This full text paper was peer reviewed at the direction of IEEE Communications Society subject matter experts for publication in the IEEE CCNC 2006 proceedings.

Performance Evaluation of a Distributed OCSP Protocol Over MANETs

K. Papapanagiotou, G. F. Marias, P. Georgiadis
Dept. of Informatics and Telecommunications
University of Athens
Athens, Greece
conpap@di.uoa.gr, marias@mm.di.uoa.gr,
georgiad@di.uoa.gr

S. Gritzalis
Dept. of Information and Communication Systems Engineering
University of the Aegean
Karlovassi, Samos, Greece
sgritz@aegean.gr

***Abstract*— Several methods that rely on public or private cryptographic systems have been proposed for trust establishment in mobile ad hoc networks (MANETs). Such methods aim to provide end-entity authentication, communications integrity and privacy. When public key certificates schemes are deployed in MANETs, they must be accompanied by efficient mechanisms for certificate revocation and validation. In this paper we address this issue, and a distributed, on-demand, OCSP-based scheme is adapted to be applicable over MANETs. This scheme, called ADOPT, uses caches of OCSP responses that are distributed and stored on intermediate nodes. ADOPT takes into account the status of intermediate nodes, such as network topology, energy thresholds, and connectivity, to materialize the caching of OCSP responses. This paper uses different MANET con-figurations to evaluate the efficiency of ADOPT. The simulation results show that ADOPT manages to rapidly identify and locate the status of a certificate without introducing significant communication or storage costs.**

Keywords-OCSP; MANETs; certificate status information; caching

I. INTRODUCTION

Autonomous Ad hoc Networks (AANs) are dynamic, self-configured, peer-to-peer networks. They consist of nodes that are responsible for their creation, operation and maintenance in an absence of a central authority. AANs are referenced to as "fully self-organized" [12], whilst the IEEE uses the term Independent Basic Service Set (IBSS) [13] [14]. In addition, CANs (Connected Ad hoc Networks) offer extension of terrestrial, wired infrastructures, such as the Internet. In such architectures, nodes that maintain a physical connection with the wired network act as relays, offering access to nearby nodes, extending the coverage area. For the IEEE 802.11 standard, CANs are referred to as Extended Service Set (ESS) [13]. An ad hoc network, by definition, is dynamic: nodes constantly join or leave the network and the mobility of the nodes alters the network topology. Additionally, network communications are open, since the transfer medium is the unlicensed electro-magnetic spectrum. In such a dynamic and open environment, selfish and malicious entities can attack on all fronts, aiming to violate information messages' confidentiality and integrity, entities' authenticity, network's robustness and nodes' availability. Flooding and sleep deprivation torture [1] are techniques commonly used by malicious nodes. Passive eavesdropping, sinkhole, wormhole attacks, active impersonation and Sybil attacks [2] might also be materialized. To prevent attacks on the network performance, to preserve entities' authentication and to ensure privacy and integrity of messages, several proposals that rely on public key cryptography and certificates have been made. Public key certificates require the existence of a Certification Authority (CA) for the issuance, distribution, renewal, revocation and validation of entities' public keys. For MANETs the CA has to be online in order to revoke issued certificates, since a private key might be com-promised, or a node might be no longer trusted.

When digital certificates are used, the nodes need to hold CA's public key to validate the signatory. In any case, the binding between the ad-hoc entity and its public key, and the validation of this binding should be provided online, when requested. Providing status information of certificates is essential and has received much attention in recent years for traditional networks [11]. On the other hand, MANET nodes often have limited computational capability and power supply. Thus, any certificate status information (CSI) scheme should take into account these limitations, and avoid the creation, distribution and processing of computationally heavy lists, such as Certificate Revocation Lists (CRLs) [16]. Moreover, due to mobility, entities that provide CSI should be selected carefully, since peers require high availability of these nodes, whilst the avoidance of CSI flooding is essential for bandwidth saving reasons.

In this paper we discuss and evaluate a scheme that we have already proposed, referred to as ADOPT (Ad-hoc Distributed OCSP for Trust, [20][21]). ADOPT is based on a distributed version of the Online Certificate Status Protocol (OCSP), applicable to MANETs. It utilizes caches of OCSP responses to examine certificates' validity. OCSP caches are distributed and stored on intermediate nodes, avoiding the exchange of extended certificate status lists. These caches, stored on nodes with specific characteristics, such as energy autonomy and cellular or WLAN connectivity, are updated dynamically. A node uses an on-demand protocol to find the closest OCSP cache that is able to provide the status of the requested, peer's certificate. This paper evaluates alternative

1-4244-0086-4/06/$20.00 ©2006 IEEE.

caching approaches of the ADOPT, to enable the revision and distribution of up-to-date OCSP responses in AANs and CANs.

The structure of this paper is as follows: First we provide a survey of the proposed certificate-based trust architectures in MANETs. We discuss existing solutions for certificate revocation in MANETs that rely on CRLs. We also briefly describe OCSP and its advantages compared to CRLs. Subsequently, we present the proposed ADOPT scheme. In section 4 we define the simulation environment and provide the performance assessment of the ADOPT frame-work. Finally, we provide some concluding remarks.

II. CERTIFICATE STATUS VALIDATION SCHEMES IN MANETS

Many of these solutions that rely on public key certificates suggest a way of revoking certificates and disseminating the revocation information in the network. In this section we examine some of these solutions, focusing on the method they propose for certificate revocation. We also present OCSP and its advantages, compared to CRLs.

In AANs, the main concern for the deployment of a centralized CA is that this approach produces a single point of failure. The accessibility of the CA entity, due to nodes' mobility, the availability of the node's resources (e.g., battery) that accommodate the CA, and the savage when this node is impersonated, attacked or even compromised, are some potential issues of a single CA scheme. Zhou and Haas have proposed a distributed key management scheme, based on threshold cryptography [3]. In [4], the CA functions are distributed through a threshold secret sharing mechanism, in which each node holds a secret share and multiple nodes in a local neighborhood jointly provide complete services. An online CA service in MANET that is based on threshold cryptography, called MOCA, is described in [5]. In [6] GSM/GPRS technologies are proposed, enabling the nodes to access these CA services. An off-line CA is considered in [7] to control an ad hoc network of mobile nodes. This CA decides which nodes can join the network, and assigns a unique identity to each one. In MANETs, digital certificates and signatures are employed to protect both routing messages as well as data packet forwarding. Secure routing protocols, such as ARAN [8], SAODV [9], and for-warding modules, such as TRM [10], involve CAs.

In MOCA [5], at least k out of n MOCA nodes have to agree in order for a certificate to be revoked. A MOCA node may generate a "revocation certificate" which contains a certificate which is revoked. This is signed with its key share and then broadcasted to the network. A node that receives at least k partially signed revocation certificates can construct the full revocation certificate. The list of revoked certificates can be stored at any node of the network, possibly at the MOCA servers, specially designated nodes or every node in the MANET. MOCA, how-ever, does not specify a protocol for certificate validation. Moreover, flooding the network with partially signed revocation certificates creates an unnecessary overhead, which, according to [5], is not a drawback as revocation should be a rather rare event. In ARAN [8] when a key is revoked the trusted server broadcasts a message in order to notify all the nodes of the network. Each node receiving the revocation message rebroadcasts it and thus, eventually all nodes get informed. This, rather simple, approach suffers from several drawbacks. For example, a malicious node in the network may choose not to propagate the revocation message. Dormant nodes may cause network partitioning as they won't be able to forward revocation messages. Moreover, they also need to get informed about revoked keys as soon as they become again active nodes in the network. Consequently, a significant amount of time may be needed to inform all the nodes participating in the network of the newly revoked keys. J. Cheambe et al. [6] propose a secure authentication scheme for MANETs. In their model, nodes can communicate with a CA by out of band means, for example using a GPRS bearer. Each node has a unique, factory-installed, pair of keys. These keys are revoked by the CA which also issues and distributes CRLs, using a simple authentication and communication procedure. When two nodes wish to mutually authenticate each other's certificate they exchange, among others, the latest CRL they have. New CRLs are flooded in the network. Many issues concerning this scheme, such as the exact mechanism of CRL distribution, are not described in detail. In addition the communication link to the CA might not always be available and thus, CRLs may become out of date. Crepeau and Davis [15] describe a certificate revocation scheme designed for MANETs. Nodes already have a certificate issued by a CA before entering the network. The scheme is actually a protocol based on accusations. Each node can accuse inconsistent nodes. Accusation information is broadcasted to the network. When the majority of the nodes in the network accuse a specific node, its certificate is revoked. Tables that include revoked certificates are delivered to each new node that enters the network. Although the accusations scheme is well designed there exist similar open issues as with [6], mostly concerning the dissemination and freshness of revocation information.

To the best of our knowledge, none of the so far proposed schemes uses OCSP for CSI in MANET. OCSP is a protocol involving requests and responses that provide the current status of one or more certificates [17]. A client can send a request to a server (usually called OCSP Responder) asking for information on the status of one or more certificates. This request contains a reference to the queried certificate(s) (certID). The server responds with a signed message that contains the status of the referenced certificate(s) and time information: the time when the OCSP responder last updated the status information about the certificate (lastUpdate), the time when the message was generated (producedAt) and the time when the responder will update again the status in-formation (nextUpdate).

Arnes discusses the advantages of OCSP over CRLs or other offline methods for CSI in [22]. CRLs grow bigger with time and become very large. MANET nodes have limited network, processing and memory resources. It is, therefore, inefficient to periodically broadcast to the network or download a revocation list, instead of propagating small OCSP responses. OCSP is a client-server protocol which can be initiated on demand, when a node needs to verify the validity of a certificate. Thus, there is no waste of valuable network resources and energy for distribution of CRLs. When CSI availability is an issue, as in MANETs, then OCSP performs

better [11]. In a distributed version of OCSP, several nodes will be able to act as OCSP responders and to pro-vide up-to-date CSI. Even if one of these nodes gets compromised, or becomes dormant, the service will still be available by peers. Moreover, each node wishing to check the status of a certificate can contact the nearest responder instead of having to rely on a single centralized server. Thus, bottlenecks are avoided and network resources are consumed efficiently.

III. THE PROPOSED ADOPT SCHEME

We distinguish three different kinds of nodes in ADOPT: Server, Caching and Client-nodes. Server-nodes are nodes that announce the CSIs. They may be part of the MANET or they may be accessible via out of band means (e.g. GPRS). They issue and pro-vide OCSP responses. These are stored at the Caching-nodes which cache and forward OCSP responses, acting as OCSP responders. They are starting to cache according to specific criteria, which are discussed in the next section. They receive and cache pre-issued and pre-signed OCSP responses from the Server-nodes. When a Client-node requests a CSI, Caching-nodes receive this request, and search their cache for a pre-issued corresponding response. If a cached response is found it is forwarded to the Client-node. Caching-nodes parse OCSP requests in order to identify the queried certificate and locate a corresponding cached response. They don't need to issue or sign OCSP responses as these are pre-signed by the Server-nodes. The cached response is for-warded to the Client-node as is and there is no requirement for further processing. Caching-nodes do not need to use additional computational power to digitally sign responses. In order to receive cached responses, they need to maintain a path to Server-nodes. The authenticity and integrity of the responses is not compromised as OCSP responses are digitally signed by the Server-nodes or by an authorized and trusted responder.

Caching-nodes need to receive and cache only updated responses. Updating cached responses in nodes is a critical part of our scheme. Each Caching-node should ideally provide the most recent response. However, due to the nature of MANETs this may not be always possible. In [21] we have pro-posed three alternative mechanisms for updating cached OCSP responses:

- **Greedy Caching.** Each node caches every OCSP response that passes through it.
- **Selective Caching.** An OCSP response is cached after m appearances, where m is a popularity index.
- **No-Caching,** where a node performs no caching.

Client-nodes have to construct OCSP requests and also parse and verify OCSP responses. When a Client-node needs to check the status of a certificate, it sends an OCSP request to an OCSP responder. In traditional OCSP this is achieved by using the authorityInfoAccess extension [16] of the X.509 certificate, the use of which may not be applicable to MANETs. Therefore, in [21] we have proposed an alternative method, which discovers available OCSP responders, which is very similar to the route discovery of the DSR [18]. Figure 1 illustrates the sequence of actions that a Client-node and the Caching or Server-nodes perform in order to request and locate an OCSP response in a cache, respectively.

Evidently, an OCSP request can circulate within the ad hoc network without ever getting a response back. In order to overcome this issue we suggest a Time-To-Live (TTL) based mechanism. We proposed in [21] a framework that enables each node to dynamically estimate the TTL parameter. A Client-node can specify in the OCSP request the maximum number of hops (maxHops) over which the request may be propagated. Each intermediate host that receives the request reduces this number by one. If the maximum number of hops is reached without finding a corresponding OCSP response the request message is dropped. If a Client-node receives no OCSP response within a Waiting Window (WW), then it will increment the TTL parameter. This window corresponds to the time a Client-node has to wait until receiving a response. In [21] we have proposed a novel method to calculate WW using maximum round trip statistics. Finally, in [21] we have developed several criteria that force nodes to act as Caching or Server-nodes, such as:

- **Caching at the Edges**, i.e. on nodes that forward packets between different of MANETs.
- **Caching at Hub Nodes**, where hub nodes cache OCSP responses with higher rate than others.
- **Caching at High Mobility Nodes**, where a node with high mobility is considered as a candidate to cache, following the results of [12].

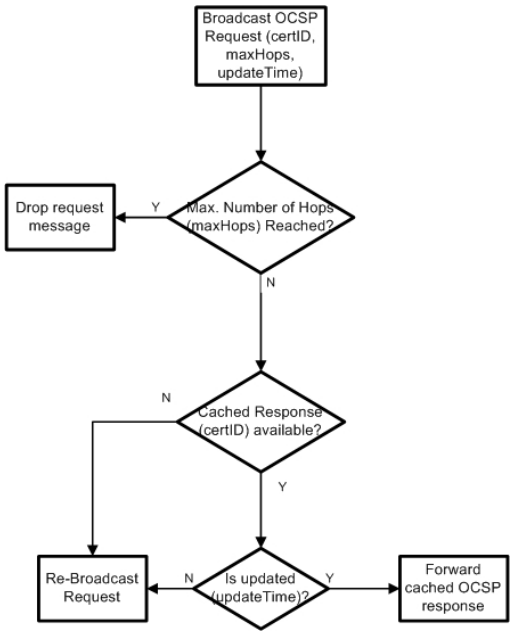

Figure 1. Flowchart for locating an OCSP response

Malicious or selfish behaviors by some nodes are important issues that should be considered when providing certificate revocation information. First of all, a malicious node in a MANET may start flooding the network with OCSP requests. An attack of this type would be flooding the network with invalid requests, asking for the status of a certificate that

doesn't exist. Intermediate nodes receiving this request will look for a corresponding response in their caches and, after finding none, forward the request to the following node. This way they consume resources to look for a cached response that doesn't even exist. A similar type of attack, which however can cause more damage as far as robustness is concerned, is the response flooding. Malicious nodes may issue and propagate false OCSP responses. As OCSP responses are digitally signed a node will realise that a response is not valid by verifying the signature. However, a node flooded by such responses may soon consume a lot of its resources in vain, in order to validate incoming responses, without ever getting a valid one. Apart from malicious behavior, some nodes may demonstrate selfishness. In terms of ADOPT, selfish nodes may, for example, decide to always follow a non-caching policy, even if their location or resources would imply otherwise. Nevertheless, they would want to use ADOPT in order to verify the revocation status of various certificates and thus would be broadcasting request messages.

The attacks we analysed are rather simple but if deployed on a large scale in a MANET, they could result in network congestion and partitioning as well as significant node resource consumption. In order to prevent and deal with these attacks a trust establishment framework could be used to support ADOPT's operation. In [25] we have proposed the Ad-hoc Trust Framework (ATF), a generic, distributed, framework for self-evolving trust establishment. ATF incorporates self-evidences, recommendations, subjective judgment and historical evidences to continuously evaluate the trust level of peers. Being a general purpose, self-evolving trust scheme, ATF can support trust aware applications, such as ADOPT. Thus, ADOPT could benefit in terms of availability and robustness if deployed in conjunction with ATF.

IV. EVALUATION OF ADOPT

A. Simulation Environment

For the evaluation of the ADOPT scheme we used the J-SIM wireless package simulator [23]. The 802.11 MAC layer and AODV routing protocol were used. The network consisted of 50 nodes, randomly distributed over a 500m x 500m terrain. The radio transmission range of each node was set equal to 30m. For our tests we used the test certificates avail-able at [24] that gave us 115 byte OCSP requests and 460 byte OCSP responses, including ADOPT extensions. We assumed that 50 certificates were issued, one for each node. Table 1 summarizes the parameters of the simulation environment.

Initially, there was only one Server-node in the net-work, which had signed and cached OCSP responses for all nodes' certificates. All other nodes where assumed to follow a greedy caching policy in the first test, and a selective caching policy in the second and third test. In the first and second selective caching policy a node would cache a response when the popularity index m was equal to 2 and 3, respectively. Concerning the capacity of the nodes' cache, we assumed that each node can store up to 25 responses. In our simulations we have measured:

- The time required for a Client-node to obtain an OCSP response.
- The number of hops required for a response to reach the Client-node.
- The time required for the propagation of information that a valid certificate has been revoked.
- The cache percentage that is occupied in each node after a simulation run.

TABLE I. SIMULATION ENVIRONMENT PARAMETERS

Number of nodes	50
Maximum speed	2 m/sec
Terrain dimensions	500m x 500m
Radio transmission range	30m
OCSP Response Cache Size	25 responses
Number of Client-Nodes	1
Number of Server-Nodes	1
Number of Caching -Nodes	49

It should be mentioned that the time axis in the following figures is expressed in J-SIM time units. During the simulations various nodes request the status of certificates, at different points in time. We only observe a specific node's CSI requests concerning 4 different certificates (with serial numbers 4, 32, 33, and 42) at discrete time instances.

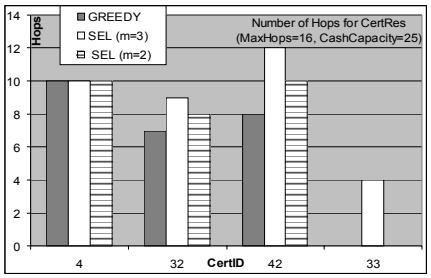

Figure 2. Number of hops that an OCSP response traverses for the different caching scenarios

B. Simulation Results and Discussion

Figure 2 shows the number of hops required for an OCSP response to reach its destination. The Client-node issues an OCSP request with the maximum TTL (i.e., 16 hops) and each node's cache capacity is equal to 25 OCSP response entries.

For the certificate with serial number 4 the three different policies produce equivalent results in terms of number of hops, since this Client-node is the only one that asks for this certificate's status. When it asks for this particular status, the corresponding response is returned from the Server-node, located 10 hops away. For the certificates with serial numbers 32 and 42, greedy caching performs better than selective policies, since the status of the certificate is maintained on interim Caching-nodes. When selective policies apply, the request is forwarded to the Server-node, since no cached response has been found in the interim nodes' caches. Figure 3 indicates the time and the number of hops required to propagate the status of a recently revoked certificate towards a Client-node. From this figure we observe that the greedy policy delivers the CSI faster, using less wireless hops.

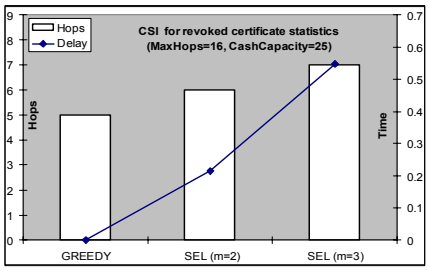

Figure 3. Time required disseminating a CSI for a recently revoked certificate

In Figure 4 we see that when large capacity caches are used, the OCSP response time is minimized. In the simulations, we observed that when the cache size is equal to 25 OCSP entries, then 34% of the Cashing-nodes fill their caches. Due to the FIFO discipline that we have applied, these nodes refresh their entries frequently. Thus, the CSI status is not located efficiently. On the other hand, when the cache size is equal to 50 OCSP entries (i.e., the number of active nodes) then a CSI status is always available, at least in one node's cache.

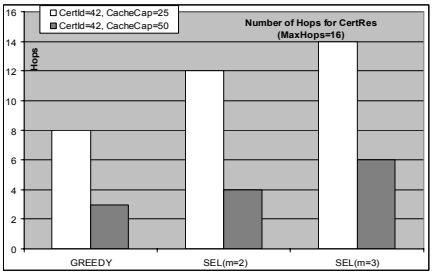

Figure 4. Nr. of hops that an OCSP response traverses using different caching policies and capacity

V. CONCLUSIONS

In this paper we discussed and evaluated the ADOPT, a novel certificate validation scheme, applicable in MANETs. ADOPT uses cached OCSP responses which are distributed to the nodes. OCSP, as a lightweight protocol, prevents the flooding of extended revocation lists, conserves the scarce band-width and avoids energy consumption that takes place during complex manipulations of revocation lists. ADOPT, furthermore, materializes efficient OCSP caching policies. The proposed caching policies enhance the performance metrics, such as the delay in the location of the certificate's status.

ACKNOWLEDGMENTS

This work was performed in the context of the project entitled "PERAS: PERvasive and Ad hoc Security" funded by the Greek Ministry of Development, General Secretariat for Research and Technology, under the framework "PENED".

REFERENCES

[1] F. Stajano, and R. Anderson, "The Resurrecting Duckling: Security Issues for Ad hoc Wireless Networks", in Proc. 7th Intl. Workshop on Security Protocols, '99

[2] J. Douceur, "The Sybil Attack", in Proc. IPTPS02

[3] L. Zhou, and Z. Haas, "Securing Ad Hoc Networks", IEEE Network, vol. 13, no.6, '99

[4] J. Kong, et al., "Providing robust and ubiquitous secu-rity support for MANETs", in Proc. ICNP2001

[5] S. Yi and R. Kravets, "MOCA: Mobile certificate authority for wireless ad hoc networks", In Proc. PKI03

[6] J. Cheambe, et al., "Security in Wireless Ad-Hoc Networks", in Proc. 13th IST Mobile & Wireless Comm., Jun. '04

[7] S. Capkun and J.-P. Hubaux, "BISS: Building Secure Routing Out of an Incomplete Set of Security Associa-tions", in Proc. ACM WiSe2003

[8] K. Sanzgiri, et al., "A secure routing protocol for ad hoc networks", In Proc. IEEE ICNP02

[9] M. G. Zapata, and N. Asokan, "Securing Ad hoc Routing Protocols", in Proc. ACM WiSe02

[10] V. Leung, et al., "Secure Routing with Tamper Resis-tant Module for Mobile Ad Hoc Networks", in Proc. of ACM MobiHoc2003

[11] J. Iliadis, S. Gritzalis, D. Spinellis, D. D. Cock, B. Preneel, D. Gritzalis, "Towards a framework for evaluat-ing certificate status information mechanisms," Computer Comm. 26(16), '03

[12] S. Capkun, et al., "Mobility Helps Security in Ad Hoc Networks", in Proc. ACM MobiHoc2003

[13] B. P. Crow, et al., "IEEE 802.11: Wireless Local Area Networks", IEEE Commn. Mag., vol. 35, no. 9, Sept. '97

[14] M. Gast, "802.11 Wireless Networks: The Definitive Guide", O'Reilly 2002, ISBN: 0-596-00183-5

[15] C. Crepeau and C.R. Davis, "A Certificate Revoca-tion Scheme for Wireless Ad Hoc Networks", in Proc. ACM SANS2003

[16] R. Housley, et al., "RFC 3280 - Internet X.509 PKI Certificate and Certificate Revocation List (CRL) Profile", IETF, Ap. '02

[17] M. Myers, et al., "RFC 2560 - X.509 Internet PKI OCSP", IETF, Jun. '99

[18] D. Johnson and D. Maltz, "Dynamic source routing in ad hoc wireless networks", Mob. Comp., Kluwer '96

[19] Deacon and R. Hurst, "Lightweight OCSP Profile for High Volume Environments", IETF Oct. '04

[20] G. F. Marias, K. Papapanagiotou, and P. Georgiadis, "ADOPT. A Distributed OCSP for Trust Establishment in MANETs", 11th European Wireless Conf., Apr. '05

[21] G. F. Marias, K. Papapanagiotou, and P. Georgiadis, "Caching Alternatives for a MANET-Oriented OCSP Scheme," IEEE SecQoS'05

[22] A. Arnes, "Public Key Certificate Revocation Schemes", PhD thesis, Norwegian University of Science and Technology, Feb. '00

[23] Available at www.j-sim.org

[24] Available at www.openvalidation.org

[25] G. F. Marias, V. Tsetsos, O. Sekkas, and P. Georgiadis, "A generic framework towards trust building in self-organized, peer, networks", in Proc. 1st International Workshop on Security, Privacy and Trust in Pervasive and Ubiquitous Computing, Greece, July 2005