IOSR Journal of Computer Engineering (IOSR-JCE)
e-ISSN: 2278-0661,p-ISSN: 2278-8727,
PP 50-57
www.iosrjournals.org

Mobile Ad-hoc Network Using P-Encryption Scheme

Shraddha R. Satpute[1] , Archita B. Deore [2], Pradnya R.Nandwalkar[3],
Sagar B.Kothale[4], Kavita S.Kumavat[5]
[1,2,3,4,5](I.T. Dept. ,B.V.C.O.E.&R.I. Anjaneri ,SPPUniv.Pune, India)

Abstract: *As MANET edge closer toward wide-spread deployment, security issues have become a central concern and are increasingly important. Various security mechanisms have been proposed, widely used, and proven to be effective in wired networks, but no single mechanism provides all the services required in a MANET. Due to certain characteristics of MANETs, some security mechanisms are not applicable to this environment. These certain characteristics of ad hoc networks include: lack of a network infrastructure and online administration, the dynamics of the network topology and node membership, the potential attacks from inside the network. an important issue in Mobile Ad Hoc Networks (MANETs) is Energy saving. the energy consumption can be reduced by network coding in MANETs by using less transmissions. However ,there are other sources of energy consumption, e.g., data encryption/decryption. To point this issue energy saving encryption scheme called Enhanced P-Coding is proposed for MANETs , by exploiting networking coding technique. let source compress the coded messages (prefixed with coding vectors) is basic idea of Enhanced P-coding using run length encoding technique and hence the original message is said to be encrypted efficiently since for the eavesdropper to obtain any meaningful information from compressed data is very difficult task.A Mobile ad hoc Network (MANET) is a self-governing network comprised of free roaming nodes which communicate wireless by radio transmission*

Keywords*–. MANET, Mobile ad hoc networks, energy saving, network coding, lightweight encryption*

I. Introduction

A new alternative way for mobile communication, in which mobile devices form a self creating, self-organizing and self-administering wireless network, called a *mobile ad hoc network* .Wireless network technology enables computing devices to communicate with each other without any physical medium. Compared with wired networks, wireless communication provides better connectivity and mobility, which allows mobile devices to access other local area networks or the Internet at anytime and anywhere. The benefits of flexible routing, global connectivity and a highly adaptive potential make mobile ad-hoc networks (MANET) suitable for a wide range of applications in both military and commercial environments, such as battlefields, disaster relief operations, mobile device/ personal networking, mobile information sharing and vehicular networks The wireless network architecture is be classified in two ways, first one is infrastructure where the node are connected with the fixed physical representation.

Thus, the nodes are communicated through AP Examples for these kinds of wireless networks are GSM, UMTS and WLAN etc. Second is infra structure less where the node is communicated without any fixed physical rep.

Fig 1.eg of MANET

The ad hoc networks are formed by connecting the terminals in the multi-hop distributed architecture absence of centralized structure, the nodes in the ad hoc network acts as router to send and receive the data. Due to the non-static nature, ad hoc network avoid the single point of failure and make the network more robustness.

Research on security of MANETs remains active, in spite of years of exploration, in both academia and industry. It is partially due to the fact that no mature solution is widely accepted and the growing availability of small, personalized mobile devices with peer to peer communication capability through wireless channels.

General security requirements for MANETs include [1]: Data Confidentiality that keeps data secret to outsiders, Data Integrity that prevents data from being altered, Data Freshness that keeps data in the correct order and up-to-date, Data Availability that ensures data to be available on request, Data & Identity Authentication that verifies that the data or request came from a specific, valid sender, and Non-repudiation that ensures a node cannot deny sending a message.

Security mechanisms that are widely used and proven to be effective in wired networks are not always applicable to MANETs. Attacks that can be effectively detected and prevented in wired networks have been big security challenges in MANETs. Examples include, but are not limited to, identity/address spoofing, message tampering and forgery, message replay, etc. Compared to wired networks, the combination of the following characteristics of MANETs makes it especially difficult to achieve security requirements:

- Lack of a network infrastructure and online administration.
- Network topology and node membership dynamics.
- The potential insider attacks.

MANET security goals:
MANETs (Mobile adhoc networks) provide security services such as
• Authentication
• Confidentiality
• Integrity
• Availability

Issues of Mobility in Ad hoc Networks:
Mobility affects
• Single Transmission
• Channel access
• Routing
• Multicasting

II. Liturature Survey

[1] P. Zhang, Y. Jiang, C. Lin, Y. Fan, and X. Shen, ‘‘P-coding: Secure Network Coding against Eavesdropping Attacks, ‘This paper proposes an under a layered model of remote systems. The straight program can be utilized to discover vitality every bit for multicasting in Portable Ad hoc Networks Because of the linearity of the estimating plan it is conceivable to accomplish least vitality every bit for directing utilizing single dissemination tree. A Unified investigation of least vitality multicasting with system coding and directing is displayed. A remote impromptu system is displayed as a diagram which is made out of structures in type of trees speaking to physical show joins. Every edge of the diagram has a value, which is the vitality every bit for the relating telecast join. The base vitality multicasting detailing adds up to minimizing the aggregate expense of the expended bit-rates on the edges, while giving a unit multicast rate.

[2] S. Singh, C. Raghavendra , and J. Stepanek, ‘‘Power-Aware Broadcasting in Mobile Ad Hoc Networks ’In this paper they present five different power-aware metrics based on battery power consumption at nodes for determining broadcast routes in wireless ad hoc networks. they show that using these metrics in a power-aware broadcasting algorithm reduces the cost/broadcast of routing packets to all destinations by 5-50%over a broadcast tree constructed using a greedy strategy based on network topology information only(this cost reduction is on top of a 40-70%reduction in energy consumption obtained by using PAMAS, our MAClayer protocol).

[3] Y. Wu, P. Chou, and S. Kung, ‘‘Minimum-Energy Multicast in Mobile Ad Hoc Networks using Network Coding In this paper ,we consider the problem of minimum-energy information multicast ,namely transmitting common information from a source nodes to a set of destination nodes with the minimum amount of total consumed energy per information bit,in a mobile ad hoc network(MANET).

III. Proposed System

This paper proposes an under a layered model of wireless networks. The linear program can be used to find energy per bit for multicasting in Mobile Ad hoc Networks s. Due to the linearity of the pricing scheme it is possible to achieve minimum energy per bit for routing using single distribution tree. A Unified study of

minimum energy multicasting with network coding and routing is presented. A wireless ad hoc network is modeled as a graph which is composed of structures in form of trees representing physical broadcast links. Each edge of the graph has a price, which is the energy-per-bit for the corresponding broadcast link.

The P-Coding is to perform permutation encryptions on the coded messages.

The P-Coding has three stages:

1. Source encoding: Suppose a source has h messages which is denoted by column vectors $x_i \ldots . x_h$ to be sent out. These h is prefixes first with their corresponding unit vectors, by the following Eq.

$$[\boldsymbol{u}_i, \boldsymbol{x}_i] = \left[\underbrace{0, \ldots, 0}_{i-1}, 1, \underbrace{0, \ldots, 0}_{h-i}, x_{i,1}, \ldots, x_{i,l}\right]$$

where each u_i is termed as a tag. The same coding operation is performed on these tags, each packet will contain its GEV automatically. After that the source will perform linear combinations on the h messeges using randomly chosen LEVs. for the instance, LEV $\beta(e_i)$ of output link e_i, we can get the coded message $y(e_i) = [\beta(e_i), \beta(e_i)X]$, where $X= [x_1^T \ldots . , x_h^T]^T$. Finally, the source performs permutation encryption on each message $y(e_i)$ to get its ciphertext $c[y(e_i)]=E_k[y(e_i)]$.

2. Intermediate recoding :
Symbols of messages and corresponding GEVs are rearranged via PEF, and the intermediate nodes have no knowledge of the key being used, it is rather difficult for them to reconstruct source messages.
$c[y(e_i)] = c\left[\sum_{e' \epsilon r^-(v)} \beta_{e'}(e) y(e')\right] = \sum_{c' \epsilon r^-(v)} \beta_{e'}(e) c[y(e')]$.

3. Sink decoding :
For each sink node , on receiving a message $c[y(e_i)]$ from its incoming link $e_i \epsilon r^-(v)$, it decrypts the message by performing decryption on it .

$$D_k\{c[y(e_i)]\} = E_k^{-1}\{E_k[y(e_i)]\} = y(e_i)$$

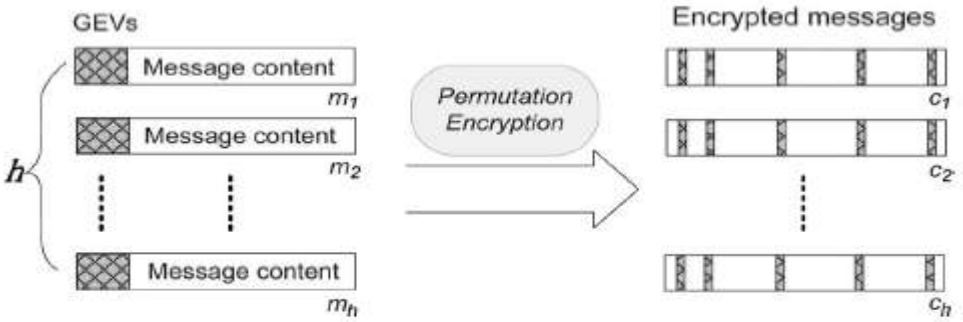


Fig 2. Permutation encryption

Advantages of Enhanced P-Coding

 Compression of coded message using run length coding is done. Eavesdroppers cannot obtain the meaningful information from the compressed data. Hence compressed data can be called as encrypted data which is transmitted to the sink.

 Faster transmission time across the network and reduced transmission cost due to run length coding.

 Intermediate recoding is avoided. No extra effort or computation is needed at intermediate nodes and energy consumption at intermediate nodes is reduced. Random linear coding and run length coding are quite simple and vulnerable to cryptographic analysis.

 Enhanced PCoding is quite lightweight in computation. In addition, Enhanced P-Coding does not cause any space overhead either.

Enhanced P-Coding reduces the encryption time due to the light weight nature of random linear coding and run length coding. Lesser the encryption time also means fewer CPU cycles, and less energy consumptions. Thus Enhanced P-Coding incurs minimal energy consumption for encryptions/decryptions compared to other encryption schemes.

IV. System Architecture

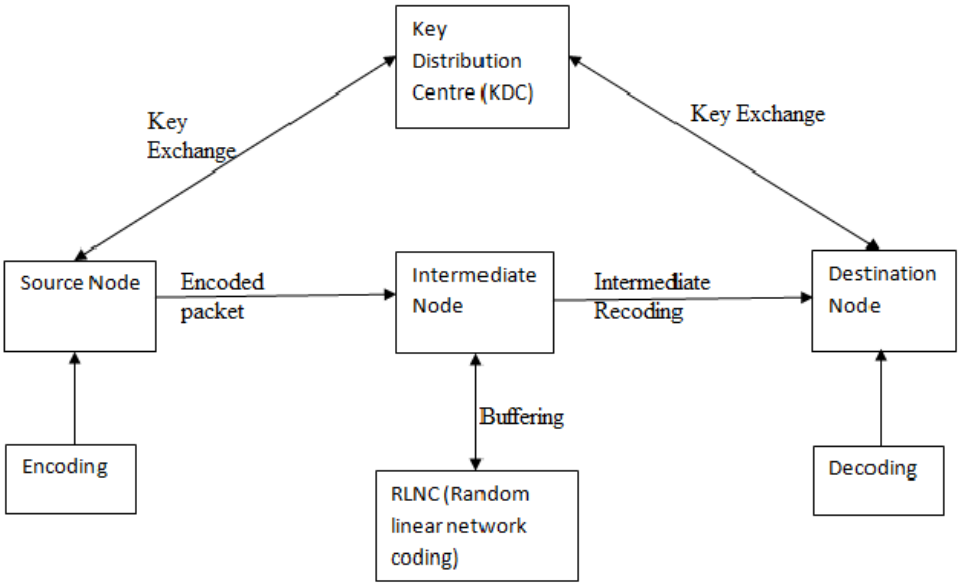


Fig 3.System Architecture

Source node:-In source node there will be message can be encoded in packet and that encoded packet can be send to intermediate node .

Intermediate node:- In the intermediate node the message which can be send by the source node it will be the intermediate recording and received by destination node . There can be the rearrange the global encoding vector. also the buffering form of random liner network coding.

Destination node-In this stage the message is receive from Intermediate node that send by source node receive message then decrypts for receiving the original message this operation perform the permutation decryption.

Key distribution center:-In that the key exchange between source node and destination node .

V. Algorithm

Algorithm shows p-coding strategy in the system as follow-

Input: a permutation k of length$n$, integers n, m, s, d
with$1 \leq m \leq n, s \in [0, n-m+1]$ and $d \in [0, m!-1]$

output: a permuted permutation $\tilde{Q}$ of length n

P_1 : // to generate the sequence $(a_1, \ldots\ldots, a_{m-1})$

For each$i \in [1, m-1]$**do**

$$\begin{vmatrix} a(i) \leftarrow d\%(i+1); \\ d = \left\lfloor \frac{d}{i} + 1 \right\rfloor; \end{vmatrix}$$

End

P_2 : //to generate the sequence $(b_1, \ldots\ldots, b_{m-1})$
For each $i \in [1, m-1]$**do**

$$|b(i) \leftarrow m - a(m-i);$$

End

P_3 : // Initialization of attributes
For each $i \in [1, n]$**do**

$$|w(i) \leftarrow i;$$

End
P_4 : // to calculate the partial permutation
For each $i \in [1, m-1]$ **do**

$$|w(s-1+i) \leftrightarrow w(s-1+b(i));$$

End

P_5 :// to perturb the current key Qusing w
For each $i \in [1, n]$**do**

$$|\tilde{Q}(i) \leftarrow w(Q(i));$$

End

Return $\tilde{Q}$;
Algorithm for text to ASCII

Input: Permutation k of length integer n, string s char c,
Output: Ascii of a of length i,
//to generate the sequence of ascii (a1,a2,a3,….an)
For each i ϵ (x1, ….xn)do
a(i) ← prefix end
string s
create object o;
string s=New string builder ()
for each char c do
string to char conversion(c)
int ascii=(int i) char c:
return ascii;

VI. Result

We have seen from the previous study that there are lots and lots of the method which provide the security to the wireless network. It is really hard to design and develop an authentication protocol which is applicable for the global mobility network. There are many reasons for the same but still we can figure it out and it is that there are more susceptible to attacks and each user has limited energy, processing and storage resources. Recently, some authentication schemes with user anonymity for the wireless network GLOMONET have been proposed. The paper shows some weaknesses in those schemes. The main contribution of the paper a secure and lightweight user authentication scheme which is highly acceptable for many wireless network. The main reason for it's low cost is it's low-cost functions which is use for authentication purpose. One of the authentication function such as one-way hash functions and exclusive-OR operations to achieve security. Just because of these features we can say that it's suitability if higher for the energy limited mobile devices. At the other end, the home agent only needs to receive one message and send one message to authenticate the mobile user. Therefore, this protocol enjoys both computation and communication efficiency as compared to the well-known authentication schemes. It also shows that this method enjoys important security attributes such as preventing the various kinds of attacks, single registration, user anonymity, user friendly, no password/verifier table, no synchronized time mechanisms, high efficiency in password authentication, use of one-time session key between mobile user and foreign agent, etc. Furthermore, one of the new features in our proposal is: it is secure in the case that the information stored in the smart card is disclosed but the user password of the smart card owner is unknown to the adversary.

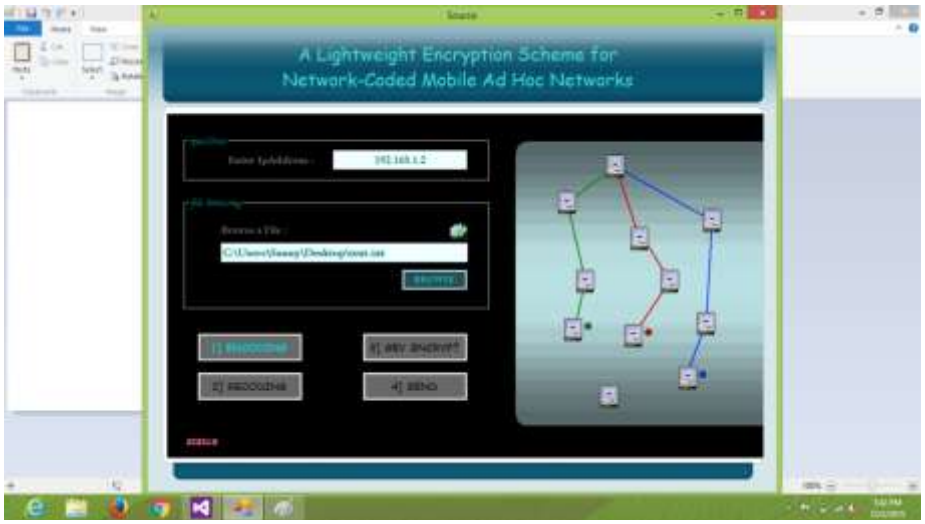


Fig 4. Main window:

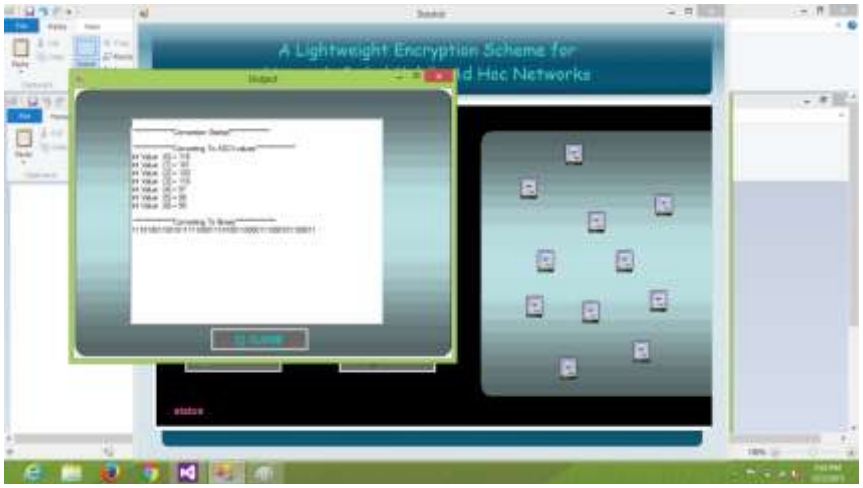


Fig 5. Encoding message:

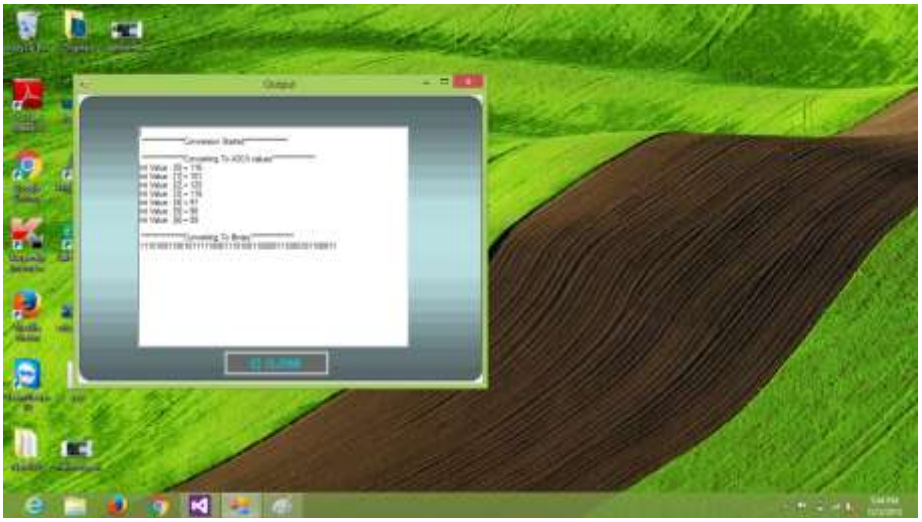
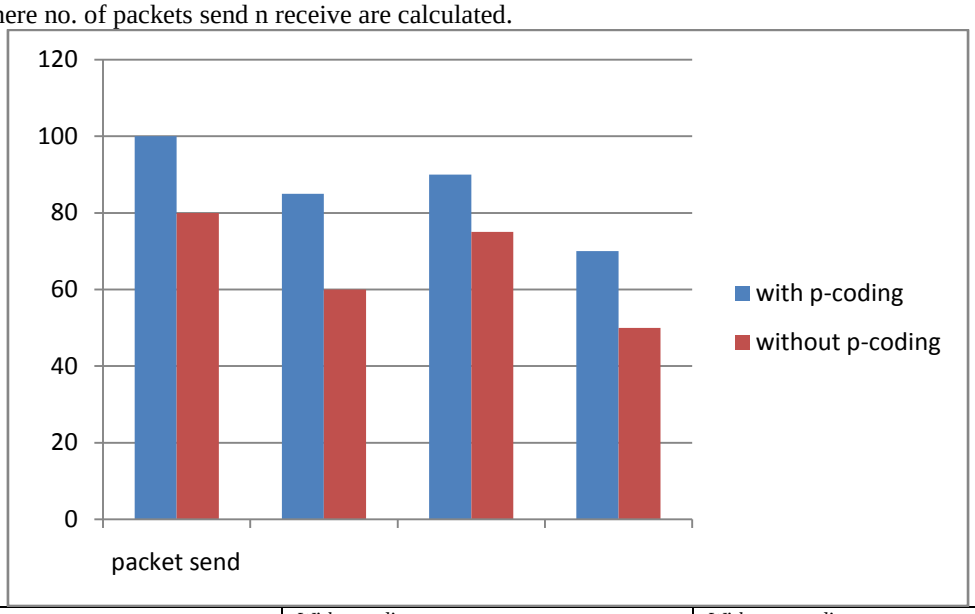


Fig 6. Send Information:

Result shows efficiency of p coding using source encoding. The below graph shows the result of p encoding scheme where no. of packets send n receive are calculated.



	With p coding	*Without p coding*
Packet send	*100*	*80*
	85	*60*
	90	*75*
	70	*50*

VII. Conclusion

The problem of energy saving in MANETs based on the technique of network coding is studied. Previous studies demonstrated that network coding can reduce energy consumption with less transmission in MANETs .Enhanced P-Coding, an energy encryption scheme on top of network coding is proposed to further reduce energy consumption in MANETs by cutting the security cost and transmission cost. Enhanced P-Coding exploits the intrinsic security property of network coding and uses simple run length coding to generate considerable confusion to eavesdropping adversaries. Hence Enhanced P-Coding is efficient in computation and incurs less energy consumption for encryptions/decryptions. The rapid developments in the field of ad hoc networking allows the nodes to form a self-creating, self-organizing and self-administering wireless network. Its intrinsic flexibility, lack of infrastructure, ease of deployment, auto configuration, low cost and potential applications makes it an essential part of future pervasive computing environments.

VIII. Futured Contribution

In this paper, we presented many kind of protocols to preserve the privacy or security of the data. This paper studied the problem of energy saving in MANETs based on the technique of network coding. Previous studies demonstrated that network coding can reduce energy consumption with less transmission in MANETs. Network-Coding exploits the intrinsic security property of network coding, and uses simple permutation encryptions to generate considerable confusion to eavesdropping adversaries. We showed that Network-Coding is efficient in computation, and incurs less energy consumption for encryptions/decryptions.

Acknowledge

We are extremely thankful to our guide Prof. K. S. Kumavat for suggesting topic for survey and providing all the assistance needed to complete the work. She inspired us to work in this area.

References

[1] P. Zhang, Y. Jiang, C. Lin, Y. Fan, and X. Shen, ‘‘P-coding: Secure Network Coding Against Eavesdropping Attacks,’’ in Proc. IEEE INFOCOM, Mar. 2010, pp. 1-9.
[2] S. Singh, C. Raghavendra, and J. Stepanek, ‘‘Power-Aware Broadcasting in Mobile Ad Hoc Networks,’’ in Proc. IEEE PIMRC, 1999, pp. 1-10.
[3] J. Wieselthier, G. Nguyen, and A. Ephremides, ‘‘Algorithms for Energy-Efficient Multicasting in Static Ad Hoc Wireless Networks,’’ Mobile Netw. Appl., vol. 6, no. 3, pp. 251-263, June 2001.

[4] B. Chen, K. Jamieson, H. Balakrishnan, and R. Morris, ‘‘Span: An Energy-Efficient Coordination Algorithm for Topology Maintenance in Ad Hoc Wireless Networks,’’ Wireless Netw., vol. 8, no. 5, pp. 481-494, Sept. 2002.
[5] R. Ahlswede, N. Cai, S.-Y.R. Li, and R.W. Yeung, ‘‘Network Information Flow,’’ IEEE Trans. Inf. Theory, vol. 46, no. 4,pp. 1204-1216, July 2000.
[6] Y. Wu, P. Chou, and S. Kung, ‘‘Minimum-Energy Multicast in Mobile Ad Hoc Networks using Network Coding,’’ IEEE Trans.Commun.,vol.53,no.11,pp.1906-1918,Nov2005
[7] M.D. Russell, J.A. Clark, and S. Stepney, ‘‘Making the Most of Two Heuristics: Breaking Transposition Ciphers with Ants,’’ in Proc.Congr.Evol.Comput.,2003,pp.2653-2658.
[8] P. Paillier, ‘‘Public-Key Cryptosystems based on Composite Degree Residuocity Classes,’’ in Proc. EUROCRYPT, May 1999, pp. 233-238. [9] D.W. Carman, P.S. Kruus, and B.J. Matt, ‘‘Constraints and approaches for distributed sensor network security (Final),’’ NAILabs, Glenwood, MD,USA,DARPAProj.Rep.,2000.
[10] K. Aoki and H. Lipmaa, ‘‘Fast Implementations of AES Candidates,’’ in Proc. 3rd AES Candidate Conf., 2000, pp. 13-14.