An assessment of Key Management using Certificateless Cryptography in Mobile adhoc Network

[1]R.Rajesh, [2]Dr.K.Ramakrishnan
[1]School of Information Technology/ Research Scholar/ Madurai KamarajUniversity, Madurai, India
[2]Professor and Head, Department of Computer science, Madurai Kamaraj University, Madurai, India

Abstract

A mobile ad hoc network is an independent group of mobile devices that interconnect with each other over wireless associations and cooperate in a dispersedwaywith the purpose of providing the required network functionality in the lack of a stable structure. Certificateless public key cryptography is involved here not simply to eradicate the necessity for certificates, but also to maintain the required properties of identity-based key management methods without the integral key escrow problem.By means of the modern acceleration in research into Identity-based Public Key Cryptography (ID-PKC), we deliberate this a suitable moment to relate and contrast ID-PKC with more Public Key Infrastructures (PKI). Due to the resemblance in the nature of both methodologies, we purpose to recognize the difference between the features of them.Fundamentally, certificateless cryptography depends onconcerning the public key cryptography and ID-based cryptography. In this effort, we accept this methodadvantage over MANET and simulate the scheme with AODV to assess the network efficiency.

Keywords: *Mobile ad hoc network, Certificateless public key cryptography, Identity-based Public Key Cryptography, Public Key Infrastructures.*

I. INTRODUCTION

An ad hoc network is a collection of independent nodes that communicate with each other by creating a multi-hop wireless network. The property of not depend on the provision from any stable infrastructure creates it valuable for a wide range of applications. However, ad hoc network affords a great flexibility for creatingcommunications; it also fetches a lot of research tasks. One of the essential issues is the security due to all the features of these networks, such as the susceptibility of the wireless associates, the restricted physical security of each node and the vigorouslyvarying topology. Key management service is animportant security problem because it is the vital assumption of many other security facilities.As a consequence of MANET's non-centralized infrastructure and extremely dynamic characteristics, routing is acrucial part of this network. Lackingof routing, devices are unable to join to each other, and the network becomes crippled. Route Paths may turn out to beworthless at any second, which may be instigated by a slight movement of one node.Since ad hoc networks are highly susceptible to several security threats as a result of its essential characteristics, such as open medium, lack of fixed central structure, vigorouslyvarying topology and inhibited resource, traditional key management methods based on public key infrastructure (PKI) is not directly relevant to ad hoc networks.

Recent research works in key management are chiefly based on traditional PKI and identity-based public key cryptography (ID-PKC). These methods based on traditional PKI use a partly distributed or a fully spreaded certificate authority (CA) to dispute and achieve public key certificates. Though, the resource-constrained ad hoc networks influenceisincapable to provide the moderatelycomplex certificate management, containing revocation, storage and circulation, and the computational costs of certificate verification.On the other hand, ID-PKC wants a reliable private key generator (PKG) which produces the private keys of the units using their public keys and a master secret key. Consequently, the reliance on the PKG who know all consumers' private keys predictably causes the key escrow problem to the ID-PKC systems. The CL-PKC does not need the use of certificates and does not have the integrated key escrow feature of ID-PKC. It is a prototype for the use of public key cryptography that is in-betweencustomary PKI and ID-PKC. The Key Generation Centerprovides a user with a partial private key that then it calculates from the consumer'suniqueness and a master key.

II. RELATED WORK

In [5] Yanchao Zhang provides Securing Mobile Ad Hoc Networks with Certificateless Public Keys. This paper studies key management, a fundamental problem in securing mobile ad hoc networks (MANETs). We present IKM, an ID-based key management scheme as a novel combination of ID-based and threshold cryptography. IKM is a certificateless solution in that public keys of mobile nodes are directly derivable from their known IDs plus some common information. IKM features a novel construction method of ID-based public/private keys, which not only ensures high-level tolerance to

node compromise, but also enables efficient network-wide key update via a single broadcast message. They also provided general guidelines about how to choose the secret-sharing parameters used with threshold cryptography to meet desirable levels of security and robustness. The advantages of IKM over conventional certificate-based solutions are justified through extensive simulations. Since most MANET security mechanisms thus far involve the heavy use of certificates, we believe that our findings open a new avenue towards more effective and efficient security design for MANETs.

In [8] Jun Zheng focused on a novel detective and self-organized certificateless key management scheme in mobile ad hoc networks. In this system, the mobile ad-hoc network is an infrastructure-free and dynamic kind of network. For its mobility and self-organized features, it is a great challenge to ensure the security of the network. And the basic aspect of providing the security is managing the encrypting keys. The current key management schemes mainly depend on certificates and identity-based key encryption. Schemes based on certificates suffer from huge computational costs of certificates verification while the identity-based schemes lead to key escrow problem. In this paper, we propose a novel detective and self-organized key management by combining certificateless public key cryptography and threshold secret share scheme, which can completely perform key generation by nodes themselves and pick up the compromised node.

III. CERTIFICATELESS PUBLIC KEY CRYPTOGRAPHY

In CL-PKC, the KGC provides a user with a partial secret key which the KGC calculates from the user's identity and a master key, and then the user syndicates its partial secret key and the KGC's public considerations with some secret information to produce its authentic secret key and public key separately. In this manner, a user's secret key is not accessible to the KGC.

A certificate less cryptosystem has three key generation algorithms: Master KeyGen, PartialKeyGen, UserKeyGen. All of them are polynomial-time and may be randomized.

1. MasterKeyGen (Master Key Generation): On input 1^K where k ϵ N is a security parameter, it generates a master public/secret key pair (*mpk,msk*). Let MPK(*k*) be set of all possible master public keys generated by MasterKeyGen(1^K). Without loss of generality, we assume that it is computable to determine if a master public key *mpk* is in MPK(*k*).

2. PartialKeyGen (User Partial Key Generation): On input *msk* and user identity ID ϵ {0, 1}*, it generates a user partial key partial key.

3. UserKeyGen (User Key Generation): On input *mpk* and user identity ID, it generates a user public/secret key pair (*upk, usk*).

A certificateless encryption (CL-ENC) scheme has two polynomial-time algorithms in addition to the three key generation algorithms: CL-Encrypt and CL-Decrypt. Similar to the case of signature schemes, both of these algorithms may be randomized but usually the second one is not.

1. CL-Encrypt: On input *mpk*, user identity ID, user public key *upk*, message m, it returns a ciphertext c.
2. CL-Decrypt: On input user secret key *usk*, user partial key partial key and cipher text c, it returns a message m.

Cipher Correctness. For all k ϵ N, mϵ {0, 1}*, ID ϵ{0, 1}*, if (*mpk,msk*) ←MasterKeyGen (1^K), partial key ←PartialKeyGen(*msk*, ID), (*upk*, usk)←UserKeyGen (mpk, ID), then we require that

m← CL-Decrypt(usk, partial key, CL-Encrypt(*mpk*, ID, *upk*,m)).

Key management can be defined as a conventional of techniques and processes to maintain the formation and preservation of keying relationships between certified parties. A keying relationship is the process by which system nodes share entering material to be used by cryptographic mechanisms. The entering material can comprise public/private key pairs; secret keys, initialization factors, and non-secret considerations associate key management in several illustrations. Key management should also explain methods to repeal keys from negotiated nodes and update keys from non-compromised ones.

Key management for MANETs isessential to deal with dynamic topology that is self-organized and distributed. It must also fulfill some requirements are as follows as

- Not consuming a single point of failure
- Existenceof compromise-tolerant; that is, the negotiation of a assured number of nodes does not have impact the security between non-compromised nodes
- Being able to resourcefully and firmlyinvalidate keys of negotiated nodes and update keys of non-compromised ones
- Being competent in expressions of storage, calculation, and communication

In this key management process, primarilyfocused on some significantstructuresthat is the differences between PKI and ID-PKC by inspecting the way in which they manage keys. Public Key Infrastructures are presently the principal

means of positioning asymmetric cryptography. Due to the essential public nature of the encryption or authentication keys, the reliability of the public keys is typicallythreatened with a certificate. The validity of the information that is used as the identity or identifier is now essential to the security of the system. In a PKI, the certificate is supposed to determine the reality of classifying information. In Identity/Identifier based Public Key Cryptography, since a private key may be produced after the public key, the Trusted Authority may not have authenticated the authenticity of the information connecting to the key pair earlier to the public key's use.

IV. PROPOSED SYSTEM

On the originof several studies, the key management procedure is characterized into three major consecutives. They are the generation of public keys, generation of private keys and revocation of keys.

A. Generation of Public Keys

The public keys are produced in the key management process of two progressions such as PKI and ID-PKC. The influences that are produced by these keys have been established in the following:

- In the Public Key Infrastructures, the certifiedkey is produced at the same time as the private key. This restricts the formation of the public key to either the CA or the user. Within an ID-PKC, the public key can be produced by any client within the system. Furthermore the public key can be selected by any customer in the system.
- Within a PKI, the keys are producedearlier to the issuance of a certificate. The authority of the binding between the public and private keys must be tested by the CA before dispensing the certificate. Within an ID-PKC, because of the split-up between generation of isolated and public keys, a public key can be caused at a different time to the isolated key and hence also at a different time to the endorsement of the issuance of the private key.
- Within a PKI, the public key is either generated at the CA or by a process which the client deems to be trustworthy. In an ID-PKC, the public key is generated at the site of the client who wishes to use the public key.
- Within a PKI, the public key usually results from a process that makes use of a random secret input to generate both public and private keys. In an ID-PKC, the public key is generated from public information.

B. Issues In Generating Public Keys

In ID-PKC, the creation public keys are different from the creation private keys for the reason that it mainly focuses on the public information that is acquired from the valid sources. The encryption method is ready to yield over the full comeback of the sender information but it does not problem about the receiver and the decrypted text. The authentication key is produced from the signer's identity. This can be agreed out either by the signer, who then attributes the verification key to the engaged message, or by the verifier who calculates it at the time of verification. In PKI, the customer would essential to know the public key that was associated to the private key to be used to decrypt the message in progresstypically the decryption key assured to the recipient's identity. In a PKI, the authentication key is generated at the same time as the authorizing key and the certificate comprehending the verification key often attends the signature. Inside a signature scheme a public key is only of any use when confirming a signature, which indirectlyneeds the former generation of a private key.

C. Methodology

The first certificateless public key encryption scheme was proposed by Al-Riyami and Paterson. We incorporate their work and adopt it to MANET key management with CL-PKE. The scheme is as follows:

1) Setup

We assume IG is a Bilinear Diffie-Hellman parameter generator and k is the security parameter for the system. This algorithm has four steps.

1. Run the IG generator on an input k, it outputs (B1, B2, r) where B1 and B2 are groups of prime order p. e: $B1 \times B1 \rightarrow B2$ is a pairing.

2. Choose an arbitrary generator $S \in B1$.

3. Select a master private key *msk* uniformly at random from $Z*P$ and set $S0 = msk \times S$.

4. Choose four cryptographic hash functions $H1 : \{0, 1\}* \rightarrow B1$, $H2 : B2 \rightarrow \{0, 1\}$, $H3 : \{0, 1\}m \times \{0, 1\}m \rightarrow Z*p$ and $H4 : \{0, 1\}l \rightarrow \{0, 1\}m$, here l will be the bit length of plaintexts.

The master public key mpk = (B1,B2, r, m, S, S0,H1,H2,H3,H4). The master private key is $msk \in Z*p$. The message space is $M = \{0, 1\}m$ and the ciphertext space $C = \{0, 1\}2m \times B1$.

2) Extract Partial-Private Key

This algorithm takes as input an $ID \in \{0, 1\}*$ and carries out the following steps.

1. Compute $\mathbb{Q}ID = H1(ID) \in B1$.

2. Output the partial private key dID = msk× ℚID ∈ G∗1.

Any user can verify its partial secret key by checkinge(dID, P) = e(ℚID, ℙ0).

*3) **Encryption***

For a message $msg \in M$ and an identity ID $\in \{0, 1\}^*$with its public key $pk_{ID}=<X_{ID},Y_{ID}>$, the encryption algorithm takes as follows:

1. Check the public key by $e(X_{ID}, P_0) = e(Y_{ID}, P)$. If the result is negative, abort the encryption and output an error symbol.

2. Compute $QID = H1(ID) \in B*1$.

3. Choose a random number $\sigma \in \{0, 1\}m$.

4. Set $r = H3(\sigma,msg)$

5. Compute and output ciphertext:
$c = <rP, \sigma \oplus H2(e(QID,YID)r), msg \oplus H4(\sigma) >$

*4) **Decryption***

Suppose $c =<U, V, W > \in C$. To decrypt this cipher text with private key *skID*:

1. Compute $V \oplus H2(e(sk_{ID},U)) = \sigma'$.

2. Compute $W \oplus H4(\sigma') = msg'$.

3. Set $r'= H3(\sigma' ,msg')$ and test if U = r' P. If not, output an error symbol and reject the Cipher text.

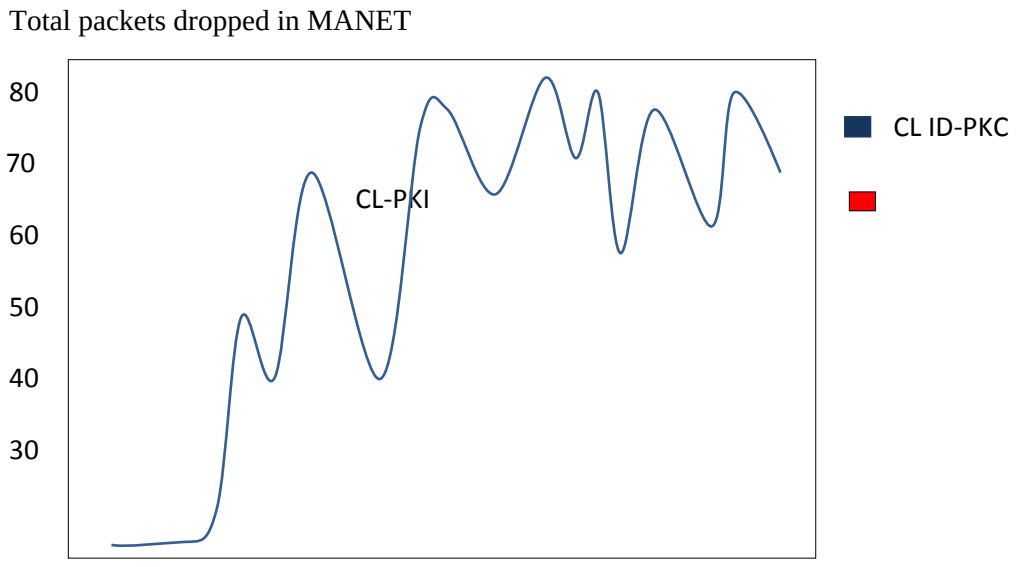
4. Output *msg' as* the decryption of *c*.

V. SIMULATION AND DISCUSSION

In the simulation process, the node in the network mainly concentrates on the continuous movement and the network is not stable in nature. This flexibility model describesthat node will prefercertain random waypoint in the wireless domain and move en route forthe waypoint with a velocity arbitrarily picked between 0 to10m/s. Whena node grows to its destination, it will break for 1 second and then move to the following waypoint. The effortreplicates till the end of model.When the simulation starts, there is an instigation time for 100 seconds, during which time; no movement is produced, except that between nodes and the KGC. Subsequently, the KGC goes disconnected and each normal node will produce back ground traffic, which is 1 packet per second in our simulation. Once a packet expected/produced, it takes 0.04 second for a node to development it.In this simulation, assume that the network propagation delay is 0ms, which means once the partial secret key is generated; it will be sent to the correspondent node immediately.

Table.1: Results for Simulation

Time (ms)	Packets dropped		Average traffic	
	ID-PKC	PKI	ID-PKC	PKI
0	0	0	0	0
5	1	10	70	50
10	30	15	40	30
15	65	18	35	20
20	80	8	30	20



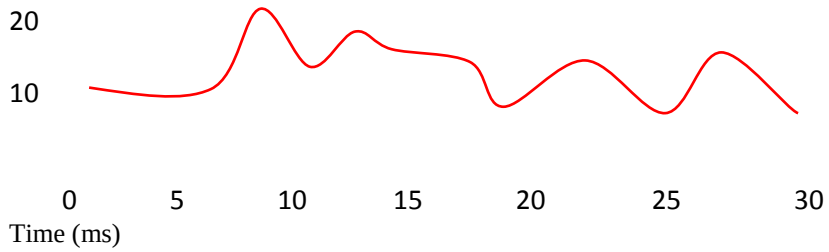


Fig.1: Total no. of Packets Dropped in MANET for ID-PKC and PKI

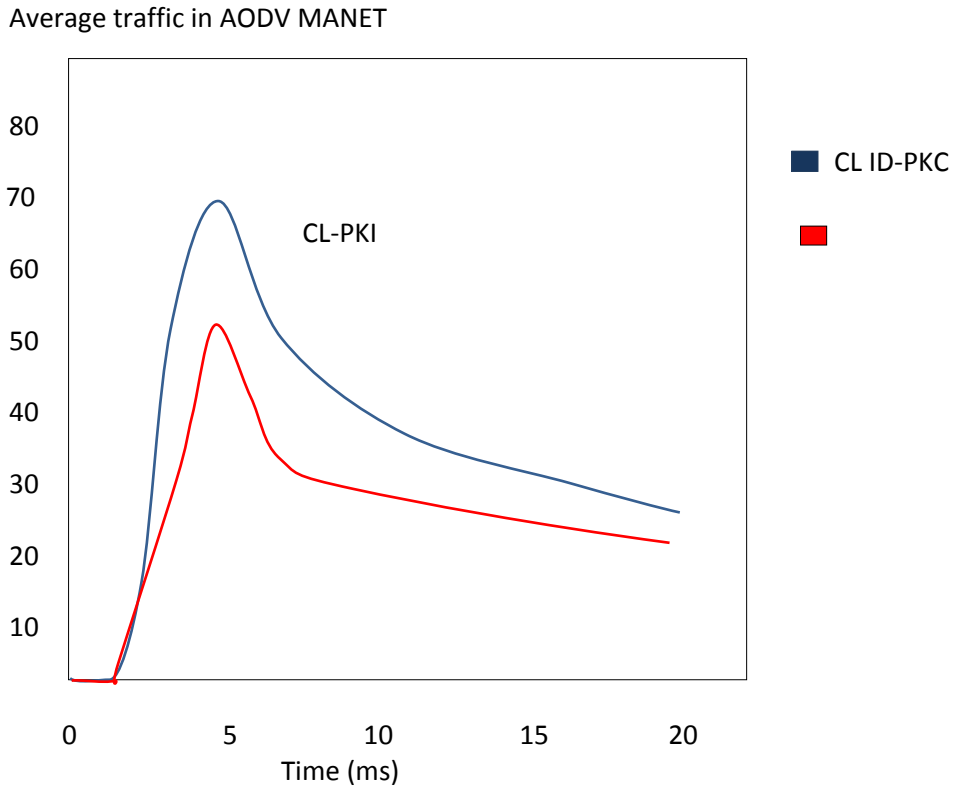


Fig.2: Traffic in AODV MANET in ID-PKC and PKI

VI. CONCLUSION

Key management is one of the most essential technologies for security of ad hoc networks. This paper suggests a novel approach for key management using certificate less public key cryptography. Although research interest in ID-PKC is very strong at the moment, it is a relatively new technology in comparison to PKI. In our article, we have sought to explore what separates ID-PKC from PKI. Our decision, certainly made in the framework of little or no commercial distribution of ID-PKC systems, is that there is scarce to isolate the two. Feasibly the significant input when determining whether to agree PKI or ID-PKC is the different way in which the two technologies logically create and confirm rights and keys. This paper offered the design and the reproduction of a key distribution scheme over mobile ad hoc network, based on the certificate less cryptography and public key generation. In this work, we have efficaciously distributed public/secret keys for users without providing certificates. This system also confirms that system can work on self-organized networks after the simulation. From the simulation, it is set up that our scheme works particularly well in a small size of MANET.

REFERENCES

[1] W. Diffie and M. Hellman, New directions in cryptography,IEEE Transactions on Information Theory, IT-22(6):644-654, 1976.

[2] Yanchao Zhang, Wei Liu, Wenjing Lou, Yuguang Fang, and Younggoo Kwon," AC-PKI: Anonymous and Certificateless Public-Key Infrastructure for Mo-bile Ad Hoc Networks , " IEEE 0-7803-8939, May 5, 2005.

[3] YANG Ya-tao, ZENG Ping, FANG Yong, CHI Ya-Ping," A Feasible Key Management Scheme in Adhoc Network , " Eighth ACIS International Conference on Software Engineering, Artificial Intelligence, Networking, and

Parallel/Distributed Computing, IEEE, 0-7695-2909,July 7, 2007.

[4] Zhenfei Zhang, Willy Susilo and Raad,"Mobile Ad hoc Network- Key Management with Certificateless Cryptography", IEEE, 978-1-4244-4242, 2008.

[5] MengboHou and QiuliangXu,"An Efficient and Secure One-Round Authenticated Key Agreement Protocol without Pairings," IEEE, 978-1-61284-774, Nov., 2011.

[6] S. Tapaswil andVirendra Singh Kushwah, "Securing Nodes in MANETs Using Node Based Key Management Scheme," International Conference on Advances in Computer Engineering, IEEE, 978-0-7695-4058, Dec., 2010.

[7] Eduardo Da Silva, Aldri L. Dos Santos, and Luiz Car-los P. Albini," Identity-based Key Management in Mobile Ad hoc Networks: Techniques and Applications," IEEE Wireless Communications, 1536-1284, Aug. 2008.

[8] K. Sanzgiri, B. Dahill, B.N. Levine, C. Shields, and E.M. Belding-Royer,"A secure routing protocol for ad hoc networks" In Proceedings of 10th IEEE InternationalConference on Network Protocols, Paris, France, pp. 78- 87, 2002.

[9] J.P. Hubaux, L. Buttyan and S. Capkun,"Self-organized public-key management for mobile ad hoc networks"IEEE Transactions on Mobile Computing, Vol. 2, No.1, pp. 52{64, 2003.

[10] S.S. Al-Riyami and K.G. Peterson,"CBE from CL-PKE: a generic construction and efficient schemes" In Public Key Cryptography-PKC 2005, Lecture Notes in Computer Science, Vol.3386, Springer-Verlag, Berlin, pp.398{415, 2005.

[11] B. C. Hu, D. S. Wong, Z. Zhang, and X. Deng, "Key replacement attack against a generic construction of certificateless signature" In Information Security and Privacy: 11th Australasian Conference, ACISP 2006, pages 235–246, Springer-Verlag, 2006.

[12] B. Libert and J.J. Quisquater, "On constructing certificateless cryptosystems from identity based encryption" In 9th International Conference on Theory and Practice in Public Key Cryptography (PKC 2006), pages 474–490, Springer, 2006.

[13] Rakesh Chandra Gangwar and Anil K. Sarje, "Secure and Efficient Dynamic Group Key Agreement Protocol for an Ad Hoc Network," IEEE, 1-4244-0731, June 1, 2006.

[14] Z. Zhang, D. Wong, J. Xu, and D. Feng, Certificateless public-key signature: Security model and efficient construction, In 4th International Conference on Applied Cryptography and Network Security (ACNS 2006), pages 293–308, Springer, 2006.

[15] D. H. Yum and P. J. Lee,"Generic construction of certificateless signature. In Information Security and Privacy: 9th Australasian Conference, ACISP 2004, pages 200–211, Springer-Verlag, 2004.

[16] YANG Ya-tao, ZENG Ping, FANG Yong, CHI Ya-Ping," A Feasible Key Management Scheme in Adhoc Network , " Eighth ACIS International Conference on Software Engineering, Artificial Intelligence, Networking, and Parallel/Distributed Computing, IEEE, 0-7695-2909,July 7, 2007.

[17] MengboHou and QiuliangXu," An Efficient and Se-cure One-Round Authenticated Key Agreement Protocol without Pairings, " IEEE, 978-1-61284-774, Nov., 2011.

[18] Chen Yixiang," Certificateless Key Agreement Protocol , " IEEE, 978-1-4244-5895, Dec., 2010.

[19] A. Khalili, J. Katz, and W.A. Arbaugh,"Toward secure key distribution in truly adhoc networks", In Proceedings of 2003 Symposium on Applications and the InternetWorkshops, Orlando, FL, USA, pp: 342{364, 2003.

[20] H. Deng, A. Mukherjee, and D. Agrawal, "Threshold and identity-based key management and authentication for wireless ad hoc networks, In Proceedings of International Conference on Information Technology: Coding and Computing, Las Vegas, NV, USA, pp. 107{111, 2004.

[21] L. Chen, K. Harrison, D. Soldera, and N.P. Smart, "Applications of multiple trust authorities in pairing based cryptosystems" In G.I. Davida, Y. Frankel, and O. Rees, editors, Infrastructure Security, International Conference, InfraSec, volume 2437 of LNCS, pages 260-275. Springer-Verlag, 2002.