An Efficient Key Pre-distribution Scheme for Multiple Attacks

S. Jabeen Begum^{a,*}**, Dr.T.Purusothaman** ^{b,1}**, G.Vidhya** ^{c,2}

Abstract - Probabilistic Key pre-distribution schemes (P-KPSs) are candidates for securing interactions between resource limited computer networks. Collusion susceptible P-KPSs are trade-offs between security and complexity and security include resistance to passive eavesdropping attacks, and active message injection attacks. The existing work presented the P-KPS, the subset keys and identity tickets (SKIT) scheme, SI Scheme, MBK Scheme whose performance were compared with deterministic KPS model to facilitate facets of the complexity of key pre-distribution schemes. The security model described the resistance of P-KPSs to active message-injection attacks. Most of the existing schemes are based on probabilistic approach and shows poor resiliency against coalition attack and connectivity. The storage costs of deterministic schemes are all relatively high and easy to support large size networks. The proposed work presented a resilient deterministic key pre-distribution scheme which show better detection against coalition attack. For the neighboring nodes in the same group, the polynomial-based key pre-distribution scheme is used to generate pair wise keys for them. And for the neighboring nodes in different groups, the binding secrets generated by a ECC are used to establish the pair wise key.

Index Terms - **Probabilistic Key pre-distribution schemes , subset keys and identity tickets (SKIT) scheme, SI Scheme, MBK Scheme resilient deterministic key pre-distribution scheme, polynomial-based key pre-distribution scheme.**

I. INTRODUCTION

An important requirement for securing interactions between nodes of any network is the ability to establish pair wise secrets between any two nodes which can be used for mutual authentication and for privacy of exchanges between the nodes. Schemes that facilitate this requirement rely on an entity trusted by all nodes in the network to bootstrap the process of key distribution. The trusted entity in the form of a key distribution center provides secrets to every node; alternately, a trusted certificate authority certifies the public key corresponding to a private key chosen by each node. Ultimately, any cryptographic security mechanism relies on the assumption that secrets of a node (say) are privy only. In conventional networks, nodes are typically desktop, laptop, or hand-held personal computers. Secrets assigned to personal computers are expected to be protected by the owner of the computer, say by restricting physical access to the computer.. For computers deployed in an unattended manner, with no explicit owner, the responsibility of protecting its secrets rests on the computers themselves. Thus, such computers will need hardware-assisted protection of secrets assigned to them. A minimal requirement then is to equip every such computer (or node) with some trustworthy hardware module (or chip) for protecting and performing computations with the secrets. Such hardware security modules (HSMs) should be tamper-responsive, and zeroise secrets under suspicious of intrusions. There are tangible reasons to deliberately limit HSMs to symmetric cryptographic primitives.

a) Several nodes (for example, sensors) may be severely resource-limited, and thus may not be able to house power-hungry HSMs.

b) Low complexity HSMs can be more readily verified and certified for compliance (or trustworthiness).

c) HSMs that do not generate excessive heat can be extended unconstrained shielding from intrusions as heat-dissipation will not be an issue, and thus rendered tamper-responsive at lower cost. Key predistribution schemes (KPSs) which employ only symmetric cryptographic primitives facilitate establishment of pair wise secrets between nodes of a network. The total number of nodes can be unlimited, and the nodes can be inducted into the network asynchronously. KPSs are, however, susceptible to collusions, an entity with access to secrets of multiple nodes can pool their secrets together to illegitimately compute secrets of other nodes. Irrespective of the total number of nodes N(t) (which can be practically unlimited, and change with time), an -secure KPS can resist an attacker who has pooled together secrets from or less nodes. For a probabilistic (n,p) –secure KPS, an attacker with access to secrets of randomly chosen nodes can illegitimately compute any pair wise secret with a probability p(n), where p(n) a monotonic is and increasing function of n.

Probabilistic key pre-distribution schemes (P-KPSs) which place modest demands on hardware are good candidates for securing interactions between resource limited computers. Collusion susceptible P-KPSs are trade-offs between security and complexity. Some facets of complexity include computation, bandwidth, and storage overhead. Metrics for security include resistance to passive eavesdropping attacks, and active message injection attacks.

Key pre-distribution schemes are a favored solution for establishing secure communication in sensor networks. Often viewed as the safest way to bootstrap trust, the main drawback is seen to be the large storage overhead imposed on resource-constrained devices. Thus those pre-distribution schemes can actually be quite insecure; pre-loading global secrets onto exposed devices strengthens the incentive for attackers to compromise nodes. Furthermore, lack of coordination between nodes arising from localized communication helps attackers hide misbehavior.

Here considering one scheme in particular Chan et al.'s random pair wise key pre-distribution and demonstrate an attack where colluding nodes reuse selected pair wise keys to create many false identities. And, found out that a small, colluding minority can hijack a majority of node communication channels. Finally, here consider countermeasures, from improved detection to scrapping pre-distribution altogether.

II. RELATED WORK

All KPSs are trade-offs between security and complexity. A metric for security is the collusion resistance. Metrics for complexity

Manuscript received, 2011.

S. Jabeen Begum^{a,*}, Research Scholar,
Department of Computer Science and Engineering,
Velalar College of Engg & Tech, Erode - 12
E-mail: sjabeenbegum@yahoo.co.in
Dr.T.Purusothaman ^{b,1}, Associate Professor,
Department of Computer Science and Engineering,
Government College of Technology, Coimbatore - 13
E-mail: drpurus@gct.ac.in
G.Vidhya ^{c,2}, II-ME CSE,
Department of Computer Science and Engineering,
Velalar College of Engg & Tech, Erode - 12
E-mail: gvidhyacse@gmail.com

include computation, bandwidth, and storage overhead. A good KPS should possess high security metrics while demanding low overhead. The main contribution of this paper is a novel probabilistic key predistribution scheme (P-KPS), the subset keys and identity tickets (SKIT) scheme. Demonstrate that while placing lower demands on complexity, SKIT simultaneously possesses better security metrics compared to other P-KPSs.

A. Combinatorial Design of Key Distribution Mechanisms

Common approach is to assign each sensor node multiple keys, randomly drawn from a key-pool, to construct a key-chain to ensure that either two neighboring nodes have a key in common in their key-chains, or there is a key-path. Thus, challenge is to decide on size of the key-chain and key-pool so that every pair of nodes can establish a session key directly or through a path. Key-chain size is limited by storage capacity of sensor nodes. Moreover, very small key-pool increases probability of key share between any pair of sensor nodes by decreasing security in that number of keys to be discovered by an adversary decreases.

Similarly, very large key-pool decreases probability of key share by increasing the security. Eschenauer et al. in [1] propose a random key pre-distribution scheme where tens to hundreds of keys are uploaded to sensors before the deployment. In their solution, initially a large key-pool of is generated. For each sensor, keys are randomly drawn from the key-pool without replacement. These keys and their identities form a key-chain which is loaded to the sensor node.

Two neighboring nodes compare the list of key identities in their key-chains. Eschenauer et al. also propose to employ a Merkle Puzzle [2] similar approach to secure the key identities which requires too much processing and storage for a resource limited sensor node. After exchanging key identities, common keys are used to secure the link in between two sensor nodes. It may be the case that some of the neighboring nodes may not be able to find a key in common. These nodes can communicate securely through other nodes, through other secured links. Chan et al. in [3] propose a modification to the basic scheme of Eschenauer et al.

They increase amount of key overlap required for key-setup. That is, common keys are needed instead of one to be able to increase the security of communication between two neighboring nodes. Their proposal requires larger key-chains and smaller key-pools than the original proposal of Eschenauer et al. In [4], common keys in the key-chains are used to establish multiple logical paths over which costly threshold key sharing scheme is used to agree on a new secret.

Random-pair wise key scheme in [3] is based on Erode and Renyi's work, to achieve probability that any two nodes are securely connected in a network of nodes, each node need to store only a random set of N_p pair wise keys instead of N-1. This scheme provides perfect resilience since each pair wise key is unique. But, it cannot support large networks because the keychain size is linearly dependent on the network size. Camtepe et al. in [5] propose a deterministic pair wise key pre-distribution scheme based on expander graphs. Slijepcevic et al. in [6] propose that sensor nodes share a list of master keys, a pseudorandom function and a seed.

Every sensor uses shared pseudorandom function and shared seed to select a network-wise or a group-wise master key. In [7] and [8], a polynomial-based key pre-distribution scheme is proposed for group key pre-distribution. In [9], polynomial pool-based key pre-distribution is used for pair wise key establishment. For each sensor, a random or a grid based pre-distribution scheme is used to select a set of polynomials from a pool of polynomials. In [10], Blom proposes a secure key pre-distribution scheme where each node stores relatively small secret and public data from which it can derive a unique pair wise key for any neighbor.

Each node stores a row of a private matrix and a column of a public matrix. Pair of nodes first exchange their public column information then each makes partial matrix multiplication to generates the common pair-wise key. Blom's scheme is a deterministic scheme where any pair of nodes can calculate a common secret key. That is, probability of key share and average key-path length are both one. Blom's scheme can resist capture of at most K nodes, credentials stored in K+1 node is enough to recover all the keys used in the network. For the same key-chain size, our symmetric algorithm provides the same probability of key share and better resilience with ω the same storage requirements but without any costly multiplication operations.

Du et al. in [11] use Blom's scheme with private matrices to increase its resilience. Each node is randomly assigned rows T from private matrices out of ω. It may be the case that two neighboring nodes do not share a key space. Unlike Du et al., here use smaller key-chains and Generalized Quadrangles (GQ) Block Design techniques to improve the resilience. In [12], Lee et al. propose two deterministic schemes,

a) ID-based one-way function scheme, and

b) Multiple spaces Blom's scheme where asymmetric key matrices are used instead of symmetric ones. They use a modification of Blom's scheme on strong regular graphs and provide better resilience than the scheme proposed by Du et al. in [11].

The first work (in the order of appearance) of a generic KPS model outlined to describe deterministic and probabilistic KPSs, and facilitate comparison of their complexities. The model identifies four facets of KPS complexity, storage, public function complexity, fetch complexity, and private function complexity.

The second work is that novel SKIT scheme outlined. The generic KPS model is used to describe SKIT, and evaluate its complexity to facilitate comparisons with other KPSs. Two other P-KPSs are compared with SKIT, the better known schemes based on random subset intersection (SI), and the more recent multiple basic KPS (MBK). While the security model can describe the resilience of P-KPSs to passive eavesdropping attacks, it is not an adequate characterization of the resistance of P-KPSs to active message injection attacks.

B.. Key Distribution Scheme

Designing a KDS for this purpose is very challenging due to the many inherent restrictions in such deployments. The nodes involved are typically battery operated wireless devices with severe resource constraints. Furthermore, the network may consist of millions or even billions of nodes. Additionally, the nodes may not have persistent access to a centralized trust authority (TA). Severe resource constraints rule out KDSs employing asymmetric cryptography. The need for scalability rules out the "basic" key distribution scheme1 as a possible choice. The lack of persistent access to a centralized trust authority rules out KDSs like Kerberos, where an active presence of a trusted server is necessary.

III. IMPLEMENTATION

Key predistribution schemes (KPSs) which employ only symmetric cryptographic primitives facilitate establishment of pair wise secrets between nodes of a network. The total number of nodes can be unlimited, and the nodes can be inducted into the network asynchronously. KPSs are, however, susceptible to collusions, an entity with access to secrets of multiple nodes can pool their secrets together to illegitimately compute secrets of other nodes. Irrespective of the total number of nodes N(t) (which can be practically unlimited, and change with time), an -secure KPS can resist an attacker who has pooled together secrets from or less nodes.

The main contribution of this work is deterministic and hybrid approaches to the key distribution problem. In particular, here brings a novel construction methodology from combinatorial design theory to address this problem. Although there are some applications of combinatorial design theory in cryptography and secret sharing [13]–[15], and in network design [16], [17], to the best of our knowledge this work is the first to apply design theory to key distribution in distributed wireless sensor networks [18], and others followed on this approach [19]. Here analysis indicates that deterministic approach has strong advantages over the randomized one since.

a) It increases probability that two a nodes share a key, and

b) It decreases average key-path length.

Here provides a brief background to combinatorial design theory without exceeding the scope of this project. Here introduces key distribution construction and explain the mapping from design theory to this practical problem. It addresses scalability issues and then present analysis and comparison with randomized methods.

A resilient deterministic key pre-distribution scheme which show better detection against coalition attack. It is an efficient hexagon-based key pre-distribution scheme, put forward by employing the ideas of the grouping key management and secret binding. For the neighboring nodes in the same group, the polynomial-based key pre-distribution scheme is used to generate pair wise keys for them. And for the neighboring nodes in different groups, the binding secrets generated by a ECC are used to establish the pair wise key.

A. Pre Key Distribution (SI SCHEME)

The key distribution scheme is a mechanism for distributing secrets and public values to all nodes to facilitate establishment of cryptographic bonds between the nodes. The participants in any key distribution scheme include nodes associated with some unique label (or identity), and some credentials, registration authorities (RAs) who verify credentials of nodes and issue unique labels, and a certificate authority (CA), or a key distribution center (KDC).

In certificate-based schemes, nodes choose a random private key and compute the corresponding public key. The CA issues a public key certificate to every node, binding the public key, label, and credentials. In identity-based schemes, the credentials themselves can be the identity. Most often, the identity is a one-way function of the credentials. The KDC chooses some master secrets, and based on the identity of a node, computes and issues secrets to nodes. In this paper, restrict ourselves to identity-based schemes which facilitate establishment of pair wise secrets between nodes.

B. Identity Based Key Pre Distribution Scheme (MBK Scheme)

In KPS, the key distribution centre (KDC) chooses a set of secrets. Every node is assigned a unique identity drawn from a set. A node assigned identity is issued a key-ring, where is a “key assignment” function. Using its key-ring, can compute. Likewise, node can use its key-ring to compute. Thus, both and can independently compute a common secret. The key-ring secrets issued to every node, and the pair wise secrets computed using such secrets, are long-lived secrets. A long-lived shared secret can be used for establishing a private channel and/or authenticating messages exchanged. Most often, long-lived secrets will be used to derive short-lived session secrets (through the use of random nonces and/or time stamps), and such session secrets can then be used for establishing private channels or mutual authentication. In this paper, restrict ourselves to mechanisms for establishing long-lived pair wise secrets

C. Probabilistic key pre distribution scheme (SKIT SCHEME)

For secure probabilistic schemes (P-KPS), an attacker with access to secret of randomly chosen nodes can compute any illegitimate pairwise secret with a probability, or such an attacker can compute a fraction of all illegitimate pairwise secrets. As long as is small enough, it may be computationally infeasible for an attacker to even determine which illegitimate pairwise secrets can be computed using the secrets pooled from nodes. P-KPS, with monotonic (increasing), fail gracefully.

Nodes are low-power, low-complexity HSMs. Such HSMs include protected registers for storing secrets, a single block-cipher/hash, and minimal additional logic to reuse the block-cipher for different types of symmetric cryptographic computations (hashing, pseudorandom number generation, repeated encryption, bulk encryption, etc.).

Every computer in the network houses such an HSM. Some practical examples of such computers include sensors deployed in unattended locations monitoring environmental conditions like temperature, pressure, SIM cards (subscriber identity modules) plugged into mobile phones, computers controlling a microwave, or a coffee maker, or a security camera at home, and computers associated with vital organ sensors, etc. For example, a computer associated with a vital organ sensor may detect early warning signs of an organ failure and send an alarm; the alarm may be relayed by other computers to a nearby hospital to facilitate timely responses. A sensor in a refrigerator monitoring the level of milk in the carton may send a message, resulting in the addition of a note “get milk” in the to-do list in a calendar of mobile phone.

The infrastructure for bootstrapping the key distribution process consists of RAs who verify the integrity of HSMs, and assign a unique identity to each HSM and KDCs. For simplicity, we shall assume a single KDC. It is also assumed that the KDC(s) are unconditionally trusted. In practice, KDCs may employ highly trustworthy computers with very little constraints on cost and capabilities. At the end of the bootstrapping process, a unique shared secret is established between every HSM and the KDC.

As the specification of the bootstrapping process have no effect on the nature of the key distribution scheme used. It is assumed that every HSM has a unique identity and every HSM shares a secret with each KDC, represent by the secret shared between the KDC and an HSM with identity.

B. Deterministic Hexagon

In deterministic KPSs, an attacker with access to the key-ring of or less nodes cannot compute any illegitimate shared secret. On the other hand, an attacker with access to secrets of more than nodes can compute all secrets of all nodes. The deterministic key pre distribution scheme used in this work is combinatorial design based key pre distribution schemes.

The algebraic properties of some combinatorial design help us to get suitable deterministic key pre distribution schemes for distributed wireless sensor network. To map a particular combinatorial design to key pre distribution scheme, the universal set of design acts as key pool of sensor network, blocks are mapped to key chain of individual sensor nodes. Merging blocks of a particular design and then assign these merged blocks to individual sensor nodes before their deployment. Due to this merging of blocks, now every node has to take extra burden of storing all the keys, but its connectivity and resiliency improves considerably.

SCHEMES	PRIVATE FUNCTION COMPLEXITY	PUBLIC FUNCTION COMPLEXITY	FETCH COMPLEXITY
SI SCHEME	12.0	133.76	9.6
MBK SCHEME	1.38	NAN	3.2
SKIT SCHEME	1.0	4.0	3.0
DETERMINISTIC SCHEME	1.03	2.0	1.36

TABLE 3.1 PERFORMANCE MEASURE ANALYSIS

IV. RESULTS AND DISCUSSION

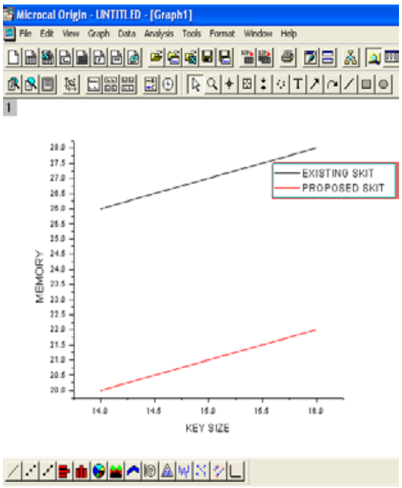

FIGURE 4.1 KEY SIZE VERSUS MEMORY

The Figure 4.1and Figure 4.2 shows that Memory space utilization and Time utilization is efficient in discrete SKIT when compared to probabilistic SKIT. Our motivation was to devise a deterministic merging scheme. Here proposed a deterministic merging scheme for transversal design based key pre distribution scheme. Another motivation was to examine other combinatorial design based key pre distribution schemes to find if merging of blocks with considering the parameters time and memory which would be helpful to improve their performances or not.

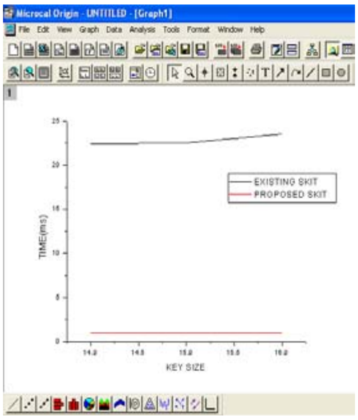

FIGURE 4.2 KEY SIZE VERSUS TIME

V. CONCLUSION AND FUTURE ENHANCEMENTS

The problem of achieving an advantageous trade-off between security, connectivity and resilience when distributing keys is fundamentally an issue of control over how the keys are allocated. Here the scheme used made use of the knowledge of the nodes' locations to give a greater degree of control. The enhanced work describes how a more fine-grained control of specific connectivity properties can be brought to this scheme through an appropriate choice with which it is implemented. The algorithms presented in this work give a means for efficiently generating distinct difference configurations that lead to KPSs with good connectivity for networks with square grid or hexagonal grid topologies, with a range of possible parameters. This gives a practical means of instantiating the grid-based KPS with its storage requirements and connectivity properties adapted to suit requirements, and a favorable degree of resilience.

In the future study, the main focus is to expect the proposed deployment model and hierarchical groups will be applied to and more investigated for heterogeneous wireless sensor networks. Having demonstrated the dramatic improvement in the performance of the Eschenauer-Gligor scheme, in future work, which investigates how much the deployment knowledge that can improve the q-composite random key pre-distribution scheme and the pair wise key pre-distribution scheme proposed by Chan, Perrig and Song. In addition, future study concentrates the global connectivity, communication overhead, and the local resilience

REFERENCES

[1] Blom.R (1984), “An optimal class of symmetric key generation systems,” in advances in Cryptology: Proc. Eurocrypt 84, Berlin, vol. 2 ,Lecture Notes in Computer Science, pp. 335–338, Springer-Verlag.

[2] Canetti.R, Garay.J, Itkis.G, Micciancio.D, Naor.M, and Pinkas.B,(1999) “ Multicast security: A taxonomy and some efficient constructions,”
INFOCOMM New York

[3]Di Pietro.R, Mancini.L.V, and Mei.A(2003), “Random key assignment for secure wireless sensor networks,” in 2003 ACM Workshop on Security of Ad Hoc and Sensor Networks, Fairfax, VA.

[4]Du.W, Deng.J,. Han.Y.S, and. Varshney.P.K(2003), “A pairwise key predistribution scheme for wireless sensor networks,” in Proc. 10th ACM Conf. Computer and Communication Security, pp. 42–51.

[5]Du.W, Deng.J, Han.Y.S, Chen.S , and Varshney.P.K(2004), “A key management scheme for wireless sensor networks using deployment knowledge,” in Conf. IEEE Communications Society (Infocom), Hong Kong.

[6]Erdos.P, Frankl.P, and Furedi.Z(1982), “Families of finite sets in which no set is covered by the union of 2 others,” J. Combinatorial Theory, Series A, vol. 33, pp. 158–166.

[7]Eschenauer.L and Gligor.V.D(2002), “A key-management scheme for distributed sensor networks,” in Proc. Ninth ACM Conf. Computer and Communications Security, Washington, D.C, pp. 41–47.

[8]Geng Yang1, Chunming Rong2, Christian Veigner2, Jiangtao Wang1(2006), “Identity-Based Key Agreement and Encryption For Wireless Sensor Networks” in IJCSNS International Journal of Computer Science and Network Security, VOL.6 No.5B.

[9]Kejie Lu, Yi Qian, “A Framework for Distributed Key Management Schemes in Heterogeneous Wireless Sensor Networks”, Royal Melbourne Institute of Technology Melbourne, VIC 3000, Australia.

[10]Liagkou1.V, Makri.E, Spirakis.Pand StamatiouY.C,” Collusion resistant key predistribution schemes and schemes with group identification properties” , in University of Patras, Department of computer Engineering, 26500, Rio, Patras, Greece.

[11]Liu.D and Ning.P(2003), “Establishing pairwise keys in distributed sensor networks,” in *Proc. 10th ACM Conf. Computer and Communication Security*, Washington, D.C.

[12]Mahalingam Ramkumar,”On the Complexity of Probabilistic Key Predistribution Schemes” in Mississippi State University, Mississippi State, MS 39762.

[13]Mitchell.C.J and Piper.F.C(1995), “Key storage in secure networks,” *Discrete Appl. Math.*, vol. 21, pp. 215–228.

[14]Piyi Yang Zhenfu Cao, and Xiaolei Dong(2009),’ A Dependable Threshold Broadcast Encryption System for Key Distribution in Mobile Ad Hoc Network’, in Second International Conference on Dependability.

[15]Ramkumar.M,. Memon.N, and Simha.R(2003), “Pre-loaded key based multicast and broadcast authentication in mobile ad hoc networks,” in *Globecom*, San Francisco, CA.

[16]Ramkumar.M and Memon.N(2005), “An efficient random key pre-distribution scheme for ad hoc network security,” *IEEE J. Sel. Areas Commun.*, vol. 23, no. 3, pp. 611–621.

[17]Ramkumar.M(2006), “On the feasibility of very low complexity trust modules using PKPS synergies,” in *IEEE Globecom*, San Francisco, CA.

[18]Ramkumar.M(2008), "Proxy aided key pre-distribution schemes for sensor networks," in *IEEE*, Austin, TX, Dec. 2008.

[19]Taekyoung Kwon(2009), "Location-Based Pairwise Key Pre distribution for Wireless Sensor Networks" in IEEE Transactions on wireless communications, VOL. 8, NO. 11.

[20]Mahalingam Ramkumar(2010)," The Subset Keys and Identity Tickets (SKIT) Key Distribution Scheme" in IEEE Transactions on Information Forensics and Security, vol.5

BIOGRAPHY

Prof.JabeenBegum.S received her M.E in Computer Science from Government College of Technology and is working towards Ph.D. in Computer Science from the Anna University of Technology, Coimbatore. Currently she is working as a HOD & Professor in CSE Dept, Velalar College of Engineering and Technology, Erode, Tamil Nadu, India and she is having 18 years of Experience in Teaching. She had published 21 Papers in Various National Conferences and she had presented 6 Papers in Various International Conferences held at many Engineering Colleges. Her Research Paper regarding "Time Complexity in Key Management" has published in AMSE, France, "An Effective Key Computation Protocol for Secure Group Communication in Heterogeneous Networks" published in IJCSNS and she had published her research paper in IEEE Explorer regarding Secure Group Communication. Her interests include Network Security, Distributed Systems, Cloud computing and DBMS.

Dr.T.Purusothaman is currently working as Associate Professor in the department of Computer Science and Engineering and Information technology, Government College of Technology, Coimbatore. He has twenty one years of teaching experience. He has completed Ph.D in the area of Network Security and Grid Computing. In his thesis, a novel key management scheme was proposed to provide service only for the paid customers in Internet. He has successfully completed a project funded by DIT (Government of India) in the area of cryptanalysis in the year 2006. He has presented a number of papers in various National and International conferences. Many of his papers were published in IEEE Explore. He has to his credit several International Journal Publications in reputed journals including Journal of Grid Computing, Springer. His research interests include Network Security, Grid Computing and Data Mining.

G.Vidhya is currently working as Assistant Professor in the department of Computer Science and Engineering in Velalar College of Engineering and Technology, Erode, Tamil Nadu, India. She had presented 4 Papers in Various National Conferences and she had presented 2 Paper in International Conference. One international conference paper presented in Systemics, Cybernetics and Informatics under the aegis of Pentagram Research Centre, Hyderabad, India on 5th Jan 2008. She had completed her M.E project based on the area of wireless sensor networks titled, "An Efficient Deterministic Key Pre-Distribution Scheme for Multiple Attacks". In her project she focused on favorable degree of resilience in deterministic key pre-distribution scheme. Her interests include Network Security, DBMS and Cloud computing.