Combinatorial Structures for Design of Wireless Sensor Networks

Dibyendu Chakrabarti and Jennifer Seberry

Applied Statistics Unit, Indian Statistical Institute,
203 B T Road, Kolkata 700 108
University of Wollongong, Northfields Av.,
NSW 2522, Australia
dibyendu_r@isical.ac.in, jennie@uow.edu.au

Abstract. Combinatorial designs are very effective tools for managing keys in an infrastructure where power and memory are two major constraints. None of the present day wireless technologies takes the advantage of combinatorial designs. In this paper, we have proposed a general framework using combinatorial designs which will enable the participating devices to communicate securely among themselves with little memory and power overhead. The scheme caters for different kinds of user requirements and allows the designer to choose different combinatorial designs for different parts or levels of the network. This general framework will find application in all wireless radio technologies, typically WPANs and WLANs. This is a hitherto unexplored technique in wireless technologies.

Keywords: Combinatorial Design, Sensor Network, Key Predistribution, Projective Plane, Transversal Design.

1 Introduction

Combinatorial designs are very effective tools for managing keys in an infrastructure where power and memory are two major constraints. None of the present day wireless technologies takes the advantage of combinatorial designs. In this paper, we have proposed a general framework using combinatorial designs which will enable the participating devices to communicate securely among themselves with little memory and power overhead. The scheme caters to different kinds of user requirements and allows the designer to choose different combinatorial designs for different parts or levels of the network. A few examples of WLAN technologies are IEEE 802.11a/b/e/g/h/i, HiperLAN/2, HomeRF etc. and on the other hand, Bluetooth, ZigBee, UWB etc. are examples of WPAN technologies.

Very recently it is reported that two researchers have been successful in cracking the Bluetooth PIN [18]. The other wireless LAN technology protocol 802.11x also suffers from several security loopholes: insertion attacks, interception and monitoring wireless traffic, misconfiguration, jamming and client to client attacks are a few of the important ones. For more details, one may refer to [7]. In the following, we shall introduce the desiderata of wireless technologies.

J. Zhou, M. Yung, and F. Bao (Eds.): ACNS 2006, LNCS 3989, pp. 365–374, 2006.

1.1 Wireless Technologies: How the Properties of Radio Waves Affect Networking Capabilities

An ideal radio wave for wireless technologies should have high speed, travel far distances and consume little energy. Had such radio waves existed, it would have been possible for us to transfer information very rapidly at any distance using little battery power. Unfortunately, real radio waves do not behave like that. The high speed and long range of a radio wave demands more energy. That is why the designers of the wireless technologies try to optimise certain parameters under a given condition. As a direct consequence, we find wireless area networks of different orders (e.g., personal, local, metropolitan, global, etc.) and each of them is suitable to a particular application or usage.

As an example, in wireless local area network (WLAN), the power consumption is less important compared to range/speed whereas the design of a wireless personal area network (WPAN) demands low power in preference to high speed or long range.

For more details on wireless technologies, refer to [17].

1.2 Our Proposal: An Uncharted Territory

However, an unexplored area in the security of wireless technologies is the use of combinatorial designs. Our proposal is an endeavour to propose the security solutions in a wireless network using combinatorial designs. The method is not restricted to smart homes only and may also find application in Hierarchical Sensor Networks where the deployment of the sensor nodes may be made in a more or less controlled manner. One can even think of other situation where a hierarchical structure may be deemed fit. As an extreme example, suppose the different countries of the world are divided into a few groups (possibly based on their geographical locations), and a multinational company operates globally, setting up branches in different countries. However, the management may decide to delegate the authority to each of the branch offices in an hierarchical structure. That structure may easily be translated to our model. In the following, we shall talk about two specific application areas viz., smart homes and sensor networks, though we have a common set of objectives in mind:

1. The entire communication in the network will take place securely.
2. The protocol will be as simple as possible.
3. The network will comprise of several logical parts. The network will be resilient to such an extent that the other parts will continue to function even if one/more parts of the network are compromised.

1.3 Smart Homes

A smart home or building is a home or building, usually a new one, that is equipped with special structured wiring to enable occupants to remotely control or program an array of automated home electronic devices by entering a single command. For example, a homeowner on vacation can use a Touchtone phone to

arm a home security system, control temperature gauges, switch appliances on or off, control lighting, program a home theater or entertainment system, and perform many other tasks. The field of home automation is expanding rapidly as electronic technologies converge. The home network encompasses communications, entertainment, security, convenience, and information systems. For more details, refer to [22].

Suppose we want to install the network in such a building. Naturally each of the rooms of the building forms a "logical part" of the network. The natural user requirement would be that the devices in one room should function independently of the devices of any other room. If one room has to be cut off from the network, still the other parts of the building should be able to function unhindered. One can use same/different combinatorial designs to model the different parts of the network.

1.4 Sensor Networks: A Brief Introduction

Secure communication among sensor nodes has become an active area of research [2, 6, 9, 14, 15, 16, 10]. One may refer to [12] for broader perspective in the area of sensor networks. Based on the architectural consideration, wireless sensor networks may be broadly classified into two categories viz.(i) Hierarchical Wireless Sensor Networks (HWSN) and (ii) Distributed Wireless Sensor Networks (DWSN). In HWSN, there is a pre-defined hierarchy among the participating nodes. There are three types of nodes in the descending order of capabilities: (a) base stations, (b) cluster heads, and (c) sensor nodes. The sensor nodes are usually placed in the neighbourhood of the base station. Sometimes the network traffic (data) is collected by the cluster heads which in turn forward the traffic to the base station.

There may be three different modes of data flow as follows: Unicast (sensor to sensor), multicast (group wise), broadcast(base station to sensor). However, it may be pointed out that the HWSN is best suited for applications where the network topology is known prior to deployment. On the other hand, there is no fixed infrastructure in the case of a DWSN and the network topology is unknown before the deployment. Once the nodes are scattered over the target area, the nodes scan their radio coverage area and find their neighbours. In this case also, the data flow may be divided into three categories (as discussed above) with the only difference that the broadcast might take place between any two nodes.

In this paper, we shall talk about wireless sensor networks in general, possibly with the exception of some special nodes with higher memory and/or computational capacity. Also we shall assume that the deployment is more or less controlled.

The size of the sensor network is usually very large (say, of size N). The sensor nodes are usually memory-constrained and that is why it is not possible to maintain $N-1$ keys in each sensor node so that ultimately different secret keys are maintained for each of the pairs. The nodes often do not have much computational capacity to implement public key framework (though very recently

implementations of ECC and RSA on 8-bit CPUs have been proposed [11]). Still key pre-distribution solutions are bound to be much faster since they are less computation intensive.

One usually faces a few problems in key pre-distribution. Often two nodes are not directly connected and communicate through one or more hops. Also the compromise of a few node results in the failure of a large part of the network since the keys revealed were also shared between the other nodes. For a more detailed account of these, please refer to [3, 4, 5, 1, 9, 14, 10, 15, 2].

1.5 Key Pre-distribution in General: Our Proposal

One possible solution is to have a situation where every node is guaranteed to have a common key with every other node that it needs to communicate with. For a very large network, this is not possible, as explained earlier. We propose to divide the network into certain logical sub networks. Intra sub network nodes always share keys with each other. For each sub network, we earmark a particular node as a special node. Inter sub network communication takes place by the communication between the special nodes of the respective sub networks.

The issues at this point are as follows:

1. One has to have some control over the deployment of the nodes.
2. For the special nodes, the number of keys to be stored in each node will clearly increase. So one needs to decide the availability of storage space. In [15, Page 4], it has been commented that storing 150 keys in a sensor node may not be practical. On the other hand, in [9, Page 47], [14, Section 5.2], scenarios have been described with 200 keys. If one considers 4 Kbytes of memory space for storing keys in a sensor node, then choosing 128-bit key (16 byte), it is possible to accommodate 256 keys.

Thus the goal in this paper is to present a scheme that aims at failsafe connectivity all-over the network. We differ from the existing works where it is considered that any two nodes will have either 0 or 1 common key all over the network. Our motivation is to have a design strategy where the entire network is divided into a number of subnetworks. Any two nodes of a particular subnetwork share a common key. The special nodes of different subnetworks share more than one common keys. This is important from resiliency consideration in an adversarial framework since even if a certain subnetwork is compromised, the other parts of the network, i.e., the other subnetworks may function without any disturbance. Moreover, even if one or more special nodes are compromised, the other special nodes can still communicate among themselves. In other words, the connectivity of the network is not disturbed at all.

The rest of the paper is organised as follows: We begin with a preliminary introduction to combinatorial designs. In the next section, we use a detailed example to explain the problem and discuss the solution. The paper concludes with the future research proposals.

2 Preliminaries

2.1 Basics of Combinatorial Design

For a ready reference to *set system, block design, BIBD, group-divisible design, projective planes* and *transversal design*, refer to [8, 20, 19, 21].

Projective Plane
A finite projective plane of order n is formally defined as a set of points with the properties that:

1. Any two points determine a line,
2. Any two lines determine a point,
3. Every point has $n + 1$ lines through it, and
4. Every line contains $n + 1$ points.

(Note that some of these properties are redundant.) A projective plane is therefore a symmetric $(n^2 + n + 1, n + 1, 1)$ block design.

A finite projective plane exists when the order n is a power of a prime, i.e., for $n = p^a$. It is conjectured that these are the only possible projective planes, but proving this remains one of the most important unsolved problems in combinatorics.

The smallest finite projective plane is of order $n = 2$, and consists of the configuration known as the Fano plane. The remarkable Bruck-Ryser-Chowla theorem says that if a projective plane of order n exists, and $n = 1$ *or* $2 (\mathrm{mod}\, 4)$, then n is the sum of two squares. This rules out $n = 6$. Even before that, Tarry ruled out projective planes of order 6 by hand calculations. Lam [13] showed, using massive computer calculations on top of some mathematics, that there are no finite projective planes of order 10. The status of the order 12 projective plane remains open.

The projective plane of order 2, also known as the Fano plane, is denoted PG(2, 2). It has incidence matrix

$$\begin{pmatrix} 1 & 1 & 1 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 1 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 1 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 & 1 & 1 & 0 \end{pmatrix}$$

Every row and column contains three 1s, and any pair of rows/columns has a single 1 in common.

3 Key Predistribution in General: Our Approach

3.1 The Correspondence Between a Combinatorial Design and a Sensor Network

The blocks of the combinatorial design corresponds to a sensor node and the elements present in a block represent the keys present in a sensor node.

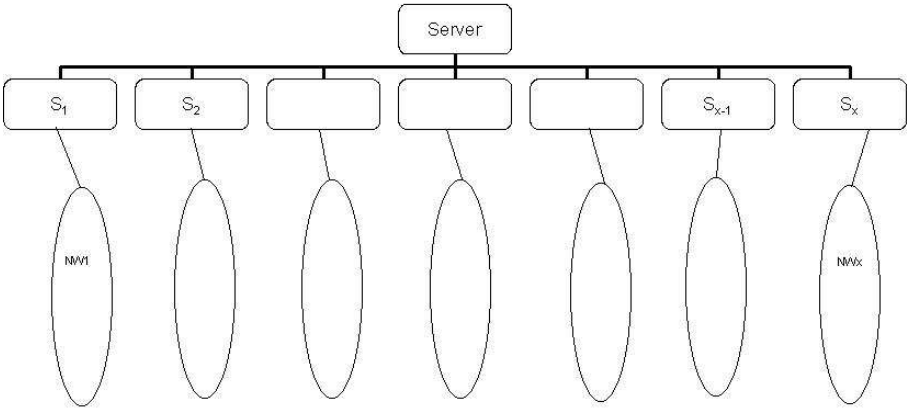

Fig. 1. The Network

3.2 The Method

In [15], it has been shown that using a transversal design, there is direct connectivity between two nodes in 60% of the cases. Overall, any two nodes can communicate either directly or through an intermediate node (i.e., a two-hop path) with almost certainty. For a large network, the compromise of even 10 nodes will render 18% of the nodes unusable.

Our approach is very different from the approach of [15]. In the diagram, we have shown a network with only two levels of hierarchy. There may be more levels depending on the user requirements. Our proposal is perfectly general and fits into networks of any size. The root of the hierarchy tree is assumed to be a central server, S. At the next level, x special nodes $S_1, S_2, \cdots, S_x$ are placed. The leaf level comprises of the subnetworks $NW_1, NW_2, \cdots, NW_x$.

One has the freedom to choose different combinatorial designs for different parts of the network. Again, that depends on the specific requirements of the user. For example, if the sub networks are required to form a totally connected network graph, one can choose projective planes. This may be applicable in case of a smart home. If the subnetworks are very large in size and total connectivity is not a requirement (i.e., if single/multi-hop connectivity is permissible), transversal designs might be a reasonable choice.

Let us assume that we are using only projective planes in all the parts of the network. We know that a projective plane of order n (n is a prime power) has $n^2 + n + 1$ number of blocks and each block contains $n + 1$ keys. If we use a projective plane of order n, we can accommodate a network of $n^2 + n + 1$ nodes with $n + 1$ keys per node.

Let us assume that $max_i|NW_i| = \alpha$ (for $i = 1, 2, \cdots, x$), i.e., the subnetwork size is at most α, so that a projective plane of order $\geq \left\lceil \sqrt{\alpha - \frac{3}{4}} - \frac{1}{2} \right\rceil$ may be used to model the subnetwork.

In fact, we should choose the sub network size $n^2 + n$ instead of $n^2 + n + 1$ because we shall have to include the special node S_i(at the next higher level) corresponding to each sub network NW_i. The corresponding projective plane is of order $\left\lceil \sqrt{\alpha + \frac{1}{4}} - \frac{1}{2} \right\rceil$.

If we have x such sub networks, we have also x corresponding projective planes. They may or may not be of the same order depending on the same / different sizes of the various sub networks. One can use different projective planes for different sub networks NW_i simple by replacing α by NW_i in the above expression.

Note that each of the subnetworks NW_i including the special node S_i, i.e., $S_i \bigcup NW_i$ (for $i = 1, 2, \cdots, x$) forms a complete network graph. Since we are using a projective plane to distribute the keys in the underlying nodes, this property is guaranteed. In other words, any two nodes of $NW_i \bigcup S_i$ for $i = 1, 2, \cdots, x$ share a common key with each other.

Had we used a transversal design $TD(k, r)$ instead of a projective plane, every pair of nodes would not have been connected. However, a constant fraction of the total number of pairs would have been connected (i.e., would have shared a common key). It is easy to see that the value of the fraction is $\frac{k}{r+1}$. Out of r^2 blocks of the $TD(k, r)$, a particular block shares keys with $kr - k = k(r - 1)$ blocks. Excepting that particular block, there are $r^2 - 1$ blocks in the $TD(k, r)$. So the fraction is $\frac{k(r-1)}{r^2-1} = \frac{k}{r+1}$.

At the next stage, we would like to have several common keys between any two special nodes S_j and S_k. In order to achieve that, we may again choose projective planes. A projective plane of order $m \geq \left\lceil \sqrt{x + \frac{1}{4}} - \frac{1}{2} \right\rceil$ will suffice to connect all the S_is for $i = 1, 2, \cdots, x$ and also the root server S may be included as the $(x + 1)$-th node. Using multiple copies (say t copies) of the projective plane of order m, and labelling them differently, we easily obtain t common keys between any two nodes of $\left(\bigcup_{i=1}^{x} S_i \right) \bigcup S$.

The special nodes/devices (which may be the cluster head in the case of a sensor network) should have more storage capacity in comparison with the other nodes in order to accommodate $t(m + 1)$ keys.

3.3 An Example Using Projective Planes

Let us continue our discussion apropos of the previous network diagram, i.e., a network with only two levels of hierarchy. The root of the hierarchy tree is the central server, S. At the next level, $x = 18$ special nodes $S_1, S_2, \cdots, S_{18}$ are placed.

The leaf level comprises of the subnetworks $NW_1, NW_2, \cdots, NW_{18}$. Let us use only projective planes all over the network.

Let us assume that $max_i |NW_i| = 900$, i.e., the subnetwork size is at most 900, or, $\alpha = 900$.

The corresponding projective plane is of order $\geq \left\lceil \sqrt{900 + \frac{1}{4}} - \frac{1}{2} \right\rceil \geq 30$.

The next highest prime being 31, let us choose a projective plane of order 31.

Since we have 18 such sub networks, we have also 18 corresponding projective planes. They may or may not be of the same order depending on the same/different sizes of the various sub networks. One can use different projective planes for different sub networks NW_i simply by replacing 900 by $|NW_i|$ in the above expression.

Note that each of the subnetworks NW_i including the special node S_i, i.e., $S_i \bigcup NW_i$ forms a complete network graph. Since we are using a projective plane to distribute the keys in the underlying nodes, this property is guaranteed. In other words, any two nodes of $NW_i \bigcup S_i$ share a common key with each other.

At the next stage, we would like to have several common keys between any two special nodes S_j and S_k. In order to achieve that, we may again choose projective planes. A projective plane of order $m \geq \left\lceil \sqrt{18 + \frac{1}{4}} - \frac{1}{2} \right\rceil \geq 4$ will suffice to connect all the S_is (for $i = 1, 2, \cdots, 18$) and also the root server S may be included as the 19-th node. Let us choose $m = 4$. Using multiple copies (say 4 copies) of the projective plane of order m, and labelling them differently, we readily have 4 common keys between any two nodes of $\left(\bigcup_{i=1}^{x} S_i \right) \bigcup S$.

The special nodes/devices (which may be the cluster head in the case of a sensor network) should have more storage capacity in comparison with the other nodes in order to accommodate $4(4 + 1) = 20$ keys.

3.4 Another Example Using Projective Planes and Transversal Designs

Suppose we have a different kind of requirement. The sub networks are very large, say each subnetwork may be of size 2500 and hence multi-hop communication is permissible.

Again let us assume that the network has only two levels of hierarchy, the root of the hierarchy tree is the central server, S. At the next level, $x = 25$ special nodes $S_1, S_2, \cdots, S_{25}$ are placed. The leaf level comprises of the subnetworks $NW_1, NW_2, \cdots, NW_{25}$.

At the sub network level, we do not have the requirement that any two nodes should be able to communicate directly. So we may use transversal designs at this level. However, since all the special nodes should be able to communicate directly among themselves and need an enhanced level of security by having multiple keys shared between any two nodes, we prefer to use projective planes at this level.

Since the sub network may have 2500 nodes, we should choose a transversal design accordingly. We know that a $TD(k, r)$ has r^2 blocks. We also know that if r is prime, and $2 \leq k \leq r$, then there exists a $TD(k, r)$ [3].

Since $\sqrt{2500} = 50$, we choose the next highest prime 53 as our r. Now we can choose k according to our convenience. We choose $k = 36$.

As mentioned earlier, the key sharing probability between any two nodes of the sub network $= \frac{k}{r+1} = \frac{36}{53+1} = 0.667$.

Note that each of the subnetworks NW_i including the special node S_i, i.e., $S_i \bigcup NW_i$ (for $i = 1, 2, \cdots, 25$) does not form a complete network graph. Since we are using a transversal design to distribute the keys in the underlying nodes, any two nodes of $NW_i \bigcup S_i$ share a common key with each other with probability 0.667.

At the next stage, we would like to have several common keys between any two special nodes S_j and S_k. In order to achieve that, we may again choose projective planes. A projective plane of order $m \geq \left\lceil \sqrt{25 + \frac{1}{4}} - \frac{1}{2} \right\rceil \geq 5$ will suffice to connect all the S_is for $i = 1, 2, \cdots, 25$ and also the root server S may be included as the 26-th node. Let us choose $m = 5$. Using multiple copies (say 4 copies) of the projective plane of order m, and labelling them differently, we readily have 4 many common keys between any two nodes of $\left(\bigcup_{i=1}^{x} S_i \right) \bigcup S$.

The special nodes/devices (which may be the cluster head in the case of a sensor network) should have more storage capacity in comparison with the other nodes in order to accommodate $4(5 + 1) = 24$ keys.

4 Conclusion and Future Research

We shall further investigate networks where "users" have differing resources and capacity requirements. One case involves a large network with large, mostly self-contained sub-networks. Another case involves networks which need more robustness at different levels of application. For example, at the second level of hierarchy (i.e., the level containing the special nodes), one may need to have different number of common keys shared between two given nodes. It will be an interesting combinatorial problem to find out a design having such a property. One may even look for better alternatives compared to the use of copies of projective planes at this level.

References

1. R. Blom. An optimal class of symmetric key generation systems. *Advances in Cryptology –Eurocrypt 84, LNCS,* vol 209, Springer Verlag, 1985, pp 335–338.
2. S. A. Camtepe and B. Yener. Combinatorial design of key distribution mechanisms for wireless sensor networks. *Computer Security – Esorics 2004, LNCS,* vol 3193, Springer Verlag, 2004.
3. D. Chakrabarti, S. Maitra and B. Roy. A key pre-distribution scheme for wireless sensor networks: merging blocks in combinatorial design. *8th Information Security Conference, ISC'05, LNCS,* vol 3650, Springer Verlag, pp 89–103.
4. D. Chakrabarti, S. Maitra and B. Roy. A hybrid design of key pre-distribution scheme for wireless sensor networks. *1st International Conference on Information Systems Security, ICISS 2005, LNCS,* vol 3803, Springer Verlag, 2005, pp 228–238.
5. D. Chakrabarti, S. Maitra and B. Roy. Clique size in sensor ketworks with key pre-distribution based on transversal design. *7th International Workshop on Distributed Computing, IWDC 2005, LNCS,* vol 3741, Springer Verlag, 2005, pp 329–337.

6. H. Chan, A. Perrig, and D. Song. Random key predistribution schemes for sensor networks. *IEEE Symposium on Research in Security and Privacy,* 2003, pp 197–213.
7. Christopher W. Klaus,Internet Security Systems (ISS). Wireless LAN Security FAQ. URL:http://www.iss.net/wireless/WLAN_FAQ.php [accessed on:17th January, 2006]
8. C. J. Colbourn, J. H. Dinitz. *The CRC Handbook of Combinatorial Designs*. CRC Press, Boca Raton, 1996.
9. W. Du, J. Ding, Y. S. Han, and P. K. Varshney. A pairwise key pre-distribution scheme for wireles sensor networks. *Proceedings of the 10th ACM conference on Computer and Communications Security, ACM CCS 2003*, pp 42–51.
10. L. Eschenauer and V. B. Gligor. A key-management scheme for distributed sensor networks. *Proceedings of the 9th ACM conference on Computer and Communications Security, ACM CCS 2002*, pp 41–47.
11. N. Gura, A. Patel, A. Wander, H. Eberle, S. C. Shantz. Comparing elliptic curve cryptography and RSA on 8-bit CPUs. *CHES 2004, LNCS,* vol 3156, Springer Verlag, 2004, pp 119–132.
12. J. M. Kahn, R. H. Katz and K. S. J. Pister. Next century challenges: Mobile networking for smart dust. *Proceedings of the 5th annual ACM/IEEE international conference on mobile computing and networking,* 1999, pp 483–492.
13. Lam, C.W.H. The search for a finite projective plane of order 10. *Amer. Math. Monthly 98, 1991*, pp 305–318.
14. J. Lee and D. Stinson. Deterministic key predistribution schemes for distributed sensor networks. *SAC 2004, LNCS,* vol 3357, Springer Verlag, 2004, pp 294–307.
15. J. Lee and D. Stinson. A combinatorial approach to key predistribution for distributed sensor networks. *IEEE Wireless Computing and Networking Conference (WCNC 2005),*13–17 March, 2005, New Orleans, LA, USA.
16. D. Liu, and P. Ning. Establishing pairwise keys in distributed sensor networks. *Proceedings of the 10th ACM conference on Computer and Communications Security, ACM CCS 2003.*
17. Michelle Man. Bluetooth and Wi-Fi: Understanding these two technologies and how they can benefit you URL: www.socketcom.com/pdf/TechBriefWireless.pdf [accessed on 17th January, 2006]
18. Y. Shaked and A. Wool. Cracking the Bluetooth PIN. *In Proc. 3rd USENIX/ACM Conf. Mobile Systems, Applications, and Services (MobiSys), Seattle, WA, June 2005,* pp 39–50.
19. D. R. Stinson. *Combinatorial Designs: Constructions and Analysis*. Springer, New York, 2003.
20. A. P. Street and D. J. Street. *Combinatorics of Experimental Design*. Clarendon Press, Oxford, 1987.
21. Projective Plane URL: http://mathworld.wolfram.com/ProjectivePlane.html [accessed on: 17th January, 2006]
22. URL:http://searchsmb.techtarget.com/sDefinition/0,,sid44_gci540859,00.html [accessed on 17th January, 2006]