributed CA without special nodes*. In the first case t special nodes, that have more computational power and that were present at the network initialization phase, represent the CA. The special role of the server nodes contradicts with the property of similar constrained devices as stated in our design goals. An example of a protocol that has been proposed in this model is [27]. In the distributed CA model without special nodes, any t network node represent the CA and can thus issue certificates. Protocols that have been proposed in this model are [16, 19].

PAM-A5. Trusted Path Model

The trusted path model emphasizes the self-organization property which is a unique and challenging feature of ad hoc networks. Network nodes issue and distribute their own certificates and sign other certificates. The model assumes the existence of trust between some nodes and generates trust between nodes in a PGP manner, i.e. by finding a so-called trusted path consisting of certificates between the communicating nodes. The performance of pre-authentication highly depends on the length of the trusted path, which is generally hard to predict. This approach is very efficient in the set-up phase and does not require any heavy computation steps from any parties other than the communicating ones. However, a node probably needs to verify more than one certificate for pre-authentication. An example of a proposed protocol in this model is [11]. This model is also applied to a group case, in which trusted subgroups search for intersections to create a trusted path [10].

6 Authentication Models

After the pre-authentication phase, the exchanged key material can be used to enable authentication and key establishment in any of the authentication models (AMs) described in this section. We briefly discuss some symmetric, hybrid, and asymmetric authentication models (AM-S, AM-H, AM-A) and summarize the models in Table 2, where we reference proposed protocols in the second column and summarize advantages and disadvantages of the models in the right column. Please note that many more models exist and we only present a small subset, where we limit our focus to models suitable to ad hoc networks.

6.1 Symmetric Solutions

After successful pre-authentication has taken place in any of the previously described symmetric pre-authentication models, we can run any symmetric AAKE protocol.

AM-S1. Challenge-response Using Symmetric Schemes
The devices can use their shared key in a challenge-response type protocol [20], in which devices authenticate each other by demonstrating knowledge of the shared key by encrypting a challenge.

Model	Implementation	Comments*
AM-S1. Challenge-Response	Devices demonstrate knowledge of shared key by encrypting a challenge [20]	+ efficient† − requires long and secure shared secret
AM-H1. Password	Shared password is used for encrypting public keys, e.g. [3, 1]	+ requires short (memorizable) password − not efficient
AM-A1. Challenge-Response	Devices either decrypt a challenge that is encrypted under their public key or sign a challenge [20]	− not efficient
AM-A2. Key Chain	Anchor x_0 of hash chain is private key, x_n public key [24, 25, 26]	+ very efficient − no key agreement

Table 2: Authentication models for ad hoc networks

* "+"/"−" denote advantages and disadvantages of the model, respectively.

† Efficiency with respect to computation cost.

6.2 Hybrid Solutions

Some ad hoc network solutions combine symmetric and asymmetric crypto schemes to provide entity authentication and optionally key establishment after pre-authentication phase has taken place in any of the presented pre-authentication models.

AM-H1. Password Model
Depending on the available memory size and the way the secret is exchanged, it might be desirable to share a short password instead of a long secret key. Note that such passwords are weak secret keys. Due to their shortness, passwords are prone to brute-force attacks, where user-friendly passwords are also prone to off-line dictionary-attacks. The password needs to be securely exchanged by one of the PAM-S discussed in Section 5.1. AAKE protocols in the *password model* combine a weak password and an asymmetric scheme to obtain a strong shared key and are called password-authenticated key exchange (PAKE) protocols [3]. Due to the use of asymmetric crypto schemes, PAKE protocols require some heavy computational steps, and are thus only applicable to ad hoc networks consisting of powerful devices that have sufficient computation power. Examples of protocols in this model are [3] for the two-party case and [1] for the multi-party case.

6.3 Asymmetric Solutions

We can implement any asymmetric AAKE protocol after pre-authentication has taken place in one of the PAM-As discussed in Section 5.2.

AM-A1. Challenge-Response Using Asymmetric Schemes
Once the devices share authentic copies of their public keys they can use either these public keys or their own private keys to prove their identities. A common method are challenge-response type protocols [20]. The establishment of an encryption key for the current session may be a part of the protocol as well.

AM-A2. Key Chain Model
Hash chains [20] are an asymmetric approach that is attractive for ad hoc network due to the excellent performance. In hash chain schemes, a hash function $h(\cdot)$ is applied n times to a random value x. The initial value $x_0 = x$ is the so-called anchor which serves as the private key, whereas the last value of the hash chain $x_n = h^n(x)$ serves as public key. Each device first computes its own hash chain, also called key chain, then authentically exchanges x_n with its communication partners in one of the pre-authentication models described in Section 5.2. The value x_0 is kept secret. A device that is challenged by a value x_i from its key chain can prove its identity by responding with the previous value x_{i-1} of the chain. Only a device that knows the anchor x_0 is able to compute the required response. This scheme requires only the computation of hash values which can be implemented very efficiently. Note that schemes implementing key chains provide only unidirectional authentication and no key is established during the protocol execution. Examples of the protocols in this model are [24, 25]. Note that the protocol in [24] is broken and fixed in [26].

7 Conclusions

Authentication and authenticated key exchange are both identified as primary security objectives in ad hoc networks. In this chapter, we introduced a security framework for general ad hoc networks to achieve these two goals. As part of the security framework we defined network phases, protocol stages, and design goals. Next, we coped with the diversity of ad hoc network applications. Therefore, we identified crucial configuration parameters of particular applications, that need to be taken into account when implementing AAKE protocols in these scenarios. Here, our special focus was on the availability of a TTP, but many other security related configuration parameters were discussed as well. Considering all special network and device constraints, we derived a set of design objectives for general ad hoc network protocols. Taking all previous results into account, we finally categorized a number of pre-authentication and authentication models based on symmetric, hybrid, and asymmetric cryptographic schemes. The models can be implemented as a part of the security framework and they correspond to the diversity of ad hoc network applications. We analyzed the models, pointed out their advantages and disadvantages, and showed for which application particular models are best suited. Furthermore, we identified several previously proposed AAKE protocols that are suitable for each model. Our results can be used as a toolbox for designing and analyzing AAKE protocols as well as a guideline for choosing the best suited protocol for particular ad hoc network applications.

We conclude from our analysis that some commercial ad hoc network applications can be securely and efficiently implemented by existing symmetric solutions. The PIN model is applicable to all PANs, in which a user can set up all of his/her devices with one PIN or password, or an administrator is able to set up all authorized devices in order to share network resources. The physical contact model is suitable for all applications where people or devices, who already trust each other, are located in a small area. Protocols in the pre-distribution scheme are suited in sensor networks in which all sensors belong to one domain. An asymmetric approach which seems to be suitable for mobile device-terminal connections is the exchange of public keys over a location-limited channel. This approach could be implemented in some civil applications, such as virtual classrooms, internet access points, and all communications between PDAs and laptops of different users. The approach is limited to networks with a small number of devices that provide moderate computational power. All approaches in the distributed CA and trusted path model are only suitable for networks with a large number of nodes. Furthermore, we believe that these two models are not efficient in terms of the computational and communication overhead. The identity-based and the self-certified public key model are both promising pre-authentication models because they do not require a secure channel. However, those models need to be further studied and protocols have to be proposed.

References

[1] N. Asokan and P. Ginzboorg, Key Agreement in Ad Hoc Networks, *Computer Communications*, Vol. 23, No. 17, 2000, pp. 1627-1637.

[2] D. Balfanz, D.K. Smetters, P. Stewart, and H. Chi Wong, Talking to Strangers: Authentication in Ad-Hoc Wireless Networks, *Proceedings of Network and Distributed System Security Symposium 2002 (NDSS '02)*, 2002.

[3] S.M. Bellovin and M. Merritt, Encrypted Key Exchange: Password-Based Protocols Secure Against Dictionary Attacks, *Proceedings of the 1992 IEEE Symposium on Security and Privacy*, IEEE Computer Society, ISBN: 0-8186-2825-1, 1992, pp. 72-84.

[4] Bluetooth SIG, *Specification of the Bluetooth System*, Version 1.1; February 22, 2001, available at `https://www.bluetooth.com`.

[5] M. Bohge and W. Trappe, An authentication framework for hierarchical ad hoc sensor networks, *Proceedings of the 2003 ACM workshop on Wireless security*, ISBN:1-58113-769-9, ACM Press, 2003, pp.79-87.

[6] M. Cagalj, S. Capkun and J.P. Hubaux, Key agreement in peer-to-peer wireless networks, to appear in *Proceedings of IEEE, Special Issue on Security and Cryptography, 2005.*

[7] S. Čapkun, J.-P. Hubaux, and L. Buttyán, Self-Organized Public-Key Management for Mobile Ad Hoc Networks, *IEEE Transactions on Mobile Computing*, Vol. 2, No. 1, 2003, pp. 52-64.

[8] L. Eschenauer and V.D. Gligor, A Key-Management Scheme for Distributed Sensor Networks, *9th ACM conference on Computer and Communications Security*, ISBN:1-58113-612-9, ACM Press, 2002, pp. 41-47.

[9] M. Girault, Self-Certified Public Keys, *Advances in Cryptology- EUROCRYPT '91*, LNCS 547, Springer, 1991, pp. 490-497.

[10] S. Gokhale and P. Dasgupta, Distributed Authentication for Peer-to-Peer Networks, *Symposium on Applications and the Internet Workshops 2003 (SAINT'03 Workshops)*, IEEE Computer Society 2003, ISBN 0-7695-1873-7, 2003, pp. 347-353.

[11] J.P. Hubaux, L. Buttyán and S. Čapkun, The Quest for Security in Mobile Ad Hoc Networks, *ACM Symposium on Mobile Networking and Computing –MobiHOC 2001*, 2001.

[12] K. Hoeper and G. Gong, Identity-Based Key Exchange Protocol for Ad Hoc Networks, *Canadian Workshop of Information Theory -CWIT 05*, 2005.

[13] K. Hoeper and G. Gong, Short Paper: Limitations of Key Escrow in Identity-Based Schemes in Ad Hoc Networks, *Security and Privacy for Emerging Areas in Communication Networks SecureComm 05*, 2005.

[14] IEEE 802.11, Standard Specifications for Wireless Local Area Networks, `http://standards.ieee.org/wireless/`.

[15] A. Khalili, J. Katz, and W. Arbaugh, Toward Secure Key Distribution in Truly Ad-Hoc Networks, *2003 Symposium on Applications and the Internet Workshops (SAINT 2003)*, IEEE Computer Society, ISBN 0-7695-1873-7, 2003, pp. 342-346.

[16] J. Kong, P. Zerfos, H. Luo, S. Lu, and L. Zhang, Providing Robust and Ubiquitous Security Support for Mobile Ad-Hoc Networks, *International Conference on Network Protocols (ICNP) 2001*, 2001.

[17] B. Lee, C. Boyd, E. Dawson, K. Kim, J. Yang, and S. Yoo, Secure key issuing in ID-based cryptography, *CRPIT '04: Proceedings of the second workshop on Australasian information security, Data Mining and Web Intelligence, and Software Internationalisation*, Australian Computer Society, Inc., 2004, pp. 69-74.

[18] D. Liu and P. Ning, Location-Based Pairwise Key Establishments for Static Sensor Networks, *1st ACM Workshop Security of Ad Hoc and Sensor Networks (SASN) '03*, ISBN:1-58113-783-4, ACM Press, 2003, pp. 72-82.

[19] H. Luo, P. Zerfos, J. Kong, S. Lu, and L. Zhang, Self-Securing Ad Hoc Wireless Networks, *Seventh IEEE Symposium on Computers and Communications (ISCC '02)*, 2002.

[20] A.J. Menezes, P.C. von Orschot, and S.A. Vanstone, *Handbook of Applied Cryptography*, 1997 by CRC press LLC.

[21] T.S. Messerges, J. Cukier, T.A.M. Kevenaar, L. Puhl, R. Struik, and E. Callaway, A security design for a general purpose, self-organizing, multihop ad hoc wireless network, *1st ACM workshop on Security of ad hoc and sensor networks (SASN) '03*, ISBN:1-58113-783-4, ACM Press, 2003, pp. 1-11.

[22] A. Shamir, Identity-based Cryptosystems and Signature Schemes, *Advances in Cryptology- CRYPTO '84*, LNCS 196, Springer, 1984, pp. 47-53.

[23] F. Stajano and R. Anderson, The Resurrecting Duckling: Security Issues for Ad-Hoc Wireless Networks, *In Proceedings of the 7th International Workshop on Security Protocols*, LNCS 1796, Springer, pp. 172-194, 1999.

[24] A. Weimerskirch and D. Westhoff. Zero Common-Knowledge Authentication for Pervasive Networks, *Tenth Annual International Workshop on Selected Areas in Cryptography (SAC 2003)*, 2003.

[25] A. Weimerskirch and D. Westhoff, Identity Certified Authentication for Ad-hoc Networks, *Proceedings of the 1st ACM workshop on Security of ad hoc and sensor networks (SASN)*, 2003, ACM Press, ISBN:1-58113-783-4, 2003, pp. 33-40.

[26] S. Lucks, E. Zenner, A. Weimerskirch, and D. Westhoff, How to Recognise a Stranger - Efficient and Secure Entity Recognition for Low-End Devices, *submitted for publication.*

[27] L. Zhou and Z.J. Haas, Securing Ad Hoc Networks, *IEEE Network Journal*, Vol. 13, No. 6, 1999, pp. 24-30.