

On Maximum Key Pool Size for a Key Pre-Distribution Scheme in Wireless Sensor Networks

Neeraj Mittal Tarun R. Belagodu*

Department of Computer Science

The University of Texas at Dallas

Richardson, TX 75083, USA

neerajm@utdallas.edu

tarun.r.belagodu@intel.com

Abstract

Bootstrapping secure communication among sensor nodes deployed in hostile environment is an important and challenging problem. A common approach to solve this problem is to use a key pre-distribution scheme in which each sensor node is assigned a subset of keys selected from some key pool. The resilience of a key pre-distribution scheme depends on the size of the key pool that the scheme uses for distributing keys among sensor nodes. After deployment, if two sensor nodes are within communication range of each other and share at least one common key, then they can establish a secure channel using the common key. We show that, when the key distribution is near-uniform, the maximum size a key pool that can be used by any key pre-distribution scheme is upper-bounded by $\frac{s^2}{p}$, where s is the amount of space available on a sensor node for storing keys and p is the probability that two sensor nodes share a common

*The author is currently working as a software design engineer at Intel Corporation.

key. We define the notion of *utilization factor* of a key pre-distribution scheme to measure how effective the scheme is in using the largest key pool available at its disposal for fixed values of s and p . We explore the effect of the utilization factor of a scheme on its resilience.

Key words: distributed systems, sensor nodes, wireless network, bootstrapping secure communication, key pre-distribution

1 Introduction

When sensor nodes are deployed in a hostile environment (*e.g.*, monitoring enemy territory in a battle), *bootstrapping* secure communication among neighboring sensor nodes is an important problem. One approach that has been recently proposed to bootstrap secure communication is to assign a subset of keys (selected from a key pool) to sensor nodes before deployment. After deployment, if two sensor nodes are within communication range of each other, they can establish a secure channel between them in case they share at least one key. Note that, to determine whether two sensor nodes share a key, it is not necessary for nodes to exchange their keys. Rather, it is sufficient for them to exchange only indices of keys they possess, which ensures that keys themselves are never sent over insecure channels. This approach is referred to as *key pre-distribution approach* [7]. The assignment of keys to sensor nodes can be either done randomly [7, 4, 6] or deterministically [8, 9, 3, 12].

Key pre-distribution approach is especially attractive for solving the bootstrapping problem because of two reasons [7, 6]. First, after deployment, the sensor network can operate independently without any additional infrastructure, which is especially hard to provide in a hostile environment. Second, the approach uses symmetric cryptography rather than asymmetric cryptography. The former is more desirable to use than the latter in a sensor network due to limited computing power, memory and energy available on sensor nodes.

Any key distribution scheme has three main objectives. First, the scheme should maximize the probability that two sensor nodes share a common key if they find themselves to be neighbors of each other after deployment. In the absence of any deployment knowledge, this

is achieved by maximizing the probability that any two nodes share a common key. This probability is referred to as the *overlap probability* of the scheme [7]. The set of nodes with which a node shares at least one common key are referred to as its *key-neighbors*. On the other hand, the set of nodes that are within communication range of a node are referred to as its *field-neighbors*. Second, the scheme should minimize the damage caused to the rest of the network once a certain number of nodes have been compromised. Specifically, it should maximize the probability that a channel between two (uncompromised) nodes is still secure given that a certain number of nodes have been compromised by an adversary. This is referred to as the *degree of resilience* of the scheme. Third, the scheme should use as little space as possible, that is, it should be *space-efficient*. Sensor nodes typically have severe resource constraints and, therefore, only have limited amount of space available for storing keys.

The three requirements are somewhat conflicting with each other. For example, a scheme that guarantees that every pair of sensor nodes share a common key and is perfectly resilient requires that a sensor node has enough space to store one unique key for each node in the network. On the other hand, a scheme that requires only one key to be stored on each node and still guarantees that every pair of sensor nodes share a common key has zero resiliency (master key based approach). Finally, a scheme that is perfectly resilient and requires only one key per node has extremely low overlap probability—a node shares a key with only one other node.

It has been observed by other researchers that, given the amount of space available on a sensor node and a desired overlap probability, the resilience of the sensor network can be increased by increasing the size of the key pool from which keys are chosen. We ask the following fundamental questions. *Is there a bound on the maximum size of key pool that can be used for selecting keys? If yes, what is the exact nature of the bound?* We show that, if the key distribution among sensor nodes is almost uniform, then the maximum key pool size that can be used by any scheme depends only on two factors, namely the amount of space available on a sensor node for storing keys and the overlap probability, irrespective of the number of sensor nodes in the network.

Specifically, in this paper, we investigate the relationship between various parameters of

a key pre-distribution scheme, namely (1) s : the amount of space available on a sensor node for storing keys, (2) p : the probability that two sensor nodes share a common key, (3) N : the number of sensor nodes in the system, and (4) K : the size of the key pool used by a key distribution scheme. We show that, when the key distribution is near uniform and $s \ll (N - 1)p$, the size of the key pool that *any* key pre-distribution scheme can use for distributing keys among sensor nodes is upper bounded by a function of s and p , namely s^2/p .

Based on the upper bound established, we define the notion of *utilization factor* of a key pre-distribution scheme. For given values of s and p , the utilization factor of a scheme, denoted by $\rho(s, p)$, is given by the ratio of the size of the actual key pool used by the scheme and the maximum size of the key pool that any scheme can use. We also investigate the relationship between resilience of a key pre-distribution scheme and its effectiveness in utilizing the largest allowable key pool as measured by its utilization factor. Note that the notion of utilization factor can be used to evaluate *how far a key pre-distribution scheme is from an optimal scheme*.

2 Estimating Bound on Key Pool Size with Near-Uniform Key Distribution

Our analysis assumes the keys are distributed almost uniformly among sensor nodes. This is because, intuitively, uniform key distribution improves the resilience of the network. If some key occurs more frequently than others in sensor nodes, then, once a node containing that key has been compromised, a large fraction of channels between sensor nodes, which themselves have not been compromised so far, may be compromised as well. Our assumption is consistent with the assumption made by other researchers (*e.g.*, [7, 4, 8, 3, 6, 12]).

Let N denote the number of sensor nodes in the system. We assume that N is sufficiently large so that $N - 1 \approx N$. Let s denote the amount of space (or memory) available on each sensor node for storing keys. We use K to refer to the size of the key pool. For a key k_i in the key pool, let f_i denote the number of sensor nodes in the network that carry the key k_i .

Symbol	Meaning
N	number of sensor nodes in the network
s	amount of space available for storing keys on each sensor node (measured in terms of number of keys)
p	probability that two sensor nodes share a common key
K	size of the key pool from which keys are chosen
k_i	i -th key in the key pool
f_i	number of sensor nodes that contain the i^{th} key, that is, frequency of key k_i
μ_f	mean value of key frequencies
	$\mu_f = \frac{1}{K} \sum_{i=1}^K f_i$
σ_f	standard deviation of key frequencies
	$\sigma_f = \sqrt{\frac{1}{K} \sum_{i=1}^K (f_i - \mu_f)^2}$
κ_f	coefficient of variation of key frequencies
	$\kappa_f = \frac{\sigma_f}{\mu_f}$

Table 1: Notation used in this paper

Clearly, for key to be useful, that is, it can be used to establish at least one common channel, f_i is at least 2. Hereafter, in this paper, we assume that each key is useful. Therefore,

$$\sum_{i=1}^K f_i = Ns \quad (1)$$

We have,

$$\begin{aligned} & \forall i : 1 \leq i \leq K : f_i \geq 2 \\ \Rightarrow & \{ \text{algebra} \} \\ & \sum_{i=1}^K f_i \geq 2K \\ \Rightarrow & \{ \text{using (1)} \} \\ & K \leq \frac{Ns}{2} \end{aligned}$$

Therefore,

$$K \leq \frac{Ns}{2} \quad (2)$$

Note that bound in (2) holds irrespective of whether key distribution is uniform or non-uniform. We now derive a tighter upper bound on key pool size that is independent of the number of sensor nodes in the network. Let C_s denote the number of pairs of sensor nodes that share a common key and p be the overlap probability, that is,

$$C_s = \left(\frac{N(N-1)}{2} \right) p = \frac{N(N-1)p}{2} \quad (3)$$

Assume that all sensor nodes are “identical” in the sense that they have approximately the same number of key-neighbors. Therefore each sensor node has approximately $(N-1)p$ key-neighbors. Typically, in a sensor network system, a sensor node is expected to have much larger number of neighbors than the amount of space it has for storing keys. Therefore, we assume the following:

$$s \leq (N-1)p \quad (4)$$

We refer to the ratio $\frac{s}{(N-1)p}$ as the *space-constraint factor (SCF)* and denote it by γ . If $\gamma = 1$ (that is, $s = (N-1)p$), then a sensor node can use a different key to encrypt the channel with each of its key-neighbor (provided the key-neighbor is also its field-neighbor). As a result, the resulting scheme has perfect resilience [4]. However, we expect the space-constraint factor to be much smaller than 1 in practice. Intuitively, the space-constraint factor measures the extent by which the space on a sensor node is short of the space required to achieve perfect resiliency.

Observe that key k_i can be used to establish at most $f_i(f_i-1)/2$ secure channels in the network. Therefore,

$$C_s \leq \sum_{i=1}^K \frac{f_i(f_i-1)}{2} \quad (5)$$

In our analysis, we use the following well-known equality in statistics:

$$\sum_{i=1}^K f_i^2 = K(\mu_f^2 + \sigma_f^2) \quad (6)$$

where μ_f and σ_f denote the mean and standard deviation, respectively, of key frequencies. The ratio $\kappa_f = \frac{\sigma_f}{\mu_f}$ is known as *coefficient of variation* and, in our case, measures “variability”

in key distribution. If the key distribution is almost uniform, that is, all key frequencies are close to the mean value, then $\kappa_f \approx 0$ provided $\mu_f \gg 1$. Now, we have,

$$\begin{aligned}
& \{ \text{using (5)} \} \\
C_s & \leq \sum_{i=1}^K \frac{f_i(f_i - 1)}{2} \\
\Rightarrow & \{ \text{using (3)} \} \\
\frac{N(N-1)p}{2} & \leq \frac{1}{2} \sum_{i=1}^K (f_i^2 - f_i) \\
\Rightarrow & \{ \text{using (1) and (6)} \} \\
N(N-1)p & \leq K(\mu_f^2 + \sigma_f^2) - Ns \\
\Rightarrow & \{ \text{simplifying} \} \\
N(N-1)p + Ns & \leq K\mu_f^2(1 + \kappa_f^2) \\
\Rightarrow & \{ \text{from (1), } K\mu_f = Ns \text{ which implies that } \mu_f = \frac{Ns}{K} \} \\
N(N-1)p + Ns & \leq K \frac{N^2 s^2}{K^2} (1 + \kappa_f^2) \\
\Rightarrow & \{ \text{simplifying} \} \\
K & \leq \frac{Ns^2}{(N-1)p + s} (1 + \kappa_f^2) \\
\Rightarrow & \{ \text{simplifying} \} \\
K & \leq \left(\frac{N}{N-1} \right) \left(\frac{s^2}{p} \right) \left(\frac{1 + \kappa_f^2}{1 + \gamma} \right) \\
\Rightarrow & \{ N \text{ is large which implies that } N-1 \approx N \} \\
K & \leq \left(\frac{s^2}{p} \right) \left(\frac{1 + \kappa_f^2}{1 + \gamma} \right)
\end{aligned}$$

Note that γ lies in the range $(0, 1]$. In fact, in real life, we expect γ to be much smaller than 1. For example, for $N = 10,000$, $p = 0.2$ and $s = 100$, $\gamma = \frac{s}{(N-1)p} = 0.05 \approx 0$. It turns out that if the key distribution is almost uniform, then γ and μ_f are closely related. Again, assume that each sensor node has approximately the same number of key-neighbors. Each key k_i on a sensor node can be used by the node to establish at most $f_i - 1$ secure channels with its neighbors, which is approximately equal to $\mu_f - 1$. We have,

$$(N-1)p \leq s(\mu_f - 1)$$

$$\begin{aligned}
&\Rightarrow \{ \text{simplifying} \} \\
&\mu_f \geq \frac{(N-1)p}{s} + 1 \\
&\Rightarrow \{ \text{definition of } \gamma \} \\
&\mu_f \geq \frac{1}{\gamma} + 1
\end{aligned}$$

In case $\gamma \ll 1$, $\mu_f \gg 2$. This in turn implies that, when the key distribution is almost uniform, $\kappa_f \ll 1$, where κ_f is the coefficient of variation. Therefore, we have,

$$K \leq \frac{s^2}{p} \left(\frac{1 + \kappa_f^2}{1 + \gamma} \right) \approx \frac{s^2}{p} \quad (7)$$

We denote the expression $\frac{s^2}{p}$ by K_{\max} . Intuitively, K_{\max} denotes the maximum size of the key pool that can be used for given values of s and p . We refer to the ratio of the actual key pool size to the maximum key pool size as the *utilization factor (UF)* and denote it by $\rho(s, p)$.

The assumption that all sensor nodes are identical is not really necessary. Let s_{avg} and p_{avg} denote the average space and average overlap probability, respectively, of a sensor node. Formally,

$$s_{avg} = \frac{1}{N} \sum_{i=1}^N s_i \quad \text{and} \quad p_{avg} = \frac{1}{N} \sum_{i=1}^N p_i$$

where s_i and p_i denote space and overlap probability, respectively, for the i -th sensor node. It can be shown that (7) still holds provided s is replaced with s_{avg} and p is replaced with p_{avg} [13].

2.1 Bound on Key Pool Size when Deployment Knowledge is Used

Du *et al.* [5] and Liu *et al.* [10, 11] show that the resilience of the network can be improved substantially (at least against random attacks by an adversary) by using deployment knowledge at the time of distributing keys among sensor nodes. Deployment knowledge basically limits the number of sensor nodes that can be neighbors of a given sensor node in the field. The main reason for improvement in resiliency is that deployment knowledge allows a much bigger key pool size to be used than is otherwise possible. *Does it mean that the upper bound derived in the previous section does not hold when deployment knowledge is used during key*

distribution? The answer is no. The upper bound holds as long as key distribution is almost uniform and space constraint factor is small (that is, coefficient of variation is small). However, the reason for the improvement in resilience can be explained as follows. We call two sensor nodes as *region-neighbors* if that can potentially be neighbors of each other in the field after deployment (based on the deployment knowledge). Let η denote the ratio of the number of region-neighbors of a sensor node to the total number of sensor nodes in the network. Further, let p_{local} denote the probability that a sensor node shares a common key with its region-neighbor. We refer to p_{local} as the *local overlap probability*. Therefore the probability that *any two* sensor nodes share a common key, which we refer to as the *global overlap probability*, is given by $p_{\text{global}} = \eta \times p_{\text{local}}$. (We assume that two sensor nodes may possibly share a common key only if they are region-neighbors of each other.)

For instance, suppose $N = 10,000$ and consider a sensor node α . In the absence of any deployment knowledge, any subset of the remaining 9,999 sensor nodes can be neighbors of α in the field after deployment. Now, suppose, using deployment knowledge, we can identify a set of 1,000 sensor nodes, say P_α such that only nodes from P_α can potentially be neighbors of α . In this case, it is sufficient for a key pre-distribution scheme to ensure that α shares a key with only nodes in P_α with certain overlap probability, say 0.5. Therefore, $\eta = 1000/10000 = 0.1$, $p_{\text{local}} = 0.5$ and $p_{\text{global}} = 0.1 \times 0.5 = 0.05$.

When no deployment knowledge is assumed, $\eta = 1$ implying that $p_{\text{global}} = p_{\text{local}}$. Based on the analysis in the previous section, the size of key pool that can be used is upper bounded by:

$$K \leq \frac{s^2}{p_{\text{global}}} = \frac{s^2}{\eta p_{\text{local}}} \quad (8)$$

For fixed values of s and p_{local} , the size of the key pool can be increased by decreasing η , which, in turn, depends on the extent of the deployment knowledge. Therefore, deployment knowledge *helps improve resiliency of the network by decreasing η* which, in turn, decreases p_{global} . Reducing p_{global} increases the size of the key pool that can be used for assigning keys to sensor nodes.

3 Effect of Utilization Factor on Network Resiliency

Suppose an adversary has compromised w randomly selected sensor nodes, where $w \geq 1$. Therefore all keys stored in these nodes have been revealed to the adversary. Consider a channel c between two sensor nodes that have not been compromised. We are interested in computing the probability that the channel c has been compromised. Let \mathcal{A}_w denote the event that the adversary has compromised w sensor nodes at random. Further, let \mathcal{B}_i denote the event that c uses key k_i for encryption and let \mathcal{C}_i denote the event that the key k_i has been compromised. Du *et al.* show in [6] that, when key distribution is uniform, the probability that channel c has been compromised given that w sensor nodes, chosen at random, have been compromised already is given by:

$$\begin{aligned} \Pr(c \text{ has been compromised} \mid \mathcal{A}_w) &= \sum_{i=1}^K \Pr(\mathcal{B}_i) \Pr(\mathcal{C}_i \mid \mathcal{A}_w) = K \cdot \frac{1}{K} \cdot \Pr(\mathcal{C}_1 \mid \mathcal{A}_w) \\ &= \Pr(\mathcal{C}_1 \mid \mathcal{A}_w) \end{aligned} \quad (9)$$

If w is small compared to N , and key distribution is almost uniform, then:

$$\Pr(\mathcal{C}_1 \mid \mathcal{A}_w) \approx 1 - \left(1 - \frac{f_1}{N}\right)^w \approx 1 - \left(1 - \frac{\mu_f}{N}\right)^w \quad (10)$$

Using (1), it follows that $Ns = K\mu_f$. This implies that:

$$\frac{\mu_f}{N} = \frac{s}{K} \quad (11)$$

Combining (9), (10) and (11), we obtain,

$$\begin{aligned} \Pr(c \text{ is compromised} \mid \mathcal{A}_w) &\approx 1 - \left(1 - \frac{s}{K}\right)^w \\ &\approx 1 - \left(1 - \frac{ws}{K}\right) \\ &= \frac{ws}{\rho(s,p) K_{\max}} \\ &= \left(\frac{ws}{\rho(s,p)}\right) \left(\frac{p}{s^2}\right) \\ &= \left(\frac{wp}{s}\right) \frac{1}{\rho(s,p)} \end{aligned} \quad (12)$$

In other words, probability that a channel between two uncompromised sensor nodes has been compromised is directly proportional to the number of nodes that have been compromised and the overlap probability. Further, it is *inversely* proportional to the utilization

factor and the amount of key space available on a sensor node. Consequently, for fixed values of s , p and w , the resilience of the network can be increased by *increasing the utilization factor of the key distribution scheme*.

4 Extensions to the Basic Key Pre-distribution Scheme

In our analysis of resiliency so far, we assume that a key corresponds to a simple symmetric cryptographic key. Therefore, once even a *single* node containing a given key is compromised, all channels encrypted using that key are compromised as well. However, there are other more sophisticated schemes which use either a matrix of size $(\lambda + 1) \times (\lambda + 1)$ [1] or a bivariate polynomial of degree λ [2] to compute a pairwise key between two sensor nodes. These schemes satisfy the desirable property that the scheme is completely secure as long as λ or fewer nodes have been compromised. Further, once $\lambda + 1$ nodes have been compromised, the scheme is completely broken, that is, the adversary can potentially decrypt all messages encrypted using the cryptographic scheme.

Du *et al.* [6] and Liu *et al.* [12] describe key pre-distribution approaches in which the key pool consists of multiple instances of these cryptographic schemes (matrix- or polynomial-based). Each sensor node carries a subset of the instances selected from the key pool (or, more appropriately, *instance pool*). If two sensor nodes share at least one instance, then the common instance can be used to establish a pairwise key among the nodes. The two approaches can be simply seen as a kind of key pre-distribution approach in which *a key corresponds to an instance of matrix- or polynomial-based scheme* [10].

Note that the upper bound established on key pool size in Section 2 is applicable to such key pre-distribution approaches as well. For such approaches, s is taken to be the *number of instances* that a sensor node can carry instead of the number of keys. The total amount of space used by a sensor node is then given by $m = (\lambda + 1)s$ (and not s as in the case of a simple key-based cryptographic scheme). Du *et al.* show in [6] that, with matrix-based scheme, the probability that a channel between two uncompromised nodes has been compromised given

that w sensor nodes have been compromised already remains close to zero for relatively large values of w . Moreover, there is a value of w after which the probability starts increasing almost exponentially. This change in behavior (or breaking point) approximately occurs at $w_{bp} \approx m \frac{K}{s^2}$. We have,

$$\begin{aligned}
w_{bp} &\approx m \frac{K}{s^2} \\
&= (\lambda + 1)s \frac{\rho(s, p) K_{\max}}{s^2} \\
&= (\lambda + 1) \frac{\rho(s, p) s^2}{s p} \\
&= \left(\frac{(\lambda + 1) s}{p} \right) \rho(s, p)
\end{aligned} \tag{13}$$

Note that the value of the breaking point is *directly* proportional to s , λ and $\rho(s, p)$ and inversely proportional to p . Again, as before, for fixed values of s , p and λ , the value at which the breaking point occurs can be increased by *increasing the utilization factor of the key (or instance) distribution scheme*.

Du *et al.* [6] observe that their scheme, which is derived from Blom's matrix-based scheme [1], has better resilience than Blom's scheme for the same amount of space. However, the main reason for the improvement is that Blom's scheme always has an overlap probability of 1, whereas Du *et al.*'s scheme has overlap probability smaller than 1. Basically, by lowering the overlap probability, they are able to increase the value of the breaking point. Since the utilization factor of their scheme is much smaller than 1, especially when p is large (at least 0.5), the value of the breaking point can be further increased by using a scheme for distributing instances among sensor nodes with better utilization factor [8].

5 Conclusion

For a given amount of space available on a sensor node for storing keys and a given probability of key overlap between sensor nodes, the resilience of a network depends on the size of the key pool used by a key pre-distribution scheme. In this paper, we have derived an upper bound on the size of the key pool that any key pre-distribution scheme can use for assigning keys to sensor nodes. Our upper bound can be used to *quantify* how far a key pre-distribution

scheme is from optimality.

Two key pre-distribution schemes that are near optimal in terms of key pool size may differ in other respects. For example, if two sensor nodes that do not share a common key wish to communicate securely, then they have to agree on a secret key using a *secure* path consisting of one or more sensor nodes (in case it exists). Therefore, in addition to resilience, another important measure of performance of a key pre-distribution scheme is the communication overhead (in terms of number of hops) required to establish such path-based keys [7]. Even if two schemes are near optimal with respect to key pool size, they may still have different communication overheads, thereby making one preferable over the other.

References

- [1] R. Blom. An Optimal Class of Symmetric Key Generation Systems. In *Advances in Cryptology—Proceedings of the Workshop on the Theory and Application of Cryptographic Techniques (EUROCRYPT)*, pages 335–338, 1984.
- [2] 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 the Annual International Cryptology Conference (CRYPTO)*, pages 471–486, August 1992.
- [3] S. A. Çamtepe and B. Yener. Combinatorial Design of Key Distribution Mechanisms for Wireless Sensor Networks. In *Proceedings of the 9th European Symposium on Research Computer Security (ESORICS)*, pages 293–308, 2004.
- [4] H. Chan, A. Perrig, and D. Song. Random Key Predistribution Schemes for Sensor Networks. In *Proceedings of the IEEE Symposium on Security and Privacy*, pages 197–213, May 2003.
- [5] W. Du, J. Deng, Y. S. Han, and P. K. Varshney. A Pairwise Key Pre-distribution Scheme for Sensor Networks using Deployment Knowledge. *IEEE Transactions on Dependable and Secure Computing*, 3(2):62–77, 2006.
- [6] W. Du, J. Deng, Y. S. Han, P. K. Varshney, J. Katz, and A. Khalili. A Pairwise Key Pre-distribution Scheme for Wireless Sensor Networks. *ACM Transactions on Information and System Security (TISSEC)*, 8(2):228–258, May 2005.

- [7] L. Eschenauer and V. Gligor. A Key Management Scheme for Distributed Sensor Networks. In *Proceedings of the 9th ACM Conference on Computer and Communications Security*, pages 41–47, November 2002.
- [8] J. Lee and D. R. Stinson. Deterministic Key Predistribution Schemes for Distributed Sensor Networks. In *Proceedings of the Annual Symposium on Selected Areas in Cryptography*, pages 294–307, 2004.
- [9] J. Lee and D. R. Stinson. A Combinatorial Approach to Key Predistribution for Distributed Sensor Networks. In *Proceedings of the IEEE Wireless Communications and Networking Conference*, 2005. CD-ROM, paper PHY53-06.
- [10] D. Liu and P. Ning. Improving Key Pre-Distribution with Deployment Knowledge in Static Sensor Networks. *ACM Transactions on Sensor Networks (TOSN)*, 1(2):204–239, November 2005.
- [11] D. Liu, P. Ning, and W. Du. Group-Based Key Pre-Distribution in Wireless Sensor Networks. In *Proceedings of the ACM Workshop on Wireless Security (WiSe)*, September 2005.
- [12] D. Liu, P. Ning, and R. Li. Establishing Pairwise Keys in Distributed Sensor Networks. *ACM Transactions on Information and System Security (TISSEC)*, 8(1):41–77, February 2005.
- [13] N. Mittal and T. R. Belagodu. On Maximum Key Pool Size for a Key Pre-Distribution Scheme in Wireless Sensor Networks. Technical Report UTDCS-17-06, Department of Computer Science, The University of Texas at Dallas, March 2006.

Neeraj Mittal received his B.Tech. degree in Computer Science and Engineering from the Indian Institute of Technology, Delhi in 1995 and M.S. and Ph.D. degrees in Computer Science from the University of Texas at Austin in 1997 and 2002, respectively. He is currently an Assistant Professor in the Department of Computer Science and a co-director of the Advanced Networking and Dependable Systems Laboratory (ANDES) at the University of Texas at Dallas. His research interests include distributed systems, sensor networks, and cognitive radio networks.

Tarun R. Belagodu received his B.E. degree in Information Science and Technology from J.S.S. Academy of Technical Education in 2003 and M.S. degree in Computer Science from the University of Texas at Dallas in 2006. He is currently working at Intel Corporation as a Software Design Engineer. His interests are in areas of key management in sensor networks, algorithms for distributed operating systems and graphics.