Identity-Based Key Management in MANETs using Public Key Cryptography

Dr. Anil Kapil anil_kdk@yahoo.com
Professor, M M Institute of Computer Technology and Business Management, M M University, Mullana, Ambala, Haryana, India

Mr. Sanjeev Rana sanjeevrana@rediffmail.com
Asst. Professor, Department of Computer Engineering, M M Engineering College, M M. University, Mullana, Ambala, Haryana, India

ABSTRACT

Wireless mobile Ad Hoc Networks (MANETs) are an emerging area of mobile computing. MANETs face serious security problems due to their unique characteristics such as mobility, dynamic topology and lack of central infrastructure support. In conventional networks, deploying a robust and reliable security scheme such as Public Key Infrastructure (PKI) requires a central authority or trusted third party to provide fundamental security services including digital certificates, authentication and encryption. In the proposed scheme, a secure identity-based key management scheme is proposed for networks in environments without any PKI. This scheme solved the security problem in the MANET and is also suitable for application to other wired network structures.

Keywords: MANETs, Key Management, Key Distribution

1. INTRODUCTION

1.1 Overview

The demand for more flexible, easy to use and advanced wireless communication technologies has provided opportunities for new networking technologies. MANETs are an innovative approach to a new form of wireless networking technology. There are several issues, such as routing, scalability, quality of service and security that need to be solved before implementing these network technologies in practice. Most of the research that has been done on ad hoc networking has faced on routing [1] [2] [3]. Other issues such as security and network addressing have received considerably less attention [4] [5]. Designing and implementing any kind of security scheme requires a secret to set up a trust relationship between two or more communicating parties. For example, the ability of node A to trust node B could be achieved by a process that permits node A to verify that node B is genuine to a set of pre-imposed rules. This in turn could be achieved by permitting such genuine node to establish authenticated shared secrets that other nodes cannot. The process of establishing such authenticated shared secrets could be achieved by a suitable key management scheme. The fundamental security services provided by every key management system are key synchronism, secrecy, freshness, independence, authentication, confirmation and forward and backward secrecy [6]. Conventional key management techniques may either require an online trusted server or not. The infrastructureless nature of MANETs precludes the use of server based protocols such as Kerberos [7]. There are two intuitive

symmetric-key solutions, though neither is satisfactory. The first one is to preload all the nodes with a global symmetric key, which is vulnerable to any point of compromise. If any single node is compromised, the security of entire network is breached. Another solution is to let each pair of nodes maintain a secret that is known to those two nodes. This approach suffers from three main drawbacks.

- First, as the size of network increases, securely updating the overall n(n-1)/2 keys in the network is not an easy task.
- Second, each node requires storing (n-1) keys, which may cause significant overhead in a large network.
- Last, there is a problem of scalability because it is difficult to establish pairwise symmetric keys between existing nodes and newly joined node.

Symmetric key techniques are commonly criticized for not supporting digital signatures because each key is known to only two nodes. This renders public key solutions more appealing for MANETs, which is used in this paper.

To address these security related issues, this paper present a proposed scheme using ID-based cryptography approach for key management and key distribution and also provides end-to-end authentication without any PKI. This paper is organized into four sections. This next section gives the overview of existing approaches. It also presents the benefits of our scheme and limitation of the existing schemes. Section two presents our proposed ID-based key management scheme for mobile ad hoc networks. Section three explains the security analysis of various attacks on the proposed scheme. Section four presents conclusion and future works.

1.2 Related Works

Recent researches have shown that wireless ad hoc networks are highly vulnerable to various security threats due to their inherent characteristics [8] [9]. This leaves ad hoc key management and key distribution as a wide open problem. There has been a rich literature on public key management in MANETs, [10] [11] [12] [13] [14] [15]. These schemes all depend on certificate-based cryptography (CBC), which uses public key certificates to authenticate public keys by binding public keys to the owner's identities. A main concern with CBC-based approaches is the need for certificate-based public key distribution. Another approach is to preload each node with all others public key based certificates prior to network deployment. This leads not only the problem of scalability when network size increases, but also difficult to update keys in a secure and cost effective fashion. One new approach is about on-demand certificate retrieval may cause both unfavorable communication latency and communication overhead. As a powerful alternative to CBC, ID-based cryptography (IBC) has been gaining momentum in recent years. The idea of Identity based cryptosystem was first proposed by Shamir [15] to simplify the conventional public key cryptosystem, and make the key management easier [16]. Khalili, et. al proposed a protocol for management and authentication in an ad hoc network that is based on an ID-based scheme in [17].

It allows public keys to be derived from entities known identity information, thus eliminating the need for public key distribution and certificates. This featured inspired a few IBC-based certificateless public key management schemes for MANETs such as [17] [18][19][20]. The basic idea is to let some [17] [18] [20] or all network nodes called a shareholders, share a network master-key using threshold cryptography [21] [22] and collaboratively issue ID-based private keys. There, however, remain many issues to be satisfactorily resolved:

- First of all, all the security of the whole network is breached when a threshold number of shareholders are compromised.
- Second, updating ID-based public/private keys requires each node to individually contact a threshold number of shareholders, which represents a significant overhead in large scale MANET.

To address these security related issues, this paper present a proposed scheme using Identity based cryptography using public key cryptography approach for key management. The main benefits of the proposed scheme are:

- This scheme does not need any inline Certification Authority to share secret key.

- The scheme avoids the need for users to generate their own public keys and to then distribute these keys throughout the network.
- There is no need to handle heavily used public key cryptography based certificates

2. THE PROPOSED SCHEME

In this section, a secured ID-based key management scheme is proposed suitable for applying in wireless mobile ad hoc network. Similar to other ID-based cryptosystems, a trusted key generation center is needed in this scheme for verifying user identity and generating the corresponding private keys. After all users have registered, the key generation center can be closed or off-line. The proposed scheme consists of four phases: initialization, registration of user, verification of user, and key exchange between two users as shown in figure 1.

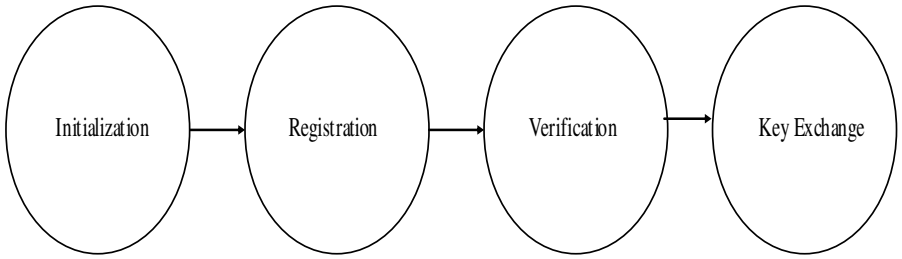

FIGURE 1: Four phases of Key Exchange process in Proposed Scheme

The proposed scheme used some notation given below in table 1.
Let U = {U_1, U_2, U_3, … U_N} are different users and ID = {ID_1, ID_2, ID_3, …. ID_N} be the identity (which is unique) of respective users in the mobile ad hoc network. Each user U_i has a unique identity ID_i, which is known to all the other users. Each user can execute the scheme multiple times with different partners. This is modeled by allowing each user an unlimited number of instances with which to execute the scheme.

TABLE 1: Notation

p & q	Two large and strong prime numbers
n	Product of p and q
ϕ (n)	Product of (p-1) and (q-1)
e	Integer number prime with respect to n
d	Part of private key of Key Center and is equal to e^{-1} mod ϕ (n)
ID_i, ID_j	Identity of users U_i and U_j
n,e	Pair used as public key of key distribution center
n,d	Pair used as private key of key distribution center
T_i , T_j	Time stamp used by users U_i and U_j
h( )	One-way hash function
g_i, g_j	Encrypted code of ID_i and ID_j of users U_i and U_j respectively created by Key Center
r_i, r_j	Large random numbers chosen as secret by users U_i and U_j respectively
SK_i , SKj	Secret session key established at user U_i and U_j

Initialization phase: In this phase, each user U_i ε U gets his long-term public and private keys. The key generation center randomly chooses a secret key as master key and then computes, and publishes corresponding public key. To construct this private-public key pair, we are motivated by the RSA [23] scheme, the key generation center calculates public key (n, e) and private key (p, q, d, ϕ(n)). In addition, the center also determines a primitive element α in both of the fields GF(p)

and GF(q), and chooses a one-way hash function h( ). Similarly, treat (α, h( )) along with (n, e) as public information. One-way hash function h( ) gives unique output for different input.

User Registration phase: User U_i take his identification number ID_i to the key registration center to obtain the signature g_i for ID_i. If the center confirms the correctness and the relationship between U_i and ID_i , then center calculates g_i using:

$$g_i = ID_i^d \bmod n \qquad \text{(i)}$$

.and hands g_j to U_i as shown in figure 2. When all the users have registered and got their g_i (i = 1...n) the center does not need to exist in ad hoc network any more.

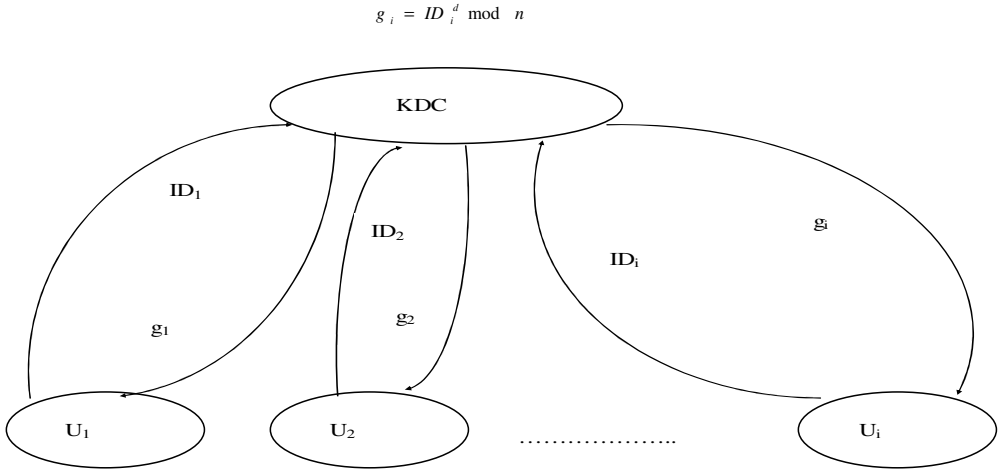

FIGURE 2: Registration phase of user with their identity

User Verification phase: Assume U_i and U_j are the two users communicate with each other. First, U_i selects a random number r_i and computes two public keys of y_i and t_i as

$$y_i = g_i.\alpha^{r_i} \bmod n \qquad \text{(ii)}$$

and

$$t_i = r_i^e \bmod n \qquad \text{(iii)}$$

Second, U_i uses a timestamp T_i and the identification number (ID_j) of user j to perform the operation of one-way function of $h(y_i,t_i,T_i,,ID_j)$, then computes

$$s_i = g_i.r_i^{h(y_i,t_i,T_i,ID_j)} \bmod n \qquad \text{(iv)}$$

Finally, U_i sends (ID_j y_i, t_i, s_i, T_j) to U_j as shown in figure 3.
Similarly, U_j selects the random number r_j and the timestamp T_j , then computes

$$y_j = g_j.\alpha^{r_j} \bmod n \qquad \text{(v)}$$

$$t_j = r_j^e \bmod n \qquad \text{(vi)}$$

$$s_j = g_j.r_j^{h(y_j,t_j,T_j,ID_i)} \bmod n \qquad \text{(vii)}$$

and sends (ID_j , y_j, t_j, s_j, T_j) to U_i as shown in figure 3.
Before generating the session key, U_i and U_j need to verify whether (ID_j, y_i ,t_i, s_i, T_j) and (ID_j , y_j, t_j, s_j, T_j) are sent from user i and user j, respectively, by checking

$$s_j^e = ID_j.t_j^{h(y_j,t_j,T_j,ID_i)} \bmod n \quad \text{(viii)}$$

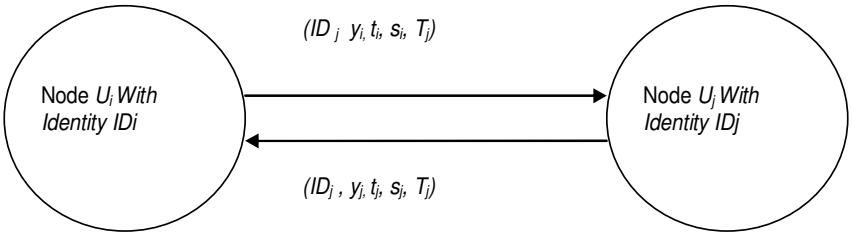

FIGURE 3: Communication between MANETs Nodes for end-to-end Authentication and Secret Shared key generation in the proposed scheme

It can be checked by user U_i as shown below:
Take L.H.S and from equation (vii)

$$s_j^e = (g_j.r_j^{h(y_j,t_j,T_j,ID_i)} \bmod n)^e$$
$$s_j^e = (g_j)^e.(r_j^{h(y_j,t_j,T_j,ID_i)} \bmod n)^e$$
$$s_j^e = (g_j)^e.(r_j^{h(y_j,t_j,T_j,ID_i)} \bmod n)^e$$
$$s_j^e = (ID_j^d \bmod n)^e.(r_j^{e*h(y_j,t_j,T_j,ID_i)} \bmod n)$$

Mathematically,
$(G^x \bmod n)^y = (G^y \bmod n)^x = G^{xy} \bmod n$
$(G^x \bmod n) \bmod n = G^x \bmod n$ because n is a very large number

$$s_j^e = (ID_j^{d*e} \bmod n).((r_j^e)^{h(y_j,t_j,T_j,ID_i)} \bmod n)$$
$$s_j^e = (ID_j^{1 \bmod \varphi(n)} \bmod n).((t_j)^{h(y_j,t_j,T_j,ID_i)} \bmod n)$$
$$s_j^e = (ID_j \bmod n).((t_j)^{h(y_j,t_j,T_j,ID_i)} \bmod n)$$

According to RSA, $d = e^{-1} \bmod \phi(n)$ and $d * e = 1 \bmod \phi(n) = 1$

$$s_j^e = ID_j.t_j^{h(y_j,t_j,T_j,ID_i)} \bmod n$$
$$s_j^e = R.H.S$$

And, similarly, user U_j verify at their end that

$$s_i^{e.?} = ID_i.t_i^{h(y_i,t_i,T_i,ID_j)} \bmod n \quad \text{(ix)}$$

Key Exchange phase: U_i and U_j compute secret session keys SK_i , SK_j , respectively, as follows: SK_i, SK_j respectively, as follows:

$$SK_i = \left(\frac{y_j^e}{ID_j}\right)^{r_j} \bmod n \quad \text{(x)}$$

$$SK_j = (\frac{y_i^e}{ID_i})^{r_j} \bmod n \quad \text{(xi)}$$

SK_i and SK_j are the same, because
Secret session can be computed by user U_i, as follows:

$$SK_i = (\frac{y^e{}_j}{ID_j})^{r_i} \bmod n$$

$$SK_i = (\frac{(g_j.\alpha^{r2} \bmod n)^e}{ID_j})^{r_i} \bmod n$$

$$SK_i = (\frac{(g_j)^e.(\alpha^{r2} \bmod n)^e}{ID_j})^{r_i} \bmod n$$

$$SK_i = (\frac{(ID_j{}^d \bmod n)^e.(\alpha^{e*r2} \bmod n)^e}{ID_j})^{r_i} \bmod n$$

$$SK_i = (\frac{(ID_j{}^{e*d} \bmod n).(\alpha^{e*r2} \bmod n)}{ID_j})^{r_i} \bmod n$$

$$SK_i = (\frac{(ID_j{}^{1 \bmod \phi(n)} \bmod n).(\alpha^{e*r2} \bmod n)}{ID_j})^{r_i} \bmod n$$

$$SK_i = (\frac{(ID_j \bmod n).(\alpha^{e*r2} \bmod n)}{ID_j})^{r_i} \bmod n$$

$$SK_i = (\frac{(ID_j).(\alpha^{e*r2} \bmod n)}{ID_j})^{r_i} \bmod n$$

$$SK_i = (\alpha^{e*r2} \bmod n)^{r1} \bmod n$$

$$SK_i = (\alpha^{e*r1*r2} \bmod n) \bmod n$$

$$SK_i = \alpha^{e*r1*r2} \bmod n$$

$$SK_i = \alpha^{e*r1*r2}$$

Thus,

$$SK_i = SK_j = \alpha^{e*r1*r2} \bmod n. \quad \text{(xii)}$$

As, n is very large generally, then

$$SK_i = SK_j = \alpha^{e*r1*r2}$$

3. ANALYSIS OF SECURITY

Several attacks are designed to analysis the security of the key exchange protocol, as the follows:

3.1 Prevention from brute-force attacks

Attack 1: The proposed scheme avoids problem of the RSA factorization. If an attacker can derive the private key d from the public key of the key generator center by computing $d = e^{-1} \bmod \phi(n)$, then he can obtain g_j by computing $g_i = ID_i^d \bmod n$; thus he can play the role of U_i to forge (ID_j y_i ,t_i, s_i, T_j) using (ii, (iii) and (iv). However derive the private key d using the operation $d = e^{-1} \bmod \phi(n)$ needs to factor the large integer n.

Attack 2: The proposed scheme avoids forgery attack.
The user U_i picks out a number R such that $ID_j = (ID_i.R^e) \bmod n$, where gcd(R,n)=l, and computes the private information of U_j using $g_j = ID_j^d = ID_i^d.R = g_i.R \bmod n$, then he can play the role of U_j to forge (ID_j,y_j,t_j,s_j,T_j). However, before picks out the number R, the security key d is required for the operation of $R = (\frac{ID_j}{ID_i})^d \bmod n$ as Attack 1, he still needs to factor n.

3.2 Prevention of replay attacks
In each of the communication sessions during key exchange, "two-way" authentication has been adopted to prevent the replaying attack. During key exchange process, user foils the replay attack by checking the freshness of datum using random number and timestamp.

3.3 Prevention of man-in-the-middle attacks
The proposed scheme avoids Man-in-the Middle attack. When U_i sending (ID_j y_i, t_i,s_i,T_j) to U_j , an adversary can intercept the datum from the public channel, then plays the role of U_i to cheat U_j or another users using (ID_j y_i, t_i, s_i, T_j) The attacker does not pass the verification of (ix) since both the timestamp T_i and the identification information ID_j are inputs of the one-way function h() and used in the operation of $s_i = g_i.r_i^{h(y_i,t_i,T_i,ID_j)} \bmod n$,

4. CONCLUSIONS & FUTURE WORKS

Key management is a fundamental, challenging issue in securing MANETs. This paper presents a secured ID-based key management scheme for MANETs which permits mobile nodes to derive their public keys directly from their known network identities and with some other common information. Most existing security mechanisms for MANETs thus far involve the heavy use of public key certificates. Our solution obviates the need of any inline Certification Authority (PKI) to share secret key. It also provides end-to-end authentication and enables mobile user to ensure the authenticity of user of peer node. The significant advantage of our solution is to avoid users to generate their own public keys and to then distribute these keys throughout the network. This scheme solved the security problem in the ad hoc network and is also suitable for application to other wired and wireless network. In this regard, we believe that the finding of this paper would have influence on the research paradigm of the whole community and stimulate many other fresh research outcomes. As our future work, we will seek efficient solutions based on our secure ID-based key management scheme to a variety of challenging security issues in MANETs such as intrusion detection and secure routing.

.

5. REFERENCES

1. David B. Johnson, David A. Maltz, Yih-Chun Hu, and Jorjeta G. Jetcheva, *"The Dynamic Source Routing Protocol for Mobile Ad Hoc Networks (DSR)*", IETF Mobile Ad Hoc Networks Working Group, Internet Draft, 15 April 2003.
2. P. Jacquet, P. Muhlethaler, T. Clausen, A. Laouiti, A. Qayyum and L Viennot, "*Optimized Link State Routing Protocol for Ad Hoc Networks*", In Proceeding of IEEE Int'l MulU Topic Con!. 2001, IEEE Press, pp. 62-68, 2001.
3. Nikola Milanovic, Miroslaw Malek, Anthony Davidson and Veljko Milutinovic, "*Routing and Security in Mobile Ad Hoc Networks*", IEEE Computer. Vol. 37, No.2, pp. 61-65, February 2004.
4. L. Zhou, and Z. J. Haas, "*Securing Ad Hoc Networks*", IEEE Network Journals, Vol. 13, No.6, pp. 24-30, 1999.
5. A.Weimerskirch, and D. Westhoff, "*Identity Certified Authentication for Ad Hoc Networks*", 2003 ACM Workshop on Security of Ad Hoc and Sensor Networks (SASN '03), pp. 33-40, October 31, 2003.

6. menezes, P. V. Oorschot, and S. A. Vanstone, "*handbook of Applied Cryptography*", CRC Press, New York, 1997
7. B. Newman and T. Tso. , *"Kerberos: An Authentication Service for Computer Networks*", vol. 32, no. 9, pp. 33-38, Sept. 1994
8. Jiejun Kong, Petros Zerfos, Haiyun Luo, Songwu Lu and Lixia Zhang, "*Providing Robust and Ubiquitous Security Support for Mobile Ad-Hoc Networks"*, In Proceeding of the IEEE 9th International Conference on Network Protocols (ICNP'01), IEEE Computer Society, pp. 251, 2001.
9. H. Deng, A. Mukheljee, and D.P. Agrawal, "*Threshold and Identity-based Key Management and Authentication for Wireless Ad Hoc Networks*", In Proceeding of the International Conference on Information Technology: Coding and Computing (ITCC'04), IEEE Computer Society, Vol. 1, No.1, pp. 107-111, January 2004.
10. J. Kong, P. Zerfos, H. Luo, S. Lu, and L. Zhang, "*Providing Robust and Ubiquitous Security Support for Mobile Adhoc Networks*", In Proceeding of IEEE Int'l Conf. Network Protocols, Nov. 2001
11. M. Narasimha, G. Tsudik, and J.H. Yi, "*On the Unitility of Distributed Cryptography in P2P and Manets: The Case of Membership Control*", In Proceeding of IEEE Int'l Conf. Network Protocols Nov. 2003
12. S. Yi and R. Kravets, "*Moca: Mobile Certificate Authority Wireless Ad Hoc Networks*", In Proceeding of Second Ann. PKI Research Workshop (PKI '03), Apr. 2003
13. M. Bechler, H.-J. Hof, D. Kraft, F. Pahlke, and L. Wolf, *"A Cluster-Based Security Architecture for Ad Hoc Networks*", In Proceeding IEEE INFOCOM, Mar. 2004
14. H. Luo, J. Kong, P. Zerfos, S. Lu, and L. Zhang, "*URSA: Ubiquitous and Robust Access Control for Mobile Ad Hoc Networks*", IEEE/ACM Trans. Networking, vol. 12, no. 6, pp. 1049-1063, Dec. 2004
15. Shamir, "*Identity-based cryptosystems and signature schemes*", in Advances in Cryptology - Crypto '84, Lecture Notes in Computer Science 196, Springer, pp. 47-53, Springer-Verlag, 1984.
16. M. Bohio, and A. Miri, *"An Authenticated Broadcasting Scheme for Wireless Ad Hoc Network*", In Proceedings of the Second Annual Conference on Communication Networks and Services Research (CNSR '04), IEEE Computer Society, pp. 6974, May 19-21, 2004.
17. A. Khalili, J. Katz, and W. Arbaugh, "*Toward Secure Key Distribution in Truly Ad Hoc Networks*", 2003 Symposium on Applications and the Internet Workshop (SAINT 2003), IEEE Computer Society, pp. 342-346, 2003.
18. H. Deng, A. Mukherjee, and D. Agrawal, "*Threshold and Identity-Based Key Management and Authentication for Wireless Ad Hoc Networks*", In Proceeding Int'l Conf. Information Technology: Coding and Computing (ITCC '04), Apr. 2004
19. N. Saxena, G. Tsudik, and J.H. Yi, *" Identity-Based Access Control for Ad Hoc Groups*", In Proceeding of International Conference of Information Security and Cryptology, Dec. 2004
20. Y. Zhang, W. Liu, W. Lou, Y. Fang, and Y. Kwon, "*AC-PKI Anonymous and Certificateless Public-Key Infrastructure for Mobile Ad Hoc Networks*", In Proceeding of IEEE Int'l Conf. Comm pp. 3515-3519, May 2005
21. A. Shamir, "*How to Share a Secret*," Comm. ACM, vol. 22, no. 11, pp. 612-613, 1979.
22. Y. Desmedt and Y. Frankel, "*Threshold Cryptosystems*", In Proceeding of CRYPTO '89, pp. 307-315, Aug. 1989.
23. R. L. Rivest, A. Shamir, and L. Adelman, "*A Method for Obtaining Digital Signatures and Public-Key Cryptosystems*", Comm. Of ACM Vol.21, no.2, pp. 122-126, 1978.