Identifying different scenarios for group access control in distributed environments

Joan Arnedo-Moreno and Jordi Herrera-Joancomartí

Estudis d'Informàtica i Multimèdia
Universitat Oberta de Catalunya
Av. Tibidabo 39–43, 08035 Barcelona
{jarnedo,jordiherrera}@uoc.edu

Abstract. Access control in distributed networking environments, such as peer-to-peer and ad hoc networks, presents a difficult challenge since these new paradigms assume a self-organizing group structure with peer equality where no central service provider is needed. In this paper we present an exhaustive description of all possible scenarios for an access control procedure in a peer-to-peer environment depending on the involvement of the peers during the registration process. We discuss the main properties of every scenario and we provide a literature review of the main proposals in the field of access control for peer-to-peer and ad-hoc networks. Such exhaustive study allows us to identify which scenarios are not efficiently solved in terms of group access control.

Keywords: Access control, peer-to-peer authentication, distributed systems security.

1 Introduction

The enormous increase in devices' interconnection capabilities has permitted the expansion of technologies such as peer-to-peer or ad-hoc networks. Even though the former is entirely related to software and the latter to the physical devices themselves, both share the same basic principle: a group of users are able to create a communications framework from scratch without the need of a central service provider. This is achievable via the aggregation of resources each one of them provide, creating a completely distributed collaborative environment based in a flat hierarchy of users, without any kind of centralization.

At first, applications from such technologies assumed a completely open environment where all peers may access everyone's resources with the only limitation of having other peers within reach. However, under some circumstances a group of users may need to create a closed community, limiting access to the shared resources to the members of the same community. In this case, we are no longer in an open environment and several security issues need to be addressed in order to protect some group's resources.

Different security solutions are based on a central service provider, often represented as a trusted third party, but in the case of peer-to-peer and ad-hoc network environments it is very important to avoid such approach, or at least minimize the system's dependency on very specific peers, trying to keep equality between them.

Several studies on this field are summarized in [1] and the basic requirements for peer-to-peer security are specified in [2]. The need for the concept of group membership is specifically the main focus in some cases such as in [3]. However, the fact that peer-to-peer networks operate at higher levels lets us focus much more in this layer, that of user equality, since it is not directly needed to tackle some big issues such as node physical proximity or real-time device mobility.

In this paper we identify different scenarios for group access based on the involvement of peers during the access process. Such classification allows a clear study of each scenario in terms of peer relevance within the group. Specifically, we will focus on the mechanisms involving group registration and authentication.

The contribution of this paper is twofold. On one hand, the paper presents a classification of each scenario based on performance properties, thus allowing application designers to choose which scenario fulfills his requirements and then which are the literature proposals that can be applied. On the other hand, the exhaustive classification of the different possible scenarios has allowed to identify some situations where the proposals that can be found in the literature do completely or efficiently solve the group access procedure.

This paper is organized as follows. Section 2 presents the different scenarios for group access in a distributed collaborative environment. In Section 3 we discuss the properties and constrains of the defined scenarios. Section 4 provides a literature review in order to identify which are the existing solutions for every different scenario. Section 5 presents the concluding remarks.

2 Group access scenarios identification.

In order to study the security issues related with group access control in peer-to-peer applications (or ad-hoc networking), we first identify the possible scenarios resulting from different levels of involvement of the peers within the group during the access process of a new member.

The access process can be split in two steps: registration and authentication, that can be defined as follows.

Registration: The process by which a new peer applies to be accepted into the group. During this process the new peer may receive any credentials (keys, passwords, tokens) that will be needed at later stages to prove he belongs to the group. It is assumed that registration is performed only once, and, if the process succeeds, the new peer will be considered a member of the group afterwards.

Authentication: The process by which a user connects to a group, proving he is one of its members. The previous registration process provides the needed evidences for the authentication procedure. In this environment we identify connection as the possibility to share some resources.

As we pointed out in Section 1, since we are restricted into peer-to-peer applications (or ad-hoc networking), registration and authentication must be performed by peers of the group without assuming any external party. For that reason it is useful to provide the following notation:

- Let $G = \{A_1, A_2, \cdots, A_n\}$ be the peers of the group G.
- Let B be the new peer who wants to access the group.
- Let $\Gamma^R = \{A_{i_1}, A_{i_2}, \cdots, A_{i_r}; i_j \in \{1, \cdots, n\}; \forall j = 1, \cdots, r\}$ be the registration structure within a group. That is, the set of r peers who are allowed to register a new peer.
- Let $\Gamma^R_B = \{A_{k_1}, A_{k_2}, \cdots, A_{k_p}; k_j \in \{i_1, i_2, \cdots, i_n\}; \forall j = 1, \cdots, p\}$ be the set of p peers who did register B, where it is obvious that $p \leq r$ and $\Gamma^R_B \subseteq \Gamma^R$ holds.
- Let $\Gamma^A = \{A_{l_1}, A_{l_2}, \cdots, A_{l_q}; l_j \in \{1, \cdots, n\} : \forall j = 1, \cdots, q\}$ be the set of q peers who may authenticate B.
- Let $\Gamma^A_B = \{A_{m_1}, A_{m_2}, \cdots, A_{m_t}; m_j \in \{l_1, l_2, \cdots, l_q\}; \forall j = 1, \cdots, t\}$ be the set of t peers who did authenticate B, where it is obvious that $t \leq q$ and $\Gamma^A_B \subseteq \Gamma^A$ holds.

Both the registration and authentication steps present several common issues and challenges that must be taken into account in order to evaluate the different scenarios we will present:

- Peer equality. Avoiding that some peer have more authoritative power than some other ones in the same group. In an ideal peer-to-peer environment, equality should be maximized.

- Availability. Since peer-to-peer networks are highly dynamic, the number of peers connected to the group in an specific instant may change very quickly over time, which may create situations where there are not enough peer available in order to let B enter the group.
- Acceptance policies. Enforcing some policy in order to decide whether a peer is accepted into the group. This issue is specially interesting in the registration scenario, since we start with no previous knowledge from B (in an authentication scenario we have some knowledge acquired during registration) and such policy must be agreed between all the members in the group.
- Collusion. To a certain degree covered by the previous issue, taking into account that under the case that some peers are compromised, it may be possible to leverage the acceptance policy in order to let any peer enter the group.

Since we are interested in the scenarios determined by the involvement of peers, we differentiate between two cases: **single-peer** and **collaborative**. The former assumes only one peer is needed in the process, that is $p = 1$ for registration and $t = 1$ for authentication. On the other hand, the collaborative case considers $p > 1$ and $t > 1$ respectively. Such distinction has been made because the specific properties of each case strongly impact the system and the security tools needed for every solution, as it is shown in Section 4.

In the next subsection the different scenarios for registration and authentication are described.

2.1 Registration scenarios

Based on the single-peer and collaborative distinction defined above, the possible scenarios for the registration process are summarized in Table 1.

	r = 0	$0 < r < n$	r = n
$\Gamma^R_B = \{A_i; \text{for some } \ A_i \in \Gamma^R\}$ case $p = 1$	1R	2Rs	3Rs
$\Gamma^R_B = \{A_{k_1}, \cdots, A_{k_p}; k_j \in \{i_1, \cdots, i_n\}; \forall j = 1, \cdots, p\}$ case $1 < p \leq r$	1R	2Rc	3Rc

Table 1. Registration Scenarios

Scenario 1R: This case, where $\Gamma^R = \emptyset$, is a degenerated case since $p \leq r$ and $r = 0$ and $p \geq 1$. This case accepts two different interpretations.

The first one considers the group G as a closed group, no registration process exists so no new peers may be registered. Only the initial peers inside the group will ever be part of it. Since there's no available registration process, both a collaborative effort or single-peer registration may be considered the same case.

The second interpretation is the opposite, and assumes that the group is completely open, no registration process is required. By default, anybody is part of the group and according to the previous registration definition, any peer may create its own credentials by himself, since nobody is responsible for registration. It is worth mention that, under this scenario, the concept of group as a segregate set of peers does not really exist, so it does not really make sense in a group access study, but it is listed for the sake of completeness.

Scenario 2Rs: In this scenario, only a subset of peers may register new ones, but each one of them may do it on its own ($p = 1$).

Scenario 3Rs: This scenario tries to keep equality between peers, by allowing every user in G to register a new peer without restrictions.

Collaborative scenarios. 2Rc and 3Rc: In both cases a minimum number of peers $p > 1$ must agree before registering B. Such strategy tries to minimize misbehavior from single malign peers (or compromised ones), since they are not able to register B alone.

The main difference between cases 2Rc and 3Rc is the fact that the latter does not make any distinction between peers, since all of them may register B ($r = n$). Furthermore, a limit situation is achieved when $p = r$ that means all peers in Γ^R must agree in registering new members.

2.2 Authentication scenarios

The authentication process allows B to prove his group membership and it will be performed after the registration process.

We divide the authentication scenarios using the same approach used in the registration process, that is single-peer cases and collaborative cases. However, since the authentication process is based on a previous registration procedure, the scenarios here are based on a three tiered approach (see Figure 1). Now we may take into account the set of peers responsible for registering B, Γ^R_B, when defining the set of authenticating peers.

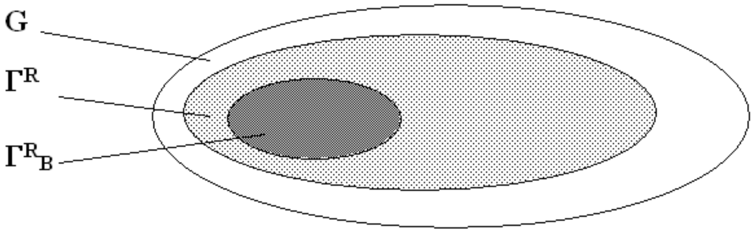

Fig. 1. Registration tiers

Despite the exact figure drawn, it is worth mention that we are not assuming only the case $\Gamma_B^R \subset \Gamma^R \subset G$ since equality may be possible ($\Gamma_B^R \subseteq \Gamma^R \subseteq G$).

Then for the authentication process, the possible scenarios are the ones described in Table 2.

	$t = 1$	$t > 1$
$\Gamma^A = \emptyset$	1A	1A
$\Gamma^A \subseteq \{A_1, \cdots, A_n\} = G$	2As	2Ac
$\Gamma^A \subseteq \Gamma^R$	3As	3Ac
$\Gamma^A \subseteq \Gamma_B^R$	4As	4Ac

Table 2. Authentication Scenarios

Scenario 1A: In this scenario there is no authentication process. That implies the registration process becomes completely useless and only makes sense under the 1R scenario. Again, this scenario may be interpreted in two completely different ways.

If we assume that the authentication process provides a mechanism for connecting to the group, then the lack of any authentication process means nobody may connect to the group, so the group becomes closed.

On the other hand, this scenario may be regarded as absolutely free access: any peer will be considered part of the group (being able to share resources) by default. Again, the concept of group itself vanishes.

Scenario 2As: In this scenario any peer may authenticate B by itself, thus providing maximum flexibility to the system by increasing its vulnerability to compromised peers.

Scenario 3As: In this case, only peers who were allowed to register new peers may authenticate B. This scenario will typically be based from a 2Rs or 2Rc registration case, where only a subset of peers, Γ^R, may register new ones ($r < n$). Otherwise, $\Gamma^R = G$, so we would be at scenario 2As.

Scenario 4As: In this scenario, we consider that only peers who took part in the registration process, Γ_B^R, may authenticate B.

It is interesting to note that this scenario highly depends from the registration case. Increasing the number of peers in Γ_B^R restricts the registration procedure but provides more flexibility to the authentication process since more peers will be available (notice that this is only true for the single-peer case where $t = 1$).

This scenario may be simplified under some circumstances. When $\Gamma_B^R = G$ in the 3Rc case, it becomes a 2As scenario, whereas in the case that $\Gamma_B^R = \Gamma^R$ in the 2Rc case, it becomes a 3As scenario.

Collaborative scenarios. 2Ac, 3Ac, 4Ac: In all these collaborative authentication scenarios $t > 1$ peers must agree before B is granted access into the group. The description is basically the same as the one for registration scenarios (see subsection 2.1).

Mixed scenarios: Each of the base scenarios previously defined may be combined producing a new subset of scenarios in which peers from explicitly different tiers may authenticate B before granting access to the group[1].

The different possibilities for mixed scenarios are shown in Table 3 where the + symbol will denote that the produced blended scenario is composed using the base scenarios indicated. For example, under scenario 3Ac+4As, B would be considered authenticated if $t > 1$ peers in Γ^R agree or $t = 1$ in Γ_B^R agrees.

In fact, mixed scenarios are equivalent to giving different levels of trust to the authenticating peers in each tier (similar to assigning weights).

However, these 20 mixed scenarios may be simplified, since some of the base cases are dependant because $\Gamma_B^R \subseteq \Gamma^R \subseteq G$ holds. In order to show this simplification, we will define the following terms for this section:

- Let t_1 be the number of peers who must agree in a 2A scenario in order to authenticate B ($t_1 = 1$ in 2As and $t_1 > 1$ in 2Ac).
- Let t_2 be the number of peers who must agree in a 3A scenario in order to authenticate B ($t_2 = 1$ in 3As and $t_2 > 1$ in 3Ac).

[1] Obviously, scenario 1A does not apply here.

2As+3As	2Ac+3As	2As+3Ac	2Ac+3Ac
2As+4As	2Ac+4As	2As+4Ac	2Ac+4Ac
3As+4As	3Ac+4As	3As+4Ac	3Ac+4Ac
2As+3As+4As	2As+3As+4Ac	2As+3Ac+4As	2As+3Ac+4Ac
2Ac+3As+4As	2Ac+3As+4Ac	2Ac+3Ac+4As	2Ac+3Ac+4Ac

Table 3. Initial Mixed Scenarios

- Let t_3 be the number of peers who must agree in a 4A scenario in order to authenticate B ($t_3 = 1$ in 4As and $t_3 > 1$ in 4Ac).

  Then, it holds that:

- Whenever $t_1 \leq t_2$, all mixed scenarios which include a 2A and 3A become a 2A scenario, since $\Gamma^R \subseteq G$.
- Whenever $t_1 \leq t_3$, all mixed scenario which include a 2A and 4A become a 2A scenario, since $\Gamma^R_B \subseteq G$.
- Whenever $t_2 \leq t_3$, all mixed scenario which include a 3A and 4A become a 3A scenario, since $\Gamma^R_B \subseteq \Gamma^R$.

  Then, Table 3 can be simplified into Table 4.

2As	2Ac+3As	2As	2Ac+3Ac*
2As	2Ac+4As	2As	2Ac+4Ac*
3As	3Ac+4As	3As	3Ac+4Ac*
2As	2As	2As	2As
2Ac+3As	2Ac+3As	2Ac+3Ac+4As*	2Ac+3Ac+4Ac*

Table 4. Simplified Mixed Scenarios

After this transformation, we can see that there are actually only 8 mixed scenarios: 2Ac+3As, 2Ac+3Ac, 2Ac+4As, 2Ac+4Ac, 3Ac+4As, 3Ac+4Ac, 2Ac+3Ac+4As, 2Ac+3Ac+4Ac. In fact, some of them can be further simplified for specific instances of t_1, t_2 or t_3, according to the previous rules. For example, a 2Ac+3Ac where $t_1 = 2$ and $t_2 = 4$ may be simplified to a 2Ac scenario (with $t_1 = 2$).

3 Scenario properties and constraints

Up to this point, we have defined the different available scenarios regarding group access control. In this section, we discuss the different properties of every scenario, as well as its constraints, in order to asses how they may impact the system.

Scenarios 1R and 1A, where no real access control exists, will be just briefly described, as they do not deserve much interest. Under a completely open approach there is neither real security nor groups. On the other hand, the opposite scenario, a closed one, is the least dynamic but provides tighter security. Both cases are the easiest to implement, and strictly speaking, keep peer equality.

Single-peer scenarios are the ones which offer maximum flexibility and responsiveness, at the cost of presenting a single point of failure. Only the corruption of one peer is needed to compromise the system.

In collaborative scenarios, for both registration and authentication, higher security is achieved since they are resistant to peer misbehavior or compromise. However, a protocol for collaborative agreement may be needed. Such protocol should be based in some kind of policy upon which agreement between peers is achieved. This extra protocol implies some overhead, then reducing responsiveness.

Another constraint in the collaborative environments is the fact that, under some circumstances, connection may become impossible unless a minimum number of peers are connected to the group, creating a sort of chicken-egg problem. There are two different approaches in order to minimize this constraint. The most straightforward one would be using collaborative parameters (p for registration, t for authentication) which are dynamic, allowing changes in its base requirements during group operations. This is specially critical in registration scenarios when the group itself is still establishing. Another possibility would be delegation upon other peers, which would temporally act as proxies of some number of peers in $\mathit{\Gamma}^R$ or $\mathit{\Gamma}^A$.

Taking another approach, the different scenarios may be evaluated from a peer equality point of view. In scenarios where $\mathit{\Gamma}^R = G$ or $\mathit{\Gamma}^A = G$ (3R, 2A respectively) peer equality is preserved. On the other hand, scenarios in which a restricted set of peers control group access (2R, 3A, 4A, where $\mathit{\Gamma}^R \subset G$ or $\mathit{\Gamma}^A \subset G$ respectively) lead to different degrees of inequality. Such degrees will require group policies in order to determine which peers belong to these restricted sets.

4 Security proposals for access control in distributed environments

In this section we provide a literature review that will allow us to determine which security schemes provide a solution for the different scenarios we defined. Due to the paper length constraints, we only take into account those proposals that use public key cryptography since these approaches allow to address other security issues such us privacy or data integrity. Symmetric key proposals such as those in [21] are not considered.

Obviously, scenarios 1R and 1A are not discussed, since in that case there is no real security scheme to be used (or its implementation is trivial).

4.1 CA based approaches

A widely accepted way to solve access control is using a certification authority (CA), which will provide digital public key certificates to the rightful members of the group. These certificates will serve as a credential for the authentication procedure. Different specific implementations are needed for each scenario.

Scenario 2Rs when $r = 1$ might be considered the most basic one, as it is the classical CA approach [4], with a single point of registration. In this scenario we must completely rely on the peer which provides CA operations. In order to allow B to be registered, the peer providing CA operations must be connected to the group, and this feature may not be desirable in a completely peer-to-peer environment. Despite this shortcoming, some peer-to-peer applications are based on this centralized model [5].

Scenarios 2Rs and 3Rs when $r > 1$ are exactly the same. In this case, we are implicitly stating that the CA is replicated in each one of the peers which may provide access (Γ^R in 2Rs and G in 3Rs) since every peer must be able to provide the same functionalities as a single CA. This scenarios greatly improve availability, but are extremely vulnerable, since now the points of failure are equal to the number of peers who may register B (r and n for each case, respectively), as stated in [6].

Scenarios 2Rc and 3Rc are the ones that offer a better trade off between availability and vulnerability, specially since we can choose different values for p and r for every specific case. Because of these reasons, this cases are the most used approach for group access in distributed environments [6–9]. Usually, the usage of threshold cryptography [10] is the way a collaborative registration procedure is solved. There are several ways to split a private key between several peers so it cannot be computed without the cooperation of minimum number of peers [11–13]. The main drawback of such approach is the rekeying problem. When a new peer joins Γ^R, the threshold shares must be recomputed which may be a problem in a highly dynamic group, although some efficient proposals exist [7].

In [6] a proposal for distributed CA-based access control is presented, where a set of special server peers provide CA capabilities. Choosing which peers will act as a server determines whether the scenario is 2Rc or 3Rc. The proposed solution also takes into account two other important aspects in a distributed CA. On one hand, it allows to operate in an asynchronous mode when not all peers which conform the CA are connected at the same time. On the other hand, it provides proactive security via share refreshing [14] in order to avoid that mobile adversaries may have a very long time to compromise enough peers.

Another similar approach, also based on a threshold cryptosystem, is provided in [7] and later improved in [8]. The main difference with the other proposals is that no special server peers are needed for CA operation, so this solution falls into the 3Rc scenario.

In all of these cases that use a CA approach, once the new peer has been provided with a certificate, it is easy to complete the authentication procedures for scenarios 2As, 3As or 4As, via a simple challenge-response protocol [15]. Unfortunately, under single peer authentication each peer becomes a single point of failure and is open to man-in-the-middle attacks. In [16] these problems are highlighted and the authors propose an authentication scheme based on a byzantine systems, as introduced by Lamport [17], in order to avoid them. The use of these collaborative proposals for authenticating a new peer would be encompassed within scenarios 2Ac, 3Ac and 4Ac.

Collaborative registration scenarios may also be complemented using byzantine systems. In this case, they add fault tolerance to a distributed CAs. An approach in that sense may be found in [9]. Again, this case is much nearer to a 2Rc scenario, since all peers are not equal.

Mixed scenarios are not considered in the literature. However, they could be solved in the same way as a collaborative scenario.

4.2 Self-organized based approaches

In the self-organized based approaches, B is accepted according on whether some of the peers in the group individually trust him and established trust relationships between the different peers in G. In this case, peers only represent themselves and never act as a higher level entity such as CA. Each peer manages its own individual keys and is able to sign certificates with them. This approach is the one used in the PGP model [18], based on a web of trust.

Literature in CA-based systems argues that self-organized based approaches are not scalable and they are focused on small groups of peers [7]. Nevertheless, we consider that self-organized based solutions represent an interesting approach since they allow to maximize peer autonomy. Furthermore, they also mitigate the bootstrap problems during the initialization phase in a distributed CA, at the creation of the initial private key that has to be distributed.

In [19, 20], the author's proposal is based on the verification of certificate chains, in order to assess whether B is part of the group. In this case, when B wants to register to G, any peer, A_i, can issue a certificate to B generated with A_i's private key. Reciprocally, B also generates a certificate to A_i. This process is named *certificate exchange* and is the way a trust relationship is created. At a later stage, any peer A_j in G may authenticate B by trying to find a trust relationship between A_j and A_i. This solution falls in scenarios 3Rs and 2As. Notice that scenario 2Rs works in the same way that 3Rs but we will only accept trust relationship between B and those peers in Γ^R. The rest of single-peer authentication scenarios, 3As and 4As, can be solved like 2As.

To our knowledge, there are no proposals that deal with collaborative scenarios in a self-organized based approach. For the registration process, 2Rc and 3Rc, it would typically involve that some number of trust relationships between peers in Γ^R or G respectively must exist before B is granted access. That means that at least p different peers must sign B's public key. It is worth mention that in this process there is no need for a collaborative agreement protocol between peers in Γ^R_B during registration since the establishment of every trust relationship can be created independently. That implies the registration procedure can be performed asynchronously.

In the case of authentication in collaborative scenarios, 2Ac, 3Ac and 4Ac, there is no distinction from the CA-based approach since trust relationship validation must be performed by $t > 1$ peers in Γ^A using an agreement protocol.

Mixed scenarios are considered the same case that collaborative scenarios since an agreement protocol is needed between peers of different tiers.

5 Conclusions and further research

In this paper we have presented an exhaustive description of the different possible scenarios for an access procedure in a peer-to-peer environment depending on the involvement of the peers during the registration process. Furthermore, we have discussed the main properties of every scenario from a performance point of view (availability, responsiveness, misbehavior tolerance,...) and also from a peer equality approach. Finally, we have provided a literature review of the main proposals in the field of access security for peer-to-peer and ad-hoc network. We have identified in which defined scenario can be classified each proposal.

Further research will be focused on providing efficient and complete solutions for those scenarios that are not sufficiently solved with the current available solutions. Furthermore, we should carefully deal with other group operations that impact on access control like for instance peer withdrawal from the group, which in a public key scenario basically means certification revocation.

Acknowledgements and disclaimer

This work is partially supported by the Spanish MCYT and the FEDER funds under grant SEG2004-04352-C04-04 PROPRIETAS-WIRELESS. The work described in this paper has been supported in part by the European Commission through the IST Programme under Contract IST-2002-507932 ECRYPT. The information in this document reflects only the author's views, is provided as is and no guarantee or warranty is given that the information is fit for any particular purpose. The user thereof uses the information at its sole risk and liability.

References

1. Hoeper, K., Gong, G.: Models of authentications in ad hoc networks and their related network properties. Technical report, Waterloo, Ontario, Canada (2004)
2. Zhang, Y., Zhang, D.: Authentication and access control in p2p network. In Minglu Li, Xian-He Sun, Q.D.e.a., ed.: Grid and Cooperative Computing: Proceedings of Second International Workshop, GCC 2003, Berlin, Springer-Verlag (2003) 468–470 Lecture Notes in Computer Science Volume 3032.
3. Aura, T., Mäki, S.: Towards a survivable security architecture for ad-hoc networks. In Christianson, B., Crispo, B., Malcolm, J.A., Roe, M., eds.: Security Protocols, 9th International Workshop. Volume 2467 of Lecture Notes in Computer Science., Springer-Verlag, Berlin (2002) 63–73
4. CCITT: The directory authentication framework. recommendation (1988)
5. Groove. http://www.groove.net
6. Zhou, L., Haas, Z.: Securing ad hoc networks. Technical report, Ithaca, NY, USA (1999)

7. Luo, H., Zerfos, P., Kong, J., Lu, S., Zhang, L.: Self-securing ad hoc wireless networks. In: ISCC '02: Proceedings of the Seventh International Symposium on Computers and Communications (ISCC'02), Washington, DC, USA, IEEE Computer Society (2002) 567
8. Luo, H., Zerfos, P., Kong, J., Lu, S., Zhang, L.: Providing robust and ubiquitous security support for mobile ad hoc networks. In: ICNP '01: Proceedings of the Ninth International Conference on Network Protocols (ICNP'01), Washington, DC, USA, IEEE Computer Society (2001) 251
9. Zhou, L., Schneider, F.B., Renesse, R.V.: Coca: A secure distributed online certification authority. ACM Trans. Comput. Syst. **20** (2002) 329–368
10. Desmedt, Y.G., Frankel, Y.: Threshold cryptosystems. In: CRYPTO '89: Proceedings on Advances in cryptology, New York, NY, USA, Springer-Verlag New York, Inc. (1989) 307–315
11. Cocks, C.: Split knowledge generation of rsa parameters. In: Proceedings of the 6th IMA International Conference on Cryptography and Coding, London, UK, Springer-Verlag (1997) 89–95
12. Boneh, D., Franklin, M.: Efficient generation of shared rsa keys. J. ACM **48** (2001) 702–722
13. Frankel, Y., MacKenzie, P.D., Yung, M.: Robust efficient distributed rsa-key generation. In: PODC '98: Proc. of the seventeenth annual ACM symposium on Principles of distributed computing, New York, NY, USA, ACM Press (1998) 320
14. Herzberg, A., Jakobsson, M., Jarecki, S., Krawczyk, H., Yung, M.: Proactive public key and signature systems. In: CCS '97: Proc. of the 4th ACM conference on Computer and communications security, New York, NY, USA, ACM Press (1997) 100–110
15. A.J. Menezes, P.v.O., Vanstone, S.: Handbook of Applied Cryptography. CRC Press (1996)
16. Pathak, V., Iftode, L.: Byzantine fault tolerant public key authentication in peer-to-peer systems. Technical report (2005)
17. Lamport, L., Shostak, R., Pease, M.: The byzantine generals problem. ACM Trans. Program. Lang. Syst. **4** (1982) 382–401
18. Garfinkel, S.: Pgp: Pretty good privacy. (O'Reilly and Associates Inc.)
19. Capkun, S., Buttyn, L., Hubaux, J.P.: Self-organized public-key management for mobile ad hoc networks. IEEE Transactions on Mobile Computing **2** (2003) 52–64
20. Hubaux, J.P., Buttyn, L., Capkun, S.: The quest for security in mobile ad hoc networks. In: MobiHoc'01: Proc. of the 2nd ACM int'l symposium on Mobile ad hoc networking & computing, New York, USA, ACM Press (2001) 146–155
21. Michael Steiner and Gene Tsudik and Michael Waidner: Key Agreement in Dynamic Peer Groups. In: IEEE Trans. Parallel Distrib. Syst., Piscataway, USA, IEEE Press (2000) 769–780