ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 8, August 2015

Reliable Data Recovery for Decentralized Disruption-Tolerant Military Networks

Gururaj Patil[1], Rajaram M Gowda[2]

M. Tech Student (Software Engineering), Dept. of Information Science Engineering, M S Ramaiah Institute of Technology, Karnataka, India[1]

Associate Professor, Dept. of Information Science Engineering, M S Ramaiah Institute of Technology, Karnataka, India[2]

ABSTRACT: Mobile nodes in some stimulating network situations suffer from intermittent connectivity and repeated partitions e.g. battlefield and catastrophic recovery scenarios. Disruption-tolerant network (DTN) technologies are fetching successful results that let wireless devices carried by soldiers to interconnect among themselves and access the trustworthy data or command dependably by manipulating external storage nodes. Some of the supreme challenging concerns in this situation are the execution of consent policies and the policies modernize for protected data repossession. Ciphertext-policy attribute-based encryption (CP-ABE) is an encouraging cryptographic explanation to the access control concerns. Though, the issue of applying CP-ABE in decentralized DTNs introduces numerous security and secrecy tasks with concern to the attribute revocation, key escrow, and coordination of attributes delivered from different authorities. In this paper, we offer a reliable data retrieval scheme using CP-ABE for decentralized DTNs where multiple key establishments achieve their attributes independently. We show how to put on the proposed mechanism to firmly and proficiently achieve the private data scattered in the disruption-tolerant military network.

KEYWORDS: Access control, attribute-based encryption (ABE), secure data retrieval.

I. INTRODUCTION

With the progress in technology, we have various wireless computing devices. Such devices can form structure less adhoc networks and interconnect with each other with the help of intermediary nodes. Such adhoc networks are very beneficial in numerous scenarios e.g. battlefield operations. In several military network scenarios, connections of wireless devices supported by soldiers may be momentarily cut off by blocking, environmental factors, and mobility, particularly when they function in intimidating environments. Disruption- tolerant network (DTN) technologies are fetching prosperous explanations that let nodes to interconnect with each other in these dangerous networking environments [1]–[3]. Usually, when there is no end-to-end connection among a source and a destination couple, the messages from the source node might need to wait in the midway nodes for a significant amount of time till the construction would be ultimately established.

Roy [4] and Chuah [5] presented storage nodes in DTNs where information is kept or imitated such that solitary certified mobile nodes can access the essential info rapidly and proficiently. Several military applications necessitate improved shelter of trustworthy data comprising access control approaches that are cryptographically required [6], [7]. In many circumstances, it is appropriate to offer distinguished access services such that information access strategies are well-defined over user qualities or roles that are achieved by the key consultants. For example, in a disruption-tolerant military network, a commander may stock secret information at a storage node, which must be retrieved by members of “Group 1” who are contributing in “Region 2.” In this case, it is a sensible statement that several key specialists are expected to achieve their own active attributes for soldiers in their installed regions or levels, which could be repeatedly, altered [4], [8], [9]. We mention to this DTN construction where several establishments issue and achieve their own attribute keys individually as a decentralized DTN [10].

DOI: 10.15680/IJIRCCE.2015. 0308101

The idea of attribute-based encryption (ABE) [11] [13] is an encouraging method that accomplishes the necessities for safe data retrieval in DTNs. ABE features a mechanism that allows an access control over encrypted data using access strategies and credited attributes among private keys and ciphertexts. Specifically, ciphertext-policy ABE (CP-ABE) offers an accessible way of encrypting data such that the encryptor describes the attribute set that the decryptorwishes to possess in order to decrypt the ciphertext [12]. Thus, dissimilar users are permitted to decrypt unlike pieces of data per the safety policy. Though, the difficulty of assigning the ABE to DTNs announces various security and privacy challenges. Meanwhile some users could change their associated attributes at some point, or some private keys might be compromised, key withdrawal (or update) for each attribute is essential to make systems protected. Though, this topic is even more problematic, particularly in ABE systems, and then each attribute is possibly shared by several users. This infers that withdrawal of any attribute or any single user in an attribute group would mark the other users in the group. It may outcome in blockage in rekeying process, or security deprivation due to the windows of weakness if the earlier attribute key is not updated instantaneously. Additional task is the key escrow problem. In CP-ABE, the key expert produces private keys of users by relating the authority's master secret keys to users' related group of attributes. Therefore, the key authority can decrypt each ciphertext addressed to definite users by producing their attribute keys.

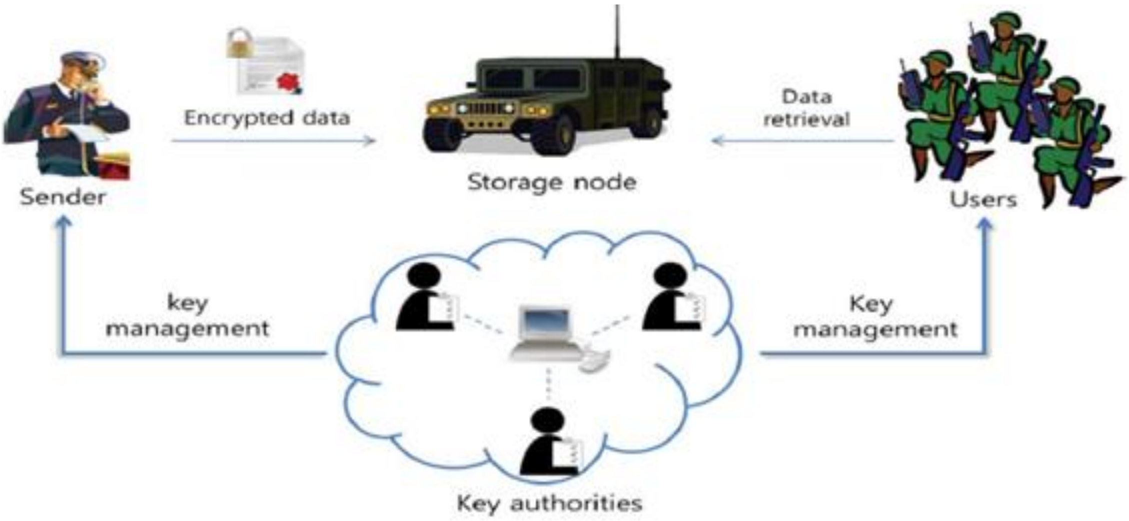

Fig 1: Architecture of secure data retrieval in a disruption – tolerant military network

If the key authority is co-operated by adversaries when installed in the inimical environments, this could be a possible danger to the files privacy or secrecy specifically when the data is extremely subtle. The key escrow is an intrinsic issue even in the various-authority systems provided that each key authority has the entire honour to produce their individual attribute keys with their own chief secrets. The last task is the direction of attributes delivered from dissimilar authorities. When several authorities bring about and issue attribute keys to users independently with their own master secrets, it is very difficult to express fine-grained access strategies over attributes given out from various authorities.

II. Related work

Preceding work on DTNs has been centred on numerous expectations about connectivity and the accessibility of environmental information and control. A number of the suggested routing procedures for DTNs mark little expectations and are hence broadly suitable.

ABE comes in two flavours known key-policy ABE (KP-ABE) and ciphertext-policy ABE (CP-ABE). In KP-ABE, the encryptor only gets to tag a ciphertext with a group of attributes. The key authority selects a rule for each user which decides which ciphertexts he can decrypt and issues the key to each user by embedding the policy into the user's key. However, the parts of the ciphertexts and keys are inverted in CP-ABE. In CP-ABE, the ciphertext is encoded with an access rule selected by an encryptor, nevertheless a key is solely created with respect to an attributes group. CP-ABE is more suitable to DTNs than KP-ABE since it allows encryptors such as a commander to select an access rule on attributes and to encrypt intimate info under the access organisation via encrypting with the conforming public keys [4], [7], [14].

1) *Attribute Revocation:* Bethencourt*et al.* [12] and Boldyreva*et al.* [15] first recommended key cancellation methods in CP-ABE and KP-ABE, individually. Their explanations are to attach to each attribute a termination date (or time) and dispense a new set of keys to effective users after the expiration.

2) *Key Escrow:* Maximum of the current ABE systems are built on the architecture where a solitary trusted consultant has the control to produce the entire private keys of users with its master furtive information [11], [12], [13], [16]–[18]. Therefore, the key escrow difficulty is essential such that the key authority can decode each ciphertext addressed to users in the system by producing their secret keys at any stage.

III. **NETWORK ARCHITECTURE**

In this piece, we define the DTN construction and outline the security model.

A. System Description and Assumptions

The architecture comprises of the following system objects.

1) Key Authorities: They are key generation centres which produce public/secret bounds for CP-ABE. The key authorities comprise of a central authority and numerous local authorities. We assume that there are safe and dependable communication networks among a central consultant and each local authority through the early key arrangement and generation phase. Each local authority manages different attributes and issues corresponding attribute keys to users.

2) Storage node: This is an object that stocks data from senders and offer conforming admittance to users. Like to the preceding systems, we also undertake the storage node to be partially confidential that is honest-yet-curious.

3) Sender: This is a unit who possesses trustworthy posts or information (e.g., a commander) and desires to stock them into the exterior data storing node for simplicity of distribution or for consistent distribution to users in the risky networking environments.

4) User: This is a moveable node who desires to access the information deposited at the storage node (e.g., a soldier).

B. Threat Model and Security Requirements

1) Data confidentiality: Users who do not have the access to the data should be prevented from accessing the data and unauthorised users must be prevented from accessing the data.

2) Collusion-resistance: When multiple users are there in the network, then the users may club the information they have and decode the information, care must be taken that even after combining the attributes the information shouldn’t be decrypted.

3) Backward and forward Secrecy: ABE system has backward secrecy, which does not allow any user from accessing the previous text that has the access to the data. In contrast forward secrecy refers that any users who access an attribute must be prohibited from accessing the plaintext of the succeeding data swapped after he drops the attribute.

IV. **PROPOSED SCHEME**

In this division, we offer a multi-authority CP-ABE system for safe data recovery in distributed DTNs. Every local authority concerns fractional modified and attribute key constituents to a user by executing reliable 2PC protocol with the vital authority. Every attribute key of a user can be rationalized independently and instantaneously. Therefore, the scalability and safety can be improved in the proposed system.

Table 1: Expressiveness, Key Escrow, and Revocation Analysis

Scheme	Authority	Expressiveness	Key Escrow	Revocation
BSW[13]	Single	-	Yes	Periodic attribute revocation
HV[9]	Multiple	AND	Yes	Periodic attribute revocation
RC[4]	Multiple	AND	Yes	Immediate system-level user revocation
Proposed	Multiple	Any monotone access structure	No	Immediate system-level user revocation

Table I displays the authority architecture, logic expressiveness of access structure that can be well-defined under diverse disjoint sets of attributes (managed by different authorities), key escrow, and revocation granularity of each CP-ABE scheme.

Table 2: Efficiency Analysis

System	Ciphertext size	Rekeying message	Private key size	Public key size
BSW[13]	$(2t + 1)C_0 + C_1 + C_T$	$l(2k + 1)C_0$	$(2k + 1)C_0$	$C_0 + C_1$
HV[9]	$(2t + m)C_0 + mC_1 + C_T$	$l(2k + 1)C_0$	$(2k + m)C_0$	$mC_0 + mC_1$
RC[4]	$(2t + 3r + m)C_0 + mC_1 + C_T$	0	$(3k + 2m)C_0$	$M(t + 4)C_0 + mC_1$
Proposed	$(2t + 1)C_0 + C_1 + C_T$	$(n-1) \log n/n-1\ C_p$	$(2k + 1)C_0 + \log n\ C_k$	$C_0 + mC_1$

C_0: bit size of an element in G_0, C_1: bit size of an element in G1, C_p: bit size of an element in Z_p,
C_k: bit size of a KEK, C_T: bit size of an access tree T in the ciphertext, r: the number of revoked users,
l: the number of users in an attribute group, n: the number of all users in the system,
m: the number of authorities in the system, k: the number of attributes associated with private key of a user,
u: the number of attributes in the system, t: the number of attributes appeared in T.

Table II summarizes the efficiency comparison results among CP-ABE schemes. In the comparison, rekeying message size represents the communication cost that the key authority or the storage node needs to send to update nonrevoked users' keys for an attribute. Private key size represents the storage cost required for each user to store attribute keys or KEKs. Public key size represents the size of the system public parameters. In this comparison, the access tree is constructed with attributes of different authorities except in BSW of which total size is equal to that of the single access tree in BSW.

Meanwhile the first CP-ABE system offered by Bethencourt*et al.* [12], lots of CP-ABE schemes have been suggested [7], [16]–[18]. The consequent CP-ABE schemes are typically encouraged by further difficult safety immune in the customary model. Though, furthermost of the outlines were unsuccessful to attain the feeling of the Bethencourt*et al.*'s scheme, that defined a proficient scheme that was animated in that it certified an encryptor to express an admittance base in associations of any monotonic method above attributes. Therefore, in this unit, we cultivate a difference of the CP-ABE algorithm partly established on (but not limited to) Bethencourt*et al.*'s building in order to improve the poignancy of the access control policy instead of building a new CP-ABE scheme from scratch.

V.ANALYSIS

In this section, we analyze and compare the efficiency of the proposed scheme to the former multiauthority CP-ABE schemes in hypothetical aspects. Then, the proficiency of the projected scheme is verified in the network reproduction in terms of the communication cost. We also discuss its efficiency when applied with precise parameters and relate these effects to those acquired by the other schemes.

A. Efficiency

In the proposed scheme, the logic can be very expressive as in the single authority system like BSW [12] such that the access policy can be expressed with any monotone access structure under attributes of any chosen set of authorities; while HV [9] and RC [4] schemes only allow the AND gate among the sets of attributes managed by different authorities. The revocation in the proposed scheme can be done in an immediate way as opposed to BSW. Therefore, attributes of users can be cancelled at any time even before the expiration time that might be set to the attribute. This enhances security of the stored data by reducing the windows of vulnerability. In addition, the proposed scheme realizes more fine-grained user revocation for each attribute rather than for the whole system as opposed to RC. Thus,even if a user comes to hold or drop any attribute during the service in the proposed scheme, he can still access the data with other attributes that he is holding as long as they satisfy the access policy defined in the ciphertext. The key escrow problem is also resolved in the proposed scheme such that the confidential data would not be revealed to any curious key authorities.

As shown in Table II, the proposed scheme needs rekeying message size of at most to realize user-level access control for each attribute in the system. Although RC does not need to send additional rekeying message for user revocations as opposed to the other schemes, its ciphertext size is linear to the number of revoked users in the system since the user revocation message is included in the ciphertext. The proposed scheme requires a user to store more KEKs than BSW. However, it has an effect on reducing the rekeying message size. The proposed scheme is as efficient as the basic BSW in terms of the ciphertext size while realizing more secure immediate rekeying in multiauthority systems.

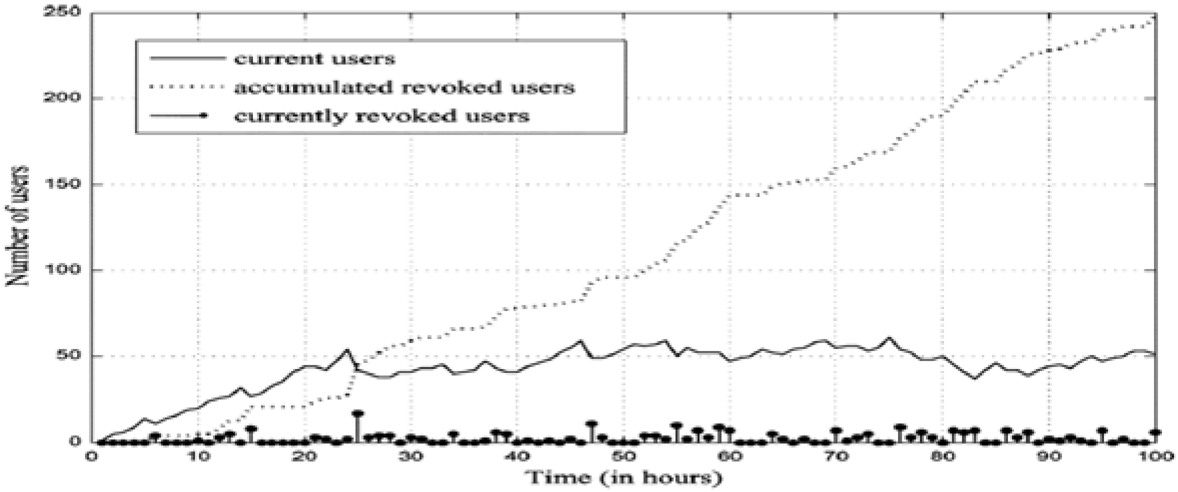

Fig 2: Number of users in the attribute group

We assume that user join and leave events are independentlyand identically distributed in each attribute group following Poisson distribution. The membership duration time for an attribute is assumed to follow an exponential distribution. We set the interarrival time between users as 20 min and the average membership duration time as 20 h. Fig. 2 represents the number of current users and revoked users in an attribute group during 100 h. Fig. 3 shows the total communication cost that the sender or the storage node needs to send on a membership change in each multiauthority CP-ABE scheme. It includes the ciphertext and rekeying messages for nonrevoked users. It is measured in bits.

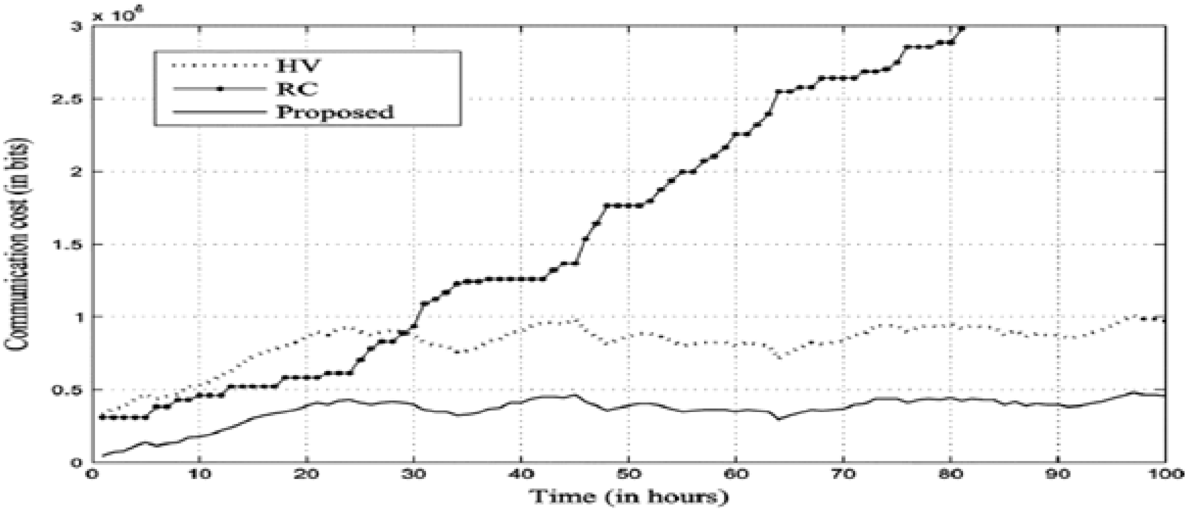

Fig 3: Communication cost in the multiauthority CP-ABE systems

B. Simulation

In this simulation, we consider DTN applications using the Internet protected by the attribute-based encryption. Almeroth and Anmar [19] demonstrated the group behavior in the Internet's multicast backbone network (MBone). They showed that the number of users joining a group follows a Poisson distribution with rate , and thememembership duration time follows an exponential distribution with a mean duration . Since each attribute group can be shown as an independent network multicast group where the members of the group share a common attribute, we show the simulation result following this probabilistic behavior distribution [19].

We suppose that user join and leave events are independently and identically distributed in each attribute group following Poisson distribution. The membership duration time for an attribute is assumed to follow an exponential distribution. We set the interarrival time between users as 20 min and the average membership duration time as 20 h .

In this simulation, the total number of users in the network is the time result. In this analysis, we assume that the access tree in the ciphertext is a complete binary tree. Therefore, we can observe that there is a tradeoff between computational overhead and granularity of access control, which is closely related to the windows of vulnerability. However, the computation cost for encryption by a sender and decryption by a user are more efficient compared to the other multiauthority schemes.

VI. Conclusion

DTN expertise are attracting positive results in military applications which let wireless devices to connect with each other and access the trusted data consistently by manipulating exterior storage nodes. CP-ABE is an accessible cryptographic clarification to the access control and protected data recovery problems. In this paper, we suggested an effective and safe data recovery method by means of CP-ABE for dispersed DTNs where several key authorities accomplish their attributes self-reliantly.The essential key escrow difficult is fixed such that the privacy of the deposited data is certain even under the aggressive situation where key authorities might be conceded or not fully reliable. In accumulation, the fine-grained key cancellation can be complete for each attribute group. We validate how to put on the planned mechanism to firmly and proficiently accomplish the intimate data distributed in the disruption-tolerant military network.

DOI: 10.15680/IJIRCCE.2015. 0308101

REFERENCES

1. J. Burgess, B. Gallagher, D. Jensen, and B. N. Levine, "Maxprop: Routing for vehicle-based disruption tolerant networks," in *Proc. IEEE INFOCOM*, 2006, pp. 1–11.
2. M. Chuah and P. Yang, "Node density-based adaptive routing schemefor disruption tolerant networks," in *Proc. IEEE MILCOM*, 2006, pp.1–6.
3. M. M. B. Tariq, M. Ammar, and E. Zequra, "Mesage ferry route designfor sparse ad hoc networks with mobile nodes," in *Proc. ACM MobiHoc*, 2006, pp. 37–48.
4. S. Roy andM. Chuah, "Secure data retrieval based on ciphertextpolicyattribute-based encryption (CP-ABE) system for the DTNs," LehighCSE Tech. Rep., 2009.
5. M. Chuah and P. Yang, "Performance evaluation of content-basedinformation retrieval schemes for DTNs," in *Proc. IEEE MILCOM*,2007, pp. 1–7.
6. M. Kallahalla, E. Riedel, R. Swaminathan, Q. Wang, and K. Fu,"Plutus: Scalable secure file sharing on untrusted storage," in *Proc. Conf. File Storage Technol.*, 2003, pp. 29–42.

7 L. Ibraimi, M. Petkovic, S. Nikova, P. Hartel, and W. Jonker, "Mediatedciphertext-policy attribute-based encryption and its application," in*Proc. WISA*, 2009, LNCS 5932, pp. 309–323.

8 N. Chen, M. Gerla, D. Huang, and X. Hong, "Secure, selective groupbroadcast in vehicular networks using dynamic attribute based encryption,"in*Proc. Ad Hoc Netw. Workshop*, 2010, pp. 1–8.

9 D. Huang and M. Verma, "ASPE: Attribute-based secure policy enforcementin vehicular ad hoc networks," *Ad Hoc Netw.*, vol. 7, no. 8,pp. 1526–1535, 2009.

10 A. Lewko and B. Waters, "Decentralizing attribute-based encryption,"CryptologyePrint Archive: Rep. 2010/351, 2010.

11 A. Sahai and B. Waters, "Fuzzy identity-based encryption," in *Proc.Eurocrypt*, 2005, pp. 457–473.

12 J. Bethencourt, A. Sahai, and B. Waters, "Ciphertext-policy attributebasedencryption," in *Proc. IEEE Symp. Security Privacy*, 2007, pp.321–334.

13 R. Ostrovsky, A. Sahai, and B. Waters, "Attribute-based encryptionwith non-monotonic access structures," in *Proc. ACM Conf. Comput.Commun. Security*, 2007, pp. 195–203.

14 S. Yu, C. Wang, K. Ren, and W. Lou, "Attribute based data sharingwith attribute revocation," in *Proc. ASIACCS*, 2010, pp. 261–270.

15 A. Boldyreva, V. Goyal, and V. Kumar, "Identity-based encryptionwith efficient revocation," in *Proc. ACM Conf. Comput. Commun. Security*,2008, pp. 417–426.pp. 26–35.

16 L. Cheung and C. Newport, "Provably secure ciphertext policy ABE,"in*Proc. ACM Conf. Comput. Commun. Security*, 2007, pp. 456–465.

17 V.Goyal, A. Jain,O. Pandey, andA. Sahai, "Bounded ciphertextpolicyattribute-based encryption," in *Proc. ICALP*, 2008, pp. 579–591.

18 X. Liang, Z. Cao, H. Lin, and D. Xing, "Provably secure and efficientboundedciphertext policy attribute based encryption," in *Proc. ASIACCS*,2009, pp. 343–352.

19 K. C. Almeroth and M. H. Ammar, "Multicast group behavior in theInternet's multicast backbone (MBone)," *IEEE Commun. Mag.*, vol.35, no. 6, pp. 124–129, Jun. 1997.