IJREAT International Journal of Research in Engineering & Advanced Technology, Volume 2, Issue 2, Apr-May, 2014
ISSN: 2320 – 8791 (Impact Factor: 1.479)
www.ijreat.org

Secure Key Distribution Scheme Using Combinatorial Design in WSN

Rekha.A.K[1], Sivasankar.S[2]

[1]PG student, Department of Electronics and Communication Engineering, CK College of Engineering and Technology, Cuddalore ,Tamil Nadu, India

[2]Assistant Professor, Department of Electronics and Communication Engineering, Anand Institute of Higher Technology, Chennai, Tamil Nadu, India

Abstract

To protect the confidentiality, integrity, and authenticity of the communication, secret keys must be established for securing wireless networks. Key Distribution in senor networks is a challenging problem because the nodes could be physically compromised by an adversary. Efficient key distribution is essential for secure group communication among sensor nodes. For this purpose Pair wise key distribution scheme is taken into account. This scheme is highly resilient against node capture attacks which is achieved by key refreshing and is applicable for mobile networks, while preserving low storage, computation and communication requirements. This scheme is better in terms of security and bandwidth requirements. Triple key distribution scheme, in which three nodes share a unique common key provides secure routing, trust establishment, identifying malicious nodes and in data aggregation, key management in clustered sensor networks. This efficient key distribution scheme using combinatorial design has proved to be a more secure than the basic scheme in terms of packet delivery ratio, route overhead, packet loss, and throughput. However congestion is present in the network and it can be reduced using suitable congestion avoidance algorithm.

Keywords: *Key pre distribution, Pair wise-keys, Security, Triple Key Distribution.*

1. Introduction

Wireless Sensor networks consist of many tiny sensing devices with limited memory and power, which are deployed in large numbers to sense and collect information for various applications ranging from health care to civilian purposes like monitoring seismic activities, ocean-water temperature, in military surveillance, smoke detection, wild fire detection in forests etc. These sensor nodes communicate via radio waves within a certain range called Radio Frequency range. Sensor nodes work in a self organized way and are prone to adversarial attacks. So, secure communication is very important for many applications. Sensor networks need to rely on some cryptographic mechanism to communicate securely. Due to the resource constrained nature of sensor nodes, the symmetric key techniques are preferred over the public key ones. Key establishment using public key techniques has been used in [1].

In key pre distribution, keys are preloaded in sensor nodes prior to deployment. After deployment, the sensors need to find if they share common key. If there are no keys in common, then a path-key is established in which intermediate nodes serve as relays. The last two steps are jointly called key establishment. One way of pre distribution is to load all the nodes with a single master key. This results in an optimal storage. However if one node is compromised, then the entire network becomes insecure. At the other extreme, each pair of nodes can share a unique key. If there are N nodes in the network, then each node stores $N - 1$ pair wise keys. We call this the *naive pair wise scheme*. This results in full security of the network, meaning that even if many nodes are compromised, the adversary cannot know the common key between any two uncompromised nodes. However, the storage requirement for such a scheme can be very high.

Eschenaur and Gligor [2] were the first to propose a key pre distribution scheme for sensor networks. Keys are selected at random from a large key pool and placed in sensors prior to deployment. Two nodes share one or more keys with certain probability. Chan, Perrig and Song [3] proposed several variations of this scheme. They used a pairwise key scheme in which each node stores $k \ll N - 1$ keys. The rationale is that not all nodes may be within communication range of each other and it is enough to establish links with nodes which are in close proximity. Each node stores all the pairwise keys, and also all the node identifiers, with which it shares pairwise keys. This results in large storage cost . The scheme was proposed for a static network, but can be extended to a mobile network.

All pairwise keys have to be stored all the time, even if the nodes sharing pairwise keys are not within communication range. The primary reason why pairwise schemes are preferred over other schemes is because of increased security. If a unique pairwise key is shared by A and B and not shared by any other node in the network, then even if both A and B are compromised, other links in the network are not affected. However, in a collusion attack, the adversary might gather the information from many nodes to construct the pairwise keys of the uncompromised nodes. This may occur in Blundo et al [4] scheme, [5] and other schemes. In c-secure schemes, an adversary needs to compromise more than a c node to construct all the pairwise keys of the uncompromised schemes.

Design of deterministic techniques based on combinatorial designs is done to achieve communication and computation efficiency, and resist collusion attacks by establishing unique pairwise keys. Nodes discover their neighbors and can calculate the pairwise keys on the fly, by exchanging the node identifiers. Only required pairwise keys are stored by sensors. When a node moves, it discovers new neighbors and calculates needed pairwise keys. It can delete the previously stored pairwise keys, which are no longer required. Mitchel and Piper [6] were the first to apply combinatorial designs in key distribution.

Camtepe and Yener [7] applied combinatorial designs for key pre distribution in WSN. A *set system or design* can be mapped to a key pre distribution scheme in the following way. Let (X, A) be the *set system* with a set of elements (key identifiers) X and A set of subsets with elements from X. The subsets belonging to A are also called *blocks* of the design. Each sensor is associated with a block. Then the pool of key identifiers is the set X and the subsets of A are key chains of the sensor nodes. A special type of design is Balanced Incomplete Block Design, BIBD, with the parameters v, b, r, k and λ, where $v = |X|$, b is the number of subsets (that is, the number of sensor nodes) of A or blocks, r is the number of blocks in which a particular element occurs, k is the size of each subset, λ is the number of blocks in which a given pair of elements occur. For a t-design, every t-subset of X occurs in λ blocks. $t = 2$ for BIBD. Combinatorial designs with $\lambda = 2$ and $\lambda = 3$ can be used to establish unique pairwise and triple keys respectively, between sensor nodes. The first time the scenario where three nodes want to communicate securely is introduced, and hence this concept is called the triple key distribution. It is a special type of group key distribution, where the group size is three. Few applications of this concept is discussed. A hierarchical network typically consists of a base station, cluster heads and small sensor nodes. A group of sensors nodes sense data and send to cluster head, which processes the data and sends to the base station. Sensor nodes share keys with the cluster head which helps them to securely send data to it. If cluster head needs to monitor the communication between two nodes in its cluster then these three nodes need to share a unique common key.

Secure routing and passive monitoring of routing process can be achieved by triple key distribution. Suppose node A wants to send a message to B and it is routed via C, such that node C receives the message from A and forwards it to B. A can recognize forwarding by overhearing. If A, B and C share a triple key, then A will recognize that the message has been forwarded by C and none of the other nodes are aware of the forwarding. Tripartite key agreement has been a major topic of interest in cryptology [8]. However triple key distribution has never been discussed in a sensor network scenario.

The use of λ has never been explored before in connection to sensor networks. λ is the number of nodes, in which a pair of keys occur. When $\lambda = 2$, a pair of keys K_1 and K_2 can occur in exactly two nodes. These two keys can be used to construct a pairwise key $K = hash(K_1 \oplus K_2)$. These two nodes can thus calculate a unique pairwise key from this information. A proper interpretation of important parameter λ in the sensor network scenario is given, and pairwise key pre distribution schemes which are constructed in a deterministic fashion is discussed.

Organization of the paper is done as follows. Related work is described in Section II. In Section III presentation of some definitions of combinatorial structures is done. Introduction to trades and a new construction of trades are given in Section IV. Discussions of features of key pre - distribution scheme using trades are explained in Section V. In Section VI we compare it with existing schemes. Section VII discusses triple key distribution. Section VIII concludes with some open problems.

2. Related Work

A number of pairwise key establishment schemes have been discussed by several researchers. We have already discussed the naive scheme and Chan et al [3] scheme. One can use Blundo et al scheme [4] to establish pairwise scheme. The original scheme was used for secure conferencing between groups of members in a network. A symmetric c-degree polynomial in g-variables $(P(x_1, x_2, \ldots, x_g))$ was constructed. Each member i was given a share, $P(x_1, x_2, \ldots, x_{i-1}, i, x_{x+i}, \ldots, x_g)$ of this polynomial. g Members $m_1, m_2, \ldots, m_g$ can find a

common key $P(m_1, m_2, \ldots, m_g)$, if they know all the g identifiers. This scheme is secure unless the adversary compromises more than c nodes. Otherwise P(x,y) can be interpolated and the entire scheme is broken.

Du et al [5] proposed another c-secure scheme. Zhu et al [10] proposed a scheme to establish pairwise keys using probabilistic key sharing and threshold secret sharing. The security depends on the number of nodes compromised. Other schemes like the ones by Huang and Medhi [11], PIKE [12] cannot be used when nodes are mobile. These schemes have been discussed in [13]. A number of schemes [7], [14], [15] use combinatorial designs such as projective planes, transversal designs and partially balanced incomplete block designs (PBIBD). A survey can be found in [16]. The security of these schemes decreases with the increase in the number of nodes compromised.

3. Preliminaries

When v = b, the BIBD is called a symmetric BIBD and denoted by *SBIBD* (v, k, λ).

A $t-(v,k)$ trade consists of collections $T = \{T_1, T_2\}$, where $T_i, (i = 1,2)$ is a collection of m blocks of size k chosen from X such that the blocks of T_1 are distinct from the blocks of $T_2 (T_1 \cap T_2 = \phi)$ and, further, each t-set chosen from X occurs in precisely the same number of blocks of T_1 as those of T_2 The volume of the trade is $|T_1| = |T_2| = m$. The foundation of the trade is the subset of elements of X which occur in a block of T_1.

Throughout the paper k refers to a number and K (with or without subscript or superscript) denotes a key. Consider a network with N nodes, each node containing k keys. The identifier of key K_1 is denoted by $id(K_1)$, the identifier of node A is denoted by id_A.

4. Combinatorial Trades and new Pairwise key establishment schemes

Our problem of pairwise key establishment can be mapped to Steiner trades. If there exists a $t-(v,k)$ steiner trade with volume m, then we can consider all the k-subsets of $T_1 \cup T_2$ as the blocks of the design. Then any t-subset of elements occur in either 2 blocks or none. When we map this to key pre distribution, v is the size of the key pool, T_1 and T_2 are sensors, each containing k keys. So there are a total of $2m$ sensors in the network. Any set of t keys occurs either in two sensors or none.

The first result can be applied to the design of pairwise key pre distribution scheme in the following way. If q is a power of 2, then a key pre distribution scheme can be designed where the size of the key pool is $q^2 + q$, the maximum size of the network supported is $2q^2$, and length of the key chain is $q + 1$. If is a power of two, then the key pre distribution scheme has a key pool size of $q^2 + 2q + 1$, the maximum size of the network supported is $2(q^2 + q)$, length of key chain is $q + 1$. Moreover every pair of key occurs in exactly 2 nodes or none. These two keys that belong to a pair of nodes can be used for key establishment between the concerned nodes. The other results can be applied similarly. For a network of size N, the number of keys to be stored in each node is less than $\sqrt{N}$.

We show that any pair of elements occur either once in both T_1 and T_2 or does not occur in any of T_1 and T_1, every pair of elements of the form $\{(x,y),(y,z)\}$ does not occur in any block in either T_1 or T_2. This follows from the construction. Now we show that each pair of elements $\{(x,y),(x',y')\}$ (where $x \neq x'$) occurs at most once in T_1 and at most once in T_2.

4.1 Mapping keys to sensor network

Construct a wireless network to design a pairwise scheme in sensor network. Consider the set of blocks $T_1 \cup T_2$, if each block represents a key chain, then the size of key chain is $4 \leq k < q$, the number of sensors supported is $N = 2q^2$. the size of the key pool of q^k. any pair of keys in the key pool has a unique xor value. Thus for any two distinct pairs of keys K_1, K_2 and K_3, K_4, $K_1 \oplus K_2 \neq K_3 \oplus K_4$. The identifier of a node is denoted by (i, j, u) where (i, j) represents the block $t_{i,j}$ and u is either 1 or 2 depending on which of the sets T_1 or T_2 it belongs to. We note that pair of keys occurs either in two sensors A and B or none. If A and B share a pair of keys K_1 and K_2, then the pairwise key between A and B is calculated as $K_{AB} = K_{BA} = hash((K_1 \oplus K_2) \| id_A \| id_B), id_A < id_B$.

4.2 Pairwise key establishment

Two nodes A corresponding to block $t^u_{i,j}$ $(u \in \{1,2\})$ and B corresponding to $t^v_{i',j'}$ $(v \in \{1,2\})$ can calculate the pair of keys that they share in the following way. Nodes broadcast their identifiers (i, j, u) and (i', j', v) respectively. If $u = v$, then A and B do not share a pairwise key and the algorithm returns a null value. The algorithm returns $K_{x_1, x_1(+)j} \oplus K_{x_2, x_2(+)j'}$ if both $x_1 < k$ and $x_2 < k$, and null otherwise. The pairwise key is calculated as

$hash\left(\left(K_{x_1,x_1 i+j} \oplus K_{x_2,x_2 i+j}\right) \| id_A \| id_B\right)$. If q is composite then the square root can be found by Chinese remainder theorem. For details one may refer to [9].

5. Discussion on our scheme

The result shows that efficient key distribution scheme is fully secure. Result shows that the message communicated by a pair of nodes cannot be decrypted by any other node, i.e., a pairwise key is unique. This follows by the definition and construction of trades. A pair of keys (say K_1 and K_2) occur together either in two nodes or none of the nodes. The pairwise key between two nodes A and B is calculated as $K_{AB} = hash\left((K_1 \oplus K_2) \| id_A \| id_B\right)$, since K_1 and K_2 together exist only in nodes A and B, and $K_1 \oplus K_2, id_A, id_B$ are all unique, K_{AB} is unique. We next show that no adversary can calculate a pairwise key K_{AB} by compromising nodes other than A and B. This follows from key establishment algorithm. The input of the algorithm is the identifiers A and B and the output is $K_1 \oplus K_2$, where K_1 and K_2 are the common keys between A and B, and null if a pair of common keys do not exist. If a node C shares a common key K_1 with both nodes A and B, then the algorithm returns null. If the node C shares a common key K_1 and K_i (K_i cannot be K_2 by construction) with node A and K_1 and K_j ($K_j \neq K_1, K_i$ with B, then the algorithm returns $K_1 \oplus K_i$ and $K_1 \oplus K_j$, respectively. So an adversary is not able to know if it shares one key with any node. The algorithm either returns the xor of two keys or null. So even if nodes C and D are compromised, such that C has common key K_1 with A and B, and D has common key K_2 with A and B, they cannot collude and find the common key $K_1 \oplus K_2$. Also, since $K_1 \oplus K_2$ is unique, no other pairwise combination of keys compromised by the adversary can give the same value as

$K_1 \oplus K_2$Path keys are established in a manner, similar to [3].

6. Comparison with Existing Pairwise Schemes

The naive scheme and Chan et al scheme [3] require huge storage. Schemes like PIKE [12] and Traynor et al are not suitable for mobile networks. The simulation results for throughput, routing overhead, packet loss, packet delivery ratio is presented.Figure1 shows pairwise has better throughput. Figure 2 talks about reduced routing overhead .Figure 3 displays packet loss of pairwise scheme. Figure 4 shows minimum packet delivery ratio for pairwise scheme.

Figure 1 Throughput of pairwise

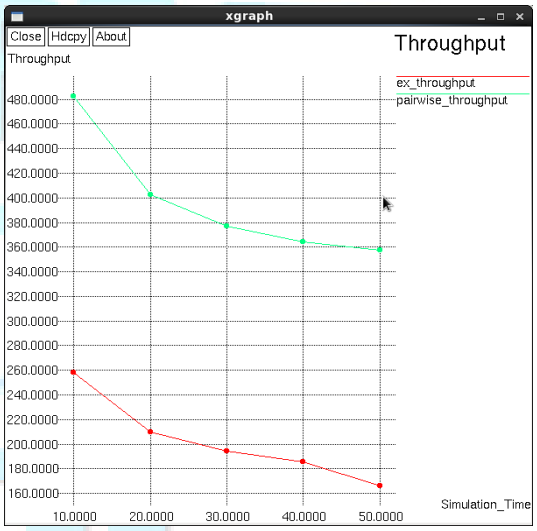

Figure 2 Routing-Overhead of pairwise

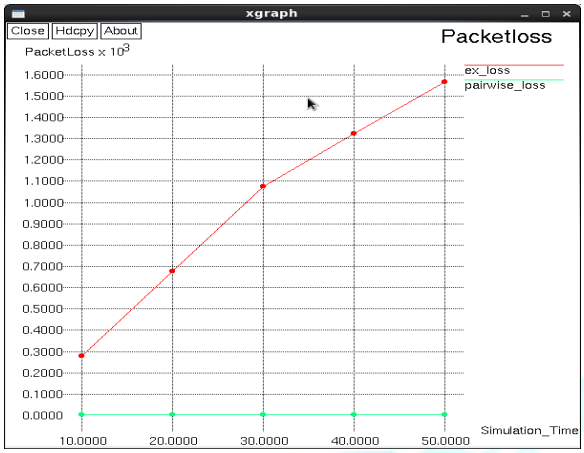

Figure 3 Packet loss of pairwise

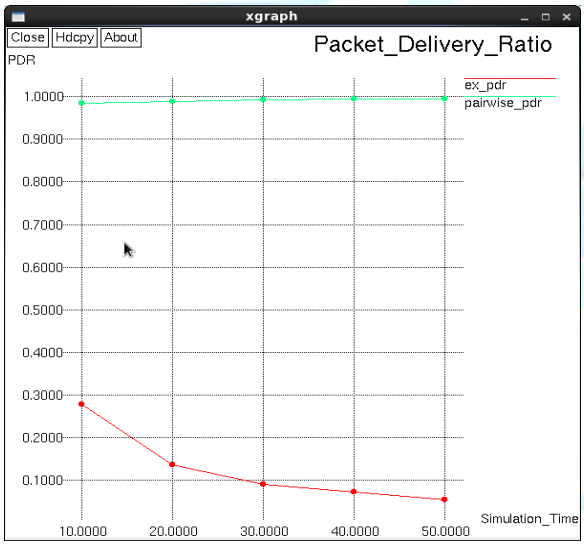

Figure 4 Packet delivery ratio of pairwise

7. Triple key Distribution schemes (tkd)

Triple key distribution is a method of assigning keys, such that three nodes share a unique common key. We introduce this novel idea of triple key distribution and present some constructions

7.1 Triple key distribution from polynomials

Blundo's scheme can be used for constructing a triple key distribution scheme. choose a *c*-degree symmetric polynomial with coefficients from F_q in three variables $P(x,y,z)$. If three nodes i , j and l want to share some information, they can calculate a common key as $P(i,j,l)$. The simulated results of throughput (figure5), routing overhead(figure6), packet loss (figure7),packet delivery ratio(figure 8) is shown.

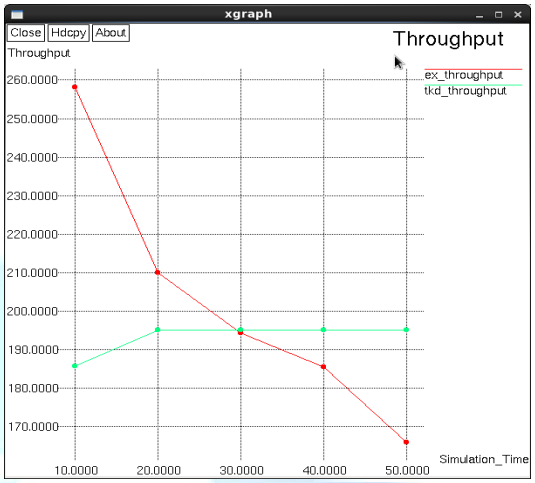

Figure 5 Throughput of TKD

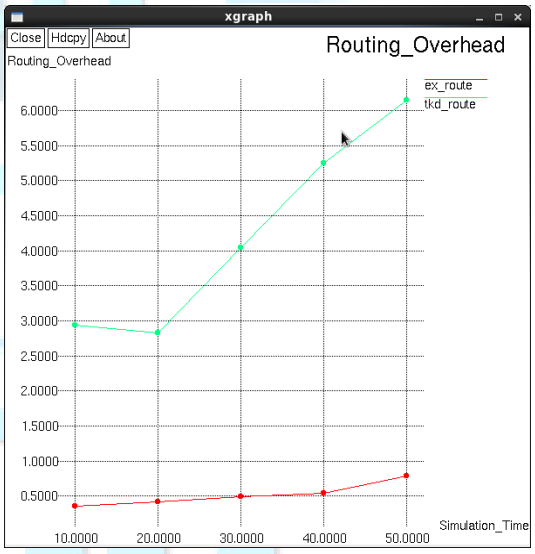

Figure 6 Routing-Overhead of TKD

7.2 Triple key distribution using combinatorial designs

A triple key distribution schemes using combinatorial designs is designed using $\lambda = 3$. Then we can ensure that a pair of keys (say K_1 and K_2) are present in exactly three nodes. The common key between the nodes can then be calculated as before as $hash\left((K_1 \oplus K_2) \parallel id_A \parallel id_B \parallel id_C\right)$, where *A*, *B* and *C* are the communicating nodes.

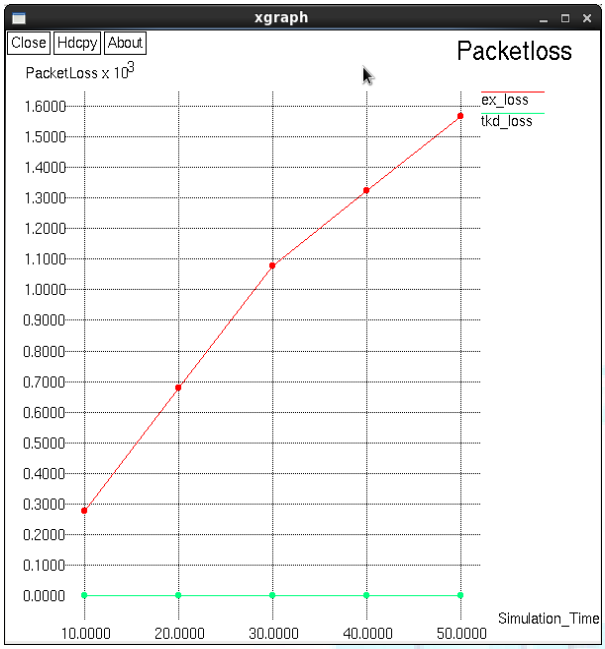

Fig 7: Packet Loss of TKD

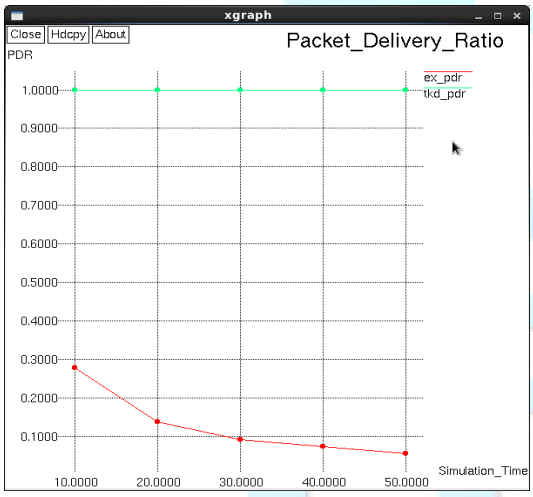

Fig 8: Packet Delivery Ratio of TKD

8. Conclusion and open problems

As wireless communication has become an integral part of today communication, its increased usage has led to many security threats. From the analysis, it can be inferred that efficient key management scheme using combinatorial design has proved to be a more secure solution than the basic scheme in terms of packet delivery ratio, route overhead, packet loss; throughput .Establishing link using combinatorial design is very efficient. Security is increased to a greater extent and the system is made more congested. Typical effects include queuing delay, packet loss or the blocking of new connections. The proposed scheme provides a flexible solution in terms of security and applicable to both static and mobile networks. The future work is to reduce the congestion present in the network and it can be reduced using suitable congestion avoidance algorithm.

References

[1] A. Liu and P. Ning, "TinyECC: A configurable library for elliptic curve cryptography in wireless sensor networks," in IPSN. IEEE Computer Society, 2008, pp. 245–256.
[2] L. Eschenauer and V. D. Gligor, "A key-management scheme for distributed sensor networks," in ACM Conference on Computer and Communications Security, V. Atluri, Ed. ACM, 2002, pp. 41–47
[3] H. Chan, A. Perrig, and D. X. Song, "Random key predistribution schemes for sensor networks," in IEEE Symposium on Security and Privacy. IEEE Computer Society, 2003, pp. 197–213.
[4] C. Blundo, A. D. Santis, A. Herzberg, S. Kutten, U. Vaccaro, and M. Yung, "Perfectly-secure key distribution for dynamic conferences," In Advances in Cryptology: Proceedings of CRYPTO'92, Santa Barbara, CA, Lecture Notes in Computer Science, vol. 740, pp. 471–486, 1993.
[5] W. Du, J. Deng, Y. S. Han, P. K. Varshney, J. Katz, and A. Khalili, "A pairwise key predistribution scheme for wireless sensor networks," ACM Trans. Inf. Syst. Secur., vol. 8, no. 2, pp. 228–258, 2005.
[6] C. J. Mitchell and F. Piper, "Key storage in secure networks," Discrete Applied Mathematics, vol. 21, pp. 215–228, 1988.
[7] S. A. C¸ amtepe and B. Yener, "Combinatorial design of key distribution mechanisms for wireless sensor networks," in ESORICS, ser. Lecture Notes in Computer Science, P. Samarati, P. Y. A. Ryan, D. Gollmann, and R. Molva, Eds., vol. 3193. Springer, 2004, pp. 293–308.
[8] A. Joux, "A one round protocol for tripartite diffie-hellman," J. Cryptology, vol. 17, no. 4, pp. 263–276, 2004.
[9] D. R. Stinson, Cryptography: Theory and Practice, Third Edition. CRC Press Inc., Boca Raton, 2006.
[10] S. Zhu, S. Xu, S. Setia, and S. Jajodia, "Establishing pairwise keys for secure communication in ad hoc networks: A probabilistic approach," in ICNP. IEEE Computer Society, 2003, pp. 326–335.
[11] D. Huang and D. Medhi, "Secure pairwise key establishment in largescale sensor networks: An area partitioning and multigroup key predistribution approach," TOSN, vol. 3, no. 3, pp. 16:1–16:34, 2007.
[12] H. Chan and A. Perrig, "PIKE: peer intermediaries for key establishment in sensor networks," in INFOCOM. IEEE, 2005, pp. 524–535.
[13] S. A. C¸ amtepe and B. Yener, "Key distribution mechanisms for wiles sensor networks: a survey," 2005, technical Report TR-

05-07 Rensselaer Polytechnic Institute, Computer Science Department, March 2005.
[14] J. Lee and D. R. Stinson, "A combinatorial approach to key predistribution for distributed sensor networks," in IEEE Wireless Communications and Networking Conference, WCNC 2005, New Orleans, LA, USA, 2005, pp. 1200–1205.
[15] S. Ruj and B. Roy, "Key predistribution using partially balanced designs in wireless sensor networks," in ISPA, ser. Lecture Notes in Computer Science, I. Stojmenovic, R. K. Thulasiram, L. T. Yang, W. Jia, M. Guo, and R. F. de Mello, Eds., vol. 4742. Springer, 2007, pp. 431–445.
[16] S. Ruj, A. Nayak, and I. Stojmenovic, Theoretical Aspects of Distributed Computing in Sensor Networks. Springer-Verlag, 2010, ch. Key Predistribution in Wireless Sensor Networks when Sensors are within Communication Range. (In Press).
[17] P. Traynor, H. Choi, G. Cao, S. Zhu, and T. L. Porta, "Establishing pairwisekeys in heterogeneous sensor networks," in INFOCOM. IEEE,2006.