Multiple-key Cryptography-based Distributed Certificate Authority in Mobile Ad-hoc Networks

Hongbo Zhou
Dept. of Computer Science
Slippery Rock University
Slippery Rock, Pennsylvania, USA
hongbo.zhou@sru.edu

Matt W. Mutka
Dept. of Computer Science & Engineering
Michigan State University
East Lansing, Michigan, USA
mutka@cse.msu.edu

Lionel M. Ni
Dept. of Computer Science
Hong Kong University of Science & Technology
Hong Kong, China
ni@cs.ust.hk

Abstract—**Most prevalent Distributed Certificate Authority (DCA) schemes in the MANET are based upon threshold cryptography, which is invulnerable to mobile adversaries and tolerable to missing or faulty DCA server nodes, and thus becomes the "de facto" standard for the security framework in the MANET. However, this scheme cannot defeat Sybil attacks, in which a malicious node impersonates many identities. To solve the problem, a multiple-key cryptography-based DCA scheme, namely the MC-DCA scheme, is proposed in the paper. It is invulnerable to Sybil attacks, and achieves lower communication overhead and moderate latency compared with the threshold-based scheme, which is supported by the simulation results.**

Keywords- Distributed Certificate Authority, MANET, security, Sybil attack

I. INTRODUCTION

A mobile ad-hoc network (MANET) is a temporary infrastructureless multi-hop wireless network in which the nodes can move arbitrarily. Because of the low cost of computing devices and wireless communication equipment and the ease of deployment, a MANET will be widely deployed in temporary networks in meeting rooms, airports, stadiums, battlefields, and open country, where it may be expensive or impossible to install a networking infrastructure.

However, prior to the practical deployment of a MANET, strict security requirements must be satisfied due to the following reasons:

(1) The communication medium is a broadcast channel. Thus, all nearby nodes can overhear the packets in transit. Therefore, encryption is necessary to protect sensitive data between the source and destination;

(2) In the MANET where an infrastructure is absent, it is more difficult to identify the source of a packet.

To solve these problems, public key cryptography can be applied in the MANET. Every node in the MANET has a unique public/private key pair. During data communications initialization, both ends can exchange their public keys to establish the secret key for the subsequent data encryption. From then on, they can switch to symmetric cryptography that is faster than public key cryptography.

Although the scheme is simple to implement, it is vulnerable to "man-in-the-middle" attacks unless there is a certificate authority (CA) in the network. With a CA being present, each node registers the binding of its public key and IP address in the CA and acquires the certificate from the CA as a proof of the binding when it enters the MANET. Thus, "man-in-the-middle" attacks and IP spoofing attacks can be defeated.

In hardwired networks, the CA can be a centralized server, which is impractical in the MANET. Because every node in the network is mobile and power-limited, none is reliable. Therefore, most research effort is spent building a distributed Certificate Authority (DCA) in the MANET.

The paper is structured as follows: Section II introduces the threshold cryptography-based DCA scheme. It is invulnerable to mobile adversaries and tolerable to missing or faulty server nodes. However, it cannot defeat Sybil attacks, which is analyzed in Section III. A new scheme based on multiple-key cryptography, namely MC-DCA scheme, is proposed in Section IV. It is invulnerable to Sybil attacks, and achieves lower communication overhead and moderate latency in comparison to a threshold-based scheme, which is supported by the simulation results in Section V. Section VI suggests future work and concludes the paper.

II. RELATED WORK

Threshold cryptography was originally proposed for the DCA in hardwired networks ([1] - [2]), which is based upon public key cryptography. The public key of the DCA is known to all the users, while the secret key is divided into many secret shares that are stored among the servers. For the (k, n)-threshold cryptography, there are n servers, each of which has a unique secret share. When a client node wants its message signed by the servers, it sends the message to each server, which applies its secret share in computation of the partial signature. With the partial signatures from at least k servers, the DCA server group can construct a valid signature that can be verified with the well-known public key. Compared with the traditional centralized CA scheme, the threshold cryptography-based DCA has the following advantages:

(1) The secret shares have no explicit relations except that they are all part of the secret key, which means that one share cannot be deducted from another share. Even if one server is compromised, the attacker still has no information about other shares. The attacker has no choice but to compromise at least k servers to find out the secret key;

This research is supported in part by NSF grant no. 0334035, Hong Kong RGC grants HKUST6264/04E, and AoE/E-01/99

0-7803-9415-1/05/$20.00 (C) 2005 IEEE

This full text paper was peer reviewed at the direction of IEEE Communications Society subject matter experts for publication in the IEEE GLOBECOM 2005 proceedings.

(2) As long as there are at least k servers that apply their shares in the signing procedures correctly, the valid signature can be generated. Thus, the threshold-based scheme is tolerable to some missing or faulty servers, which makes it especially suitable for the MANET where a server node may leave or shut down without notice;

(3) To further improve the security of the scheme, the shares can be refreshed periodically among the servers [3]. The share before the refresh operation and that after the refresh operation have no relation, which means that even if one share is leaked, it will become useless after the refresh interval. Thus, a mobile adversary is challenged to compromise at least k servers in a short time[1]. Although the secret shares are changed, the secret key is always the same, which means the corresponding well-known public key is the same. Therefore, the refresh operation is transparent to client nodes.

Threshold cryptography was introduced into the MANET in [4]. On receipt of a request from a client node, each server generates a partial signature with its share and sends it to a special node that is designated as a combinator. The combinator collects all the responses from servers and calculates the signature for the client node. The scheme was applied to a large-scale MANET in [5], in which the nodes are divided into many clusters. The cluster heads form the server group and provide certificate service to cluster members.

Due to its invulnerability to mobile adversaries and tolerance to instable nodes, the threshold-based DCA scheme becomes the "de facto" standard for certificate authority service in the MANET.

III. Vulnerability of Threshold Cryptography-Based DCA

The threshold-based DCA was originally proposed for hardwired networks, in which the administrators of the server hosts can ascertain others' identities and trust each other. In the MANET where Sybil attacks [6] may be present, the threshold scheme may be compromised.

The Sybil attack refers to the attack from a malicious node that impersonates many identities in the network when cooperation is necessary to provide the service. The attack on the threshold scheme is illustrated in Fig. 1.

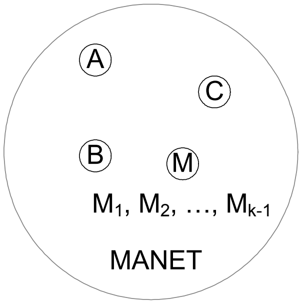

Figure 1. Sybil attack on threshold-based DCA scheme.

In Fig. 1, nodes A, B, and C are good nodes; node M is a malicious node. All of them form the (k, n)-threshold DCA server group. Node M impersonates non-existent nodes M_1, M_2, …, and M_{k-1}. It will know the value of k during the parameter negotiation procedures and forge k-1 identities as needed; or it prepares m identities beforehand and persuades other server nodes that m+1 should be large enough for parameter k, hopefully leading to the value of k that is less than or equal to m+1. In either way, once all the nodes agree on the parameters and exchange their shares, node M will have enough secret shares to construct valid signatures.

The Sybil attack is fatal to the threshold scheme, but there is no efficient way to defeat it because it is difficult to bind a single identity with one node in the MANET. The CA scheme regards the IP address of the node as its identity, which can be easily forged by a malicious node, especially in the presence of autoconfiguration schemes that are utilized to assign IP addresses to nodes automatically in an open system[2] ([7] – [12]). Similarly, it is not difficult for a malicious node to have many hardware addresses. Even if the CPUs in some nodes have unique built-in identifiers, the identifiers are hidden from outsiders. The malicious node can still forge the built-in identifiers easily.

IV. Multiple-Key Cryptography-Based DCA

To defeat Sybil attacks, a new scheme based on multiple-key cryptography, namely the MC-DCA scheme, is described in this section. We assume that a MANET is an open system where nodes are free to join and leave, and thus there is no single party of trust.

A. Multiple-key cryptography

Multiple-key cryptography was proposed in [13], which is based on public key cryptography. In the traditional public key cryptography, there are two keys: k_1 and k_2. The message encrypted/signed with one key can be decrypted/verified with the other key. Either one can be the public key; and the other is the private key. In [13], the concept is extended to multiple keys: k_1, k_2, …, and k_n. the message encrypted/signed with one subset of keys can only be decrypted/verified with all the other keys. For example, suppose that there are 4 keys: k_1, k_2, k_3, and k_4. The message encrypted with k_1 and k_3 can only be decrypted with k_2 and k_4. With only either k_2 or k_4, the message cannot be decrypted. Obviously, if one key is chosen to be the public key, all the others must be private keys, which is the way that multiple-key cryptography is applied in DCA.

Suppose that there are n servers. A central authority (i.e., the owner of the scheme in [13]) divides the secret key into n shares and stores one share at one server. If a client wants its message signed by the DCA, it sends the message to one of the servers. Each server signs the message with its share in turn, and the last server sends the signature to the client. In multiple-key cryptography, since every server node is required to generate the valid signature, even if a malicious node has many

[1] Of course, we assume that the server node is not totally controlled by the attacker. Otherwise, the attacker will know all the server's shares at different times.

[2] In a closed system where identities are assigned from a central authority, the problem is trivial.

identities in the DCA server group, it cannot forge signatures when there are good server nodes. The underlying assumption is that good nodes are encouraged to join the DCA group, just as good citizens are encouraged to provide service to others in the human society.

However, since we assume that there is no single trusted party in the MANET, the original multiple-key cryptography cannot be applied to the DCA in the MANET directly. Some modifications are necessary.

B. Algorithm

We utilize the distributed algorithm in [14] to choose secret shares and calculate the public key for server nodes. Suppose that there are *n* servers. In [14], all the server nodes agree on three parameters: two large primes *p* and *q* such that *q* divides *p*-1, and g that is a generator of G_q (G_q is the unique subgroup of Z^*_{p} of order *q*). These three parameters are parts of the public key of the DCA and known to all the users in the network. Server node *i* chooses its secret share x_i and computes the public part $h_i = g^{xi}$. The private key of the DCA is the sum of x_i, and the public key is the product of h_i. The next steps in [14] are the procedures for share refreshing, which are utilized in the threshold scheme and thus unrelated to our multiple-key scheme.

According to the algorithm in [14], if server node *i* is not the same node of server node *j*, and server node *i* does not leak its secret share, server node *j* has no idea about *i*'s secret share. As a result, a subset of the server nodes cannot forge signatures as the whole DCA group. All of the server nodes have to cooperate to generate valid signatures.

If server node *i* leaves, the DCA is down because no one else knows its secret share. Even if it knows it is going to leave, it cannot transfer its secret share to another node, say node *k*, and designate node *k* to take its place in the DCA, because node *i* cannot ascertain if node *k* is another identity of a server node (say, server node *j*) or not. If server node *j* is a malicious node that impersonates all the other server nodes simultaneously, after it impersonates node *k* and replaces server node *i*, it will have all the secret shares and be able to forge valid signatures.

To account for a missing server node, a version number associated with the public key is introduced in MC-DCA scheme. Once a server node is detected to have left the network, new nodes will be invited to join the server group. The old server nodes may keep their secret shares and public parts, while the new server nodes choose their own secret shares and calculate new public parts. As a result, a new public/private key pair for the DCA is generated with the version number increased by one. The clients store all the public keys, and verify the certificate issued from the DCA using the public key with the same version number. This scheme has a potential security advantage in comparison with the threshold scheme because the private keys are different with different version numbers, and the previous private keys cannot be recovered. If one public/private key pair of the DCA is compromised in a rare event, the certificates issued with the previous version numbers are still valid.

Notice that the partial signature signed with the secret share can be verified with the corresponding public part, the faulty server node can be easily pinpointed. The client just stores the public key of the DCA, while the server nodes store each other's public part. If the client receives a signature that cannot be verified with the DCA's public key, it can bring all the partial signatures to the server group to find out the faulty server node and exclude it from the DCA group.

To further improve the security of the MC-DCA scheme, all the server nodes can choose new secret shares and calculate the public parts occasionally. The old secret shares are discarded, and the version number of the resulting public key is increased by one. If no client applies for a certificate during the next interval, the version number can be kept to be the same even if the secret shares and public key change. For example, suppose that the time interval is *t*. At time 3*t*, the version number is 4 after the server nodes choose new secret shares and the DCA has a new public key. At time 4*t*, they choose new secret shares again. If there is no certificate issued between 3*t* and 4*t*, the version number is still 4.

To limit the number of DCA's public keys stored at the client in the MC-DCA scheme, once the increase in the version number of the public key reaches a special value, all the client nodes whose certificates are signed with previous private keys can renew their certificates at the DCA, and all the nodes remove these obsolete public keys from their repositories. For example, suppose that the special value is 20. When the version number of the public key increases from 1 to 21, all the clients with the certificates signed with the private keys from version 1 to 11 renew their certificates with the private key of version 21. After the renew procedure, the public keys with version 1 to 11 can be safely removed from all the nodes. The aforementioned method could save much communication overhead in the renew procedure because some client nodes with old certificates may have already left the MANET, just as some server nodes.

C. DCA group membership management

To maintain the registration table of bindings of IP addresses and public keys in MC-DCA scheme, the server nodes need to track each other with the aid of periodic HELLO messages. Otherwise, if all the server nodes leave without notice, the registration information will be lost, which will lead to high communication overhead in the subsequent registrations. For example, suppose that client node A registers its public key *x* at the DCA and obtains the certificate. After all the previous server nodes leave and a new DCA group forms, another client node, node B, tries to register the same public key of *x* at the DCA. Without the previous registration information, the new DCA group has to inquire all the client nodes to determine the uniqueness of the public key.

Although the threshold scheme is tolerable to some missing server nodes, it has stricter requirements on group membership maintenance than MC-DCA scheme. For example, suppose that (3, 5)-threshold cryptography is adopted. If three server nodes leave the MANET without notice, the remaining two server nodes cannot recover the secret key of the DCA. Although it can utilize the concept of the version number of public keys in MC-DCA scheme, there would be no advantage of the tolerance to missing server nodes mentioned in Section II. Thus, the periodic HELLO messages are indispensable. In the previous example, once a server node is detected to have left the MANET, the four remaining server nodes need to invite new server nodes to join the DCA server group[3]. The mechanism of periodic HELLO messages is not mentioned in [4], but the cluster head's periodic beacon messages with intervals of 10 seconds to 30 seconds are utilized in [5], which can be regarded as a kind of periodic HELLO message.

The difference between the MC-DCA scheme and threshold scheme in group membership maintenance is that the minimum number of the remaining server nodes in the former scheme is one, while the minimum number in the latter scheme is the threshold value.

D. Procedures

The procedures of MC-DCA scheme work as follows:

(1) The first client node in the MANET needs a DCA service, so it broadcasts an INVITE message to initiate an invitation to all the other nodes in the MANET;

(2) On receipt of the INVITE message, each node decides itself if it participates in the service or not, to satisfy the assumption of the multiple-key cryptography-based scheme. If it decides to join the server group, it makes an announcement with a broadcast of PARTCP message, including its own public key. All the other nodes will record it as a server node;

(3) All the server nodes agree on the parameters of p, q, and g, and each chooses its secret share and calculates the public part. Then they exchange their public parts and compute the public key by multiplying all of them. One server node makes an announcement of the public key with version number 1;

(4) The client sends to each server node its public key, IP address, and other related information encrypted with the server nodes' own public keys to request a certificate in a REQUEST message;

(5) On receipt of the REQUEST message from a client node, each server node calculates the partial signature with its secret share, signs the partial signature with its own private key, and sends a REPLY message to the client;

(6) The client verifies the signature with the public key of the DCA after it combines all the partial signatures together. If the verification fails, it brings all the signed partial signatures to the DCA group to pinpoint which server node is malfunctioning and to exclude it from the group;

(7) Each server node chooses a secret share and calculates the public part periodically, and updates the version number;

(8) The server nodes send each other periodic HELLO messages to track the membership of the DCA group and to exchange their renewed public parts. If one server node is detected to have left the MANET and they just received a request from a client node, or the number of remaining server nodes is less than a threshold value (e.g., 3), an invitation is initiated, with steps (2) and (3) repeated, except that the old server nodes may choose to keep their previous secret shares and public parts. The version number is increased by 1;

(9) If a client node detects a server node is missing, it either initiates an invitation proactively or waits reactively until the server nodes detect it and broadcast an invitation in step (8);

(10) If the number of DCA's public keys reaches the capacity of the client's repository, the client renews its certificate and updates the repository if necessary.

There may be some optimizations. For example, when a client node receives an invitation just before it is going to send a request to the DCA, it can delay the request for a while. Another example is that if the replies from some server nodes are lost due to network congestion, the client can send the request to these server nodes a second time.

V. Performance Evaluation

A. Simulation setup

The simulations were run with 50 nodes in an 800×800 m^2 topology area with *ns*-2 (version 2.27). All the nodes move with the random waypoint mobility model [15]. The maximum speed is 10.0 m/sec and the minimum speed is 2.0 m/sec. The pause time is 10.0 seconds.

In the simulation, to determine if a node is willing to participate in the DCA server group, each node chooses a random value uniformly distributed in the range of [0, 1]. The nodes that choose a random value less than a threshold value are eligible to be the server nodes. In the simulation of both schemes, the threshold values are 0.1, so that around 10% of the nodes will be the server nodes, with the minimum number of server node being 3. The simulation time is 600 seconds. All the nodes have a lifetime and the time to request certificates pre-set, both of which are evenly distributed in the range of 0 and 2 times the simulation time (i.e., 1200 seconds).

In both schemes, all the server nodes send each other periodic HELLO messages. If the HELLO messages from a server node are not received for 3 intervals, it is regarded as departed. The interval in the threshold scheme is set to be 10 seconds (a longer interval will lead to the number of server nodes being less than the minimum value). The share refreshing is also contained in the HELLO messages. In the MC-DCA scheme, because the reactive invitation method in step (9) in subsection IV.D is adopted, the interval for HELLO messages is 5 seconds to expedite the invitation process. The client node's repository has a capacity of 40 public keys.

B. Simulation results

The simulations were run 4 times. The sum of control messages in each category received at all the nodes for one simulation is illustrated in Fig. 2. Because the group membership maintenance in the threshold scheme is stricter than that in MC-DCA scheme, more communication overhead occurs to invite new members.

[3] The DCA server group may choose to wait until there are three server nodes remaining in the network in the threshold scheme. However, it cannot be predicted that one of the remaining server nodes leaves before a new server node joins.

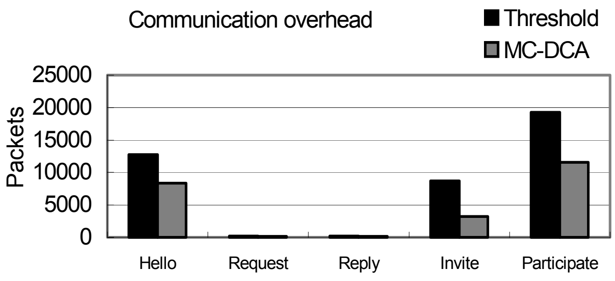

Figure 2. The number of packets in each category.

Fig. 3 compares the sum of all the control messages received for four simulations. Generally speaking, the number of packets received in MC-DCA scheme is around one-half of that in the threshold scheme.

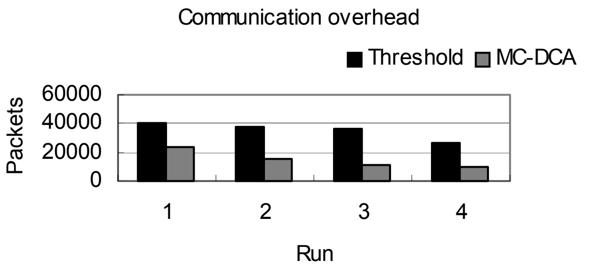

Figure 3. Communication overhead.

Fig. 4 illustrates the average latency in the MC-DCA scheme, which is defined to be the interval between the time when a node initiates the request and the time when it gets its certificate. Theoretically, the maximum latency is around 3 times the HELLO message interval (i.e., 15 seconds). Due to node mobility, network congestion, and random timeout mechanism in the simulation, a few nodes may have longer latency.

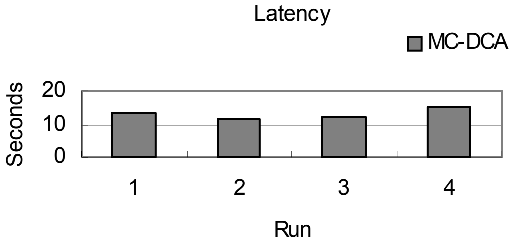

Figure 4. The latency in MC-DCA scheme.

VI. CONCLUSION

With the invulnerability to mobile adversaries and tolerance to missing or faulty server nodes, the threshold cryptography-based DCA scheme is regarded as an ideal candidate for a MANET where the nodes are instable. However, during the formation of the DCA, if a malicious node initiates Sybil attacks in which it impersonates multiple identities, it may acquire enough secret shares to forge valid signatures. Since it is not difficult for a malicious node to forge multiple identities, the security of the threshold cryptography-based DCA scheme can be easily compromised.

To defeat Sybil attacks, a new scheme based on multiple-key cryptography, namely the MC-DCA scheme, is proposed in the paper. In the scheme, every server node is required to generate signatures. Thus, as long as there are good server nodes, even if a malicious node has many identities, it cannot forge signatures of the DCA. Compared to the threshold scheme, it also achieves lower communication overhead and moderate latency, which is supported by simulation results. The application of the MC-DCA scheme in a large-scale MANET and the integration of MC-DCA, autoconfiguration algorithms, and routing protocols are still under study, which will be our future work.

REFERENCE

[1] A. Shamir, "How to share a secret," Communications of the ACM, Vol.22, pp. 612 - 613, November 1979

[2] Y. Desmedt and Y. Frankel, "Threshold cryptosystems," Proceedings of Advances in Cryptography (Crypto 89), Lecture Notes in Computer Science, Vol. 435, Springer-Verlag, pp. 307 – 315, 1989

[3] A. Herzberg, M. Jakobsson, S. Jarecki, H. Krawczyk, and M. Yung, "Proactive public key and signature systems," in ACM Conference on Computer and Communication Security, Zürich, December 1996

[4] L. Zhou and Z. J. Haas, "Securing ad hoc networks," IEEE Network, Vol. 13, No. 6, pp. 24-30, November/December 1999

[5] M. Bechler, H.-J. Hof, D. Kraft, F. Pählke, and L. Wolf, "A cluster-based security architecture for ad hoc networks," Proceedings of the 23rd Conference of IEEE Communication Society (INFOCOM 2004), Hong Kong, China, March 2004

[6] J. Couceur, "The sybil attack," In Proceedings of the 1st Workshop on Peer-to-Peer Systems (IPTPS'02), Cambridge, MA, March 2002

[7] C. Perkins, J. Malinen, R. Wakikawa, E. M. Belding-Royer, and Y. Sun, "IP address autoconfiguration for ad hoc networks," draft-ietf-manet-autoconf-01.txt, November 2001 (work in progress)

[8] K. Weniger and M. Zitterbart, "IPv6 autoconfiguration in large scale mobile ad-hoc networks," In Proceedings of European Wireless 2002, Florence, Italy, February 2002

[9] N. Vaidya, "Duplicate address detection in mobile ad hoc networks," In Proceedings of the 3rd ACM International Symposium on Mobile Ad Hoc Networking and Computing (MOBIHOC'02), Lausanne, Switzerland, June 2002

[10] S. Nesargi and R. Prakash, "MANETconf: configuration of hosts in a mobile ad hoc network," Proceedings of the 21st Annual Joint Conference of IEEE Computer and Communication Societies (INFOCOM 2002), New York, NY, June 2002

[11] H. Zhou, L. M. Ni, and M. W. Mutka, "Prophet Address Allocation for Large Scale MANETs," Proceedings of the 22nd Annual Joint Conference of IEEE Computer and Communication Societies (INFOCOM 2003), San Francisco, CA, April 2003

[12] H. Zhou, L. M. Ni, and M. W. Mutka, "Prophet Address Allocation for Large Scale MANETs," Ad Hoc Networks Journal, Vol. 1, Issue 4, pp 423-434, November 2003

[13] C. Boyd, "Some applications of multiple key ciphers," In Proceedings of Advances in Cryptography (Eurocrypt'88), Lecture Notes in Computer Science, Springer-Verlag, pp. 455 – 467, 1988

[14] T. P. Pedersen, "A threshold cryptosystem without a trusted party," In Proceedings of Advances in Cryptology (Eurocrypt'91), Lecture Notes in Computer Science, Vol. 547, Springer-Verlag, pp. 522-526, 1991

[15] J. Broch, D. Maltz, D. Johnson, Y. Hu, and J. Jetcheva, "A performance comparison of multi-hop wireless ad hoc routing protocols," Proceedings of the Fourth Annual ACM/IEEE International Conference on Mobile Computing and Networking, pp. 85–97, October 1998