Available online at www.sciencedirect.com
ScienceDirect
Electronic Notes in Theoretical Computer Science
ELSEVIER
Electronic Notes in Theoretical Computer Science 192 (2008) 31–41
www.elsevier.com/locate/entcs

An Application-Oriented Framework for Wireless Sensor Network Key Establishment

Keith M. Martin[2] Maura Paterson[1,3]

Information Security Group
Royal Holloway, University of London
Egham, UK

Abstract

The term wireless sensor network is applied broadly to a range of significantly different networking environments. On the other hand there exists a substantial body of research on key establishment in wireless sensor networks, much of which does not pay heed to the variety of different application requirements. We set out a simple framework for classifying wireless sensor networks in terms of those properties that directly influence key distribution requirements. We fit a number of existing schemes within this framework and use this process to identify areas which require further attention from key management architects.

Keywords: Wireless Sensor Networks, Key Management, Key Predistribution

1 Introduction

While the precise properties of *wireless sensor networks* vary considerably, it is generally accepted that they typically consist of small, inexpensive, battery-powered sensing devices fitted with wireless transmitters, which can be spatially scattered to form an *ad hoc network*. While sensors have the ability to communicate through wireless channels, their energy, computational power and memory are constrained. Sensor networks have been proposed for a wide range of different applications, including disaster relief operations, seismic data collection, wildlife monitoring and military intelligence gathering. Sensors are distributed around the application environment and then attempt to set up a network in order to exchange and forward data.

The wireless nature of sensor communication makes traffic highly vulnerable, hence the desire for cryptographic security services. The highly constrained nature

[1] This author was supported by EPSRC grant EP/D053285/1
[2] Email: keith.martin@rhul.ac.uk
[3] Email: m.b.paterson@rhul.ac.uk

doi:10.1016/j.entcs.2008.05.004

of sensors favours the use of symmetric cryptography, hence we restrict the survey aspect of this paper to symmetric schemes.

Sensor networks typically lack infrastructure and sensors typically have limited computational ability. Hence *key predistribution* is the favoured basis for key establishment, with keying material stored in sensor memory prior to deployment. A comprehensive classification survey of schemes prior to March 2005 is given in [2]. This classification, however, focuses on the mathematical construction techniques employed, rather than on the properties of the networks for which the schemes are to be applied.

It is clear from the survey of sensor network applications in [34] that the term *wireless sensor network* is used to describe a variety of significantly different network environments. The multidimensional design space proposed in [34] classifies established sensor networks in terms of physical and logical differences. This is a useful general taxonomy, but it does not clearly define the different application needs with respect to key establishment. In [37] Van der Merwe *et al.* survey key management in mobile ad hoc networks; they give the view that "the key predistribution field for sensor networks currently requires a comprehensive analysis of the existing schemes in terms of security, performance, and implementation practicality." [37]

The intention of this paper is to establish a framework for classifying different sensor network environments from the point of view of key establishment requirements. Fitting existing schemes within this framework permits a clearer comparison of schemes appropriate for particular network environments. Furthermore, this framework enables the identification of application environments to which inadequate attention has been paid in the literature.

In the next section we specify the networks that fall within the scope of this paper and give a brief overview of key establishment for such networks, together with issues affecting it. In Section 3 we discuss properties of sensor networks that affect the key distribution requirements and use these properties to provide a framework for studying key establishment in sensor networks. We subsequently discuss how particular schemes fall within this framework in Section 4 and highlight some topics requiring further research attention.

2 Key establishment for wireless sensor networks

Our framework is primarily designed to encompass key establishment schemes based on key predistribution. Thus we assume that sensors have keying material stored in their memories before deployment by a trusted authority, but in general have no further access to this trusted authority after deployment. In particular, schemes relying on the presence of a base station that can always communicate securely with the sensors fall outside the scope of this survey, as do schemes dependent on public-key techniques. Note that relying on key predistribution does not preclude sensors themselves acting as local distributors of keying material and enabling further key establishment through sensor-to-sensor communication.

We assume that the network is vulnerable to attack by an adversary who has

the ability to compromise any given node and extract any keys or other secret data stored in its memory, and to intercept any wireless communication within the network. Such an adversary is termed a *global passive adversary* by Anderson *et al.* [1]. The literature contains examples of schemes based on other attack models, such as [1,13], however in this study we confine ourselves to schemes based on the global passive adversary model.

Let $\mathcal{S}$ be the set of sensors in our network. The *ideal communication structure* $\mathcal{C}$ is the collection of subsets of $\mathcal{S}$ for whom we (ideally) wish to establish common (group) keys. For any $A \in \mathcal{C}$ we use k_A to denote the common key for the subset of sensors A. The choice of the term *ideal* is deliberate because:

(i) In many wireless sensor network applications there is a degree of lack of control over the sensor network that is actually established, since the precise location of sensor deployment may not be controllable, and sensors may even be mobile.

(ii) Groups of sensors may be unable to communicate due to the distance between them exceeding their communication range, or sensors becoming absent from the network due to battery failure, adversarial attack *etc.*

(iii) It may be more efficient to predistribute keys in such a way that the not every group of sensors in $\mathcal{C}$ shares a key, and rely on a limited amount of key agreement between deployed sensors to establish the remaining group keys.

There is thus often a discrepancy between the *network communication structure* $\mathcal{C}^*$, which describes the groups of sensors who share predistributed keys, and the ideal communication structure, which describes the groups of sensors that we ultimately may want to share a common key. It is acceptable to use sensor-to-sensor communication to bridge any gaps between these two communication structures since sensor networks are designed to be co-operative networks that can robustly handle absences of desirable links through adaptable routing.

3 Application-oriented key establishment framework

In this section we describe our simple framework for studying key establishment within the wide range of different sensor network environments. We split this framework into three parts:

(i) Categories of sensor networks that significantly affect key establishment design.

(ii) Relevant variable parameters that determine instances within each of the above defined categories.

(iii) Performance indicators that can be used to assess specific key establishment schemes.

3.1 Categories of sensor networks

The following three aspects of sensor networks significantly affect key establishment design. Solutions proposed for one particular set of categories are unlikely to be readily applicable for another set of categories.

(i) **Homogeneity**: The relative capabilities of different sensors. Sensor networks tend to fall into one of two classes:
   (a) *Homogeneous*: all sensors have the same capabilities.
   (b) *Hierarchical*: there is a natural hierarchy of sensors with respect to their capabilities (with fewer sensors at higher, more "powerful" levels). The most common hierarchical networks are *two-level*, where there are two classes of sensor. Note that "powerful" could relate to issues such as amount of key storage, computational capability or degree of mobility.

(ii) **Deployment location control**: The degree of control over sensor locations on deployment. Five classes of sensor network can be identified:
   (a) *Fixed, full control*: the precise location of sensors is known before deployment. Applications where sensors may then undertake strictly limited mobility (for example monitoring points on a glacier) can be placed within this class for the purposes of key management.
   (b) *Fixed, partial control*: some information about the location of sensors is known before deployment. This class includes applications where clusters of sensors are dropped from the air over fixed locations.
   (c) *Fixed, no control*: the location of sensors cannot be predicted before deployment. This class includes applications where sensors are randomly scattered over a monitoring area.
   (d) *Locally mobile*: sensors are mobile within a controlled locality. In this class, sensors can be assumed to be free to move to any location within a strictly defined local area, but cannot stray out of this area.
   (e) *Fully mobile*: sensors are mobile. In this class, sensors are free to move anywhere within the network environment.

(iii) **Nature of ideal communication structure**: The desired ideal communication structure of the sensor network. This can consists of any collection of groups of sensors. In the case of homogenous sensor networks, three important classes of ideal communication structure are:
   (a) *t-complete*: all subsets of sensors of size t. By far the most common communication structure within this class is *pairwise complete* (2-complete). This class of communication structure is particularly appropriate in the case of networks with no control over deployment location.
   (b) *Locally t-complete*: all local subsets of sensor of size t, where the precise notion of *local* varies depending on the context, but generally refers to sensors who are neighbours of one another in some sense. Again the most common communication structure is *pairwise locally complete*, which arises in applications where the most commonly required communication flow is between a (mobile) external *sink* and any sensor. In this case we need to construct paths from sensors to the mobile sink, hence the need for neighbouring sensors to be able to share key associations. Such a communication structure can only be defined when there is at least partial knowledge of sensor deployment location.
   (c) *Regionally t-complete*: all subsets of sensors of size t within a specified

region. This differs from locally t-complete in that sensors who belong to the same "region" (but are not necessarily neighbours) are required to share key associations. This type of communication structure might be employed, for example, in the case of a network with locally mobile sensors.

In heterogeneous networks, the more powerful sensors normally bear the majority of the communication burden. The ideal communication structure in such networks tends to depend on the nature of the hierarchy. For example, in the *backhaul* model [35] there are two levels and the ideal communication structure consists of:

- all pairs of top-level sensors;
- pairs of (top-level, bottom-level) sensors, such that each bottom-level sensor appears in precisely one pair.

3.2 Variable sensor network parameters

Having identified which set of categories in Section 3.1 matches a particular sensor network application, the following parameters of sensor networks define particular instances of key establishment solutions. By this we mean that while it is often possible to define a generic key establishment technique based on the first categorisation, the following parameters tend to form variables that can be set to define a specific scheme.

- **Storage**: The storage capability of a sensor. This is perhaps the most significant parameter in terms of its direct limiting effect on key establishment scheme design.
- **Energy**: The energy available for a sensor to conduct computations and communications. It is generally considered that the energy requirements for communication far outweigh those of computation.
- **Range**: The communication range over which a sensor can contact other sensors. This is also related to the energy capability since greater communication ranges tend to consume more power. Note that a sensor that has a certain communication range might choose not to use the full range capability, as a power saving measure.

We note that these variable parameters tend to be closely related. For example, in a two-level heterogenous sensor network it is likely that top-level sensors will have larger storage, more power and greater range. However, particular applications may constrain some of these variable parameters more than others.

3.3 Performance indicators

The last part of the framework identifies quantities that can be used to compare the performance of key establishment schemes. These allow two key establishment schemes for the same sensor network category set and parameter settings to be directly compared.

- **Connectivity**: This is a measure of how closely the network communication structure matches the ideal communication structure.

- **Scalability**: This measures the feasibility of use of the scheme with large network sizes. It essentially reflects the storage requirements relative to the number of nodes in the network.
- **Resilience**: This indicates the proportion of established keys that become compromised once the adversary has access to the secret data from a small proportion of the nodes.
- **Computation/Communication overheads**: These measure the precise costs of a particular solution.

While the above performance indicators are broadly adopted in the literature, there appears to be a notable lack of universally-accepted performance measures for interpreting them. Most published schemes contain parameters that can be chosen to permit a tradeoff between these quantities, although this is not always expressed directly in numeric terms.

4 Categorising existing key establishment schemes

In Section 3 we isolated categories of sensor networks that will require very different key establishment solutions. We now match a number of published key establishment schemes to part of this framework, in order to summarise what has been achieved in the literature and highlight areas that remain open for further investigation.

	2-compl/ t-compl	locally 2-compl/ locally t-compl	regionally 2-compl/ regionally t-compl	hierarchical-backhaul
fixed, full control				
fixed, partial control		[28]/	[10][11][12][38] [9][14][21][28]/[18]	
fixed, no control	[8][17][19][20] [32][39][33] [3][4][23][24][25] [5][6][7] [10][11][12][15] [27][29][31][30]			[35]

Fig. 1. Key establishment schemes within the framework

In Figure 1 we have tabulated published schemes within our framework in terms of the type of network that they are designed to support. We now consider in more detail the schemes appearing in the various categories, before discussing open problems that arise from the examination of this categorisation.

4.1 2-Complete schemes with no location control

Figure 1 clearly demonstrates that most of the key predistribution literature addresses the problem of seeking a 2-complete key predistribution scheme for a network with fixed sensors, but no control over sensor location. It appears that schemes

of this category form the default *key predistribution schemes for wireless sensor networks*, when the wireless sensor network environment for which a solution is being proposed is not clearly articulated. Within this category it is possible to identify several basic approaches to the design of key predistribution schemes. *Probablistic schemes* include Eschenauer and Gligor's seminal scheme [17] in which each node is assigned a fixed number m of keys drawn without replacement from a pool of K keys. A small value of K implies that the scheme will have good connectivity, as it increases the probability that two nodes will share a common key, but the resilience is low, as each key is likely to be stored in a significant proportion of the nodes, thus exposure of a key may disrupt a large proportion of network communication. Increasing K improves the resilience, at the cost of decreasing connectivity. Schemes that build on this basic method include [8][19][20][32][39][33].

Combinatorial schemes make use of the properties of combinatorial designs (or related structures such as strongly regular graphs) in a deterministic manner. In these schemes the choice of the underlying combinatorial object determines the final performance of the scheme. For example, in [25] Lee and Stinson propose schemes based on transversal designs, and describe a family of such designs parameterised by quantities m, a prime power, and k where $2 \leq k \leq m$. In their schemes nodes are required to store k keys, and two nodes have a probability $\frac{k}{m+1}$ of sharing a key; such schemes can support m^2 nodes. Increasing the value of m, for instance, would improve the scalability of the scheme, although the connectivity would suffer a corresponding decrease. Other schemes based on combinatorial objects can be found in [3][4][23][24][25]. Closely related are the so-called *hybrid schemes*, in which probabilistic elements are added to an underlying combinatorial structure in order achieve greater flexibility in some of the parameters involved, while hopefully keeping many of the desirable properties of the object in question. Such techniques are used in [3][5][6][7].

Another approach that is frequently employed is the use of *threshold-based techniques*. Keying material is predistributed to subsets of nodes such that any two nodes in a subset can establish a common key, and there is some threshold value t whereby an adversary compromising fewer than t nodes gets no information about keys shared by other nodes, but an adversary compromising t or more nodes can compute all keys shared by nodes within the subset. Such schemes are usually instantiated through the use of matrices [15] or polynomials [10][11][12][27][29][31][30]. Probabilistic techniques are frequently used to decide the subsets to which each node belongs (essentially the key pool is replaced by a pool of matrices/polynomials). Having higher thresholds, or using a greater number of subsets will increase the resilience of a scheme, but will require greater node storage.

The category of 2-complete schemes without location control can thus be said to be well understood, at least in the pairwise case, in that a range of solutions are available for a variety of parameter choices. Less is known about t-wise communication structures, although in some cases these will form straightforward generalisations.

4.2 Locally 2-complete schemes

In [28] Liu and Ning describe a *Closest-Pairwise scheme* for a locally 2-complete communication structure. In this scheme each node is preloaded with distinct pairwise keys shared with the c nodes that are expected to be closest to it after deployment. The fact that keys are only ever shared between two users implies, however, that the number of local nodes with which a given node can communicate securely is limited directly by the number of keys it can store.

4.3 Regionally 2-complete schemes

The regionally 2-complete schemes appearing in the literature are extensions of either probabilistic schemes ([14][21][9][18]) or threshold-based schemes ([10][11][12][38]). In the probabilistic case, separate key pools are used for distinct (although possibly overlapping) regions, and nodes are assigned keys from the pools of each region in which they are contained. Similarly, in the threshold case there is a particular matrix/polynomial associated with each region, and nodes receive keying material corresponding to the regions in which they lie. These schemes differ predominantly in their choice of regions; for instance, in [10,11,12] the regions are based on the cells of a hexagonal grid, whereas in [38] they are based on a triangular grid and in the polynomial-based scheme of [28] a square grid is employed.

4.4 Hierarchical schemes

The scheme of Traynor *et al.* [35] can be regarded as a hierarchical version of the probabilistic schemes discussed above. In this case the nodes store varying numbers of keys from the key pool according to their level in the hierarchy.

4.5 Future directions

The above classification of the schemes appearing in the literature suggests four areas for further work that emerge from this review:

(i) In many applications there is a degree of control over sensor location. Knowledge of the network topology and location of sensors is likely to be exploitable in the design of key establishment schemes that are more efficient than those defined for the default scenario. Relatively little research has been done on such schemes. In the case of schemes with partial control over sensor location, attention has focused mainly on providing regionally 2-complete solutions, in the cases where nodes are distributed uniformly [18,10,11,12,38] or the node location is based around a square grid [15]. This leaves open the problem of finding efficient solutions for other network topologies.

(ii) The majority of applications have no apparent need for a pairwise ideal communication structure. A significant number of applications involved a mobile sink communicating with individual sensors. When there is no control of sensor location then designing schemes for pairwise ideal communication structures seems the only option. However, since applications of this type only really

need local communication between sensors in order to securely relay information, partial control over sensor location should lead to more efficient schemes. There is thus considerable scope for the design of new locally complete schemes.

(iii) Most of the literature dealing with key management in heterogeneous sensor networks relies on the presence of a base station that can communicate directly with sensors *e.g.* [36,22]. It would be interesting, however, to see more solutions in the case of a network that has sensors of differing capabilities without access to a base station, as in [35]. In particular there is a lack of solutions in the case of a hierarchical networks with partial knowledge of sensor location.

(iv) Most schemes in the literature propose solutions for static sensor deployment. Intriguingly a significant number of the applications of deployed schemes in [34] involve mobile sensors, for which few dedicated schemes have been designed.

5 Conclusion

There is no single, precise, definition of a wireless sensor network. As a result this term is applied to a wide family of networking environments that support a range of applications. This ambiguity has important implications for the design of key establishment schemes.

We have proposed a simple framework that can be used to define and compare key establishment schemes for wireless sensor networks. In particular this framework is designed to isolate the important categories that make a key establishment scheme suitable for a particular type of sensor network. Our consideration of existing schemes with respect to this framework suggests that much of the current research has a focus that does not necessarily match application requirements. In particular, the default scenario of static, homogeneous sensors whose deployment location is completely uncontrolled does not apply as widely as suggested. As a result we have identified the need for further investigation of key establishment schemes under slightly different assumptions.

References

[1] Ross Anderson, Haowen Chan, and Adrian Perrig. Key infection: Smart trust for smart dust. In *ICNP '04: Proceedings of the Network Protocols, 12th IEEE International Conference on (ICNP'04)*, pages 206–215, Washington, DC, USA, 2004. IEEE Computer Society.

[2] Seyit A. Çamtepe and Bülent Yener. Key distribution mechanisms for wireless sensor networks: a survey. Technical Report TR-05-07, Rensselaer Polytechnic Institute, March 2005.

[3] Seyit Ahmet Çamtepe and Bülent Yener. Combinatorial design of key distribution mechanisms for wireless sensor networks. In *ESORICS*, pages 293–308, 2004.

[4] Seyit Ahmet Çamtepe, Bülent Yener, and Moti Yung. Expander graph based key distribution mechanisms in wireless sensor networks. In *ICC '06, IEEE International Conference onCommunications*, volume 5, pages 2262–2267, 2006.

[5] Dibyendu Chakrabarti, Subhamoy Maitra, and Bimal Roy. Clique size in sensor networks with key pre-distribution based on transversal design. In *IWDC*, pages 329–337, 2005.

[6] Dibyendu Chakrabarti, Subhamoy Maitra, and Bimal K. Roy. A hybrid design of key pre-distribution scheme for wireless sensor networks. In *ICISS*, pages 228–238, 2005.

[7] Dibyendu Chakrabarti, Subhamoy Maitra, and Bimal K. Roy. A key pre-distribution scheme for wireless sensor networks: Merging blocks in combinatorial design. In *ISC*, pages 89–103, 2005.

[8] Haowen Chan, Adrian Perrig, and Dawn Song. Random key predistribution schemes for sensor networks. In *SP '03: Proceedings of the 2003 IEEE Symposium on Security and Privacy*, page 197, Washington, DC, USA, 2003. IEEE Computer Society.

[9] Siu-Ping Chan, Radha Poovendran, and Ming-Ting Sun. A key management scheme in distributed sensor networks using attack probabilities. In *IEEE GLOBECOM '05*, volume 2, 2005.

[10] Farshid Delgosha and Faramarz Fekri. Key pre-distribution in wireless sensor networks using multivariate polynomials. In *IEEE Commun. Soc. Conf. Sensor and Ad Hoc Commun. and Networks - SECON05*, 2005.

[11] Farshid Delgosha and Faramarz Fekri. Multivariate key-establishment schemes for wireless sensor networks. submitted to IEEE Trans. Mobile Comput., 2005.

[12] Farshid Delgosha and Faramarz Fekri. Threshold key-establishment in distributed sensor networks using a multivariate scheme. In *Infocom 2006*, 2006.

[13] Jing Deng, Carl Hartung, Richard Han, and Shivakant Mishra. A practical study of transitory master key establishment forwireless sensor networks. *securecomm*, 0:289–302, 2005.

[14] Wenliang Du, Jing Deng, Yunghsiang S. Han, Shigang Chen, and Pramod K. Varshney. A key management scheme for wireless sensor networks using deployment knowledge. In *INFOCOM*, 2004.

[15] Wenliang Du, Jing Deng, Yunghsiang S. Han, and Pramod K. Varshney. A pairwise key pre-distribution scheme for wireless sensor networks. In *CCS '03: Proceedings of the 10th ACM conference on Computer and communications security*, pages 42–51, New York, NY, USA, 2003. ACM Press.

[16] B. Dutertre, S. Cheung, and J. Levy. Lightweight key management in wireless sensor networks by leveraging initial trust. Technical Report SRI-SDL-04-02, System Design Laboratory, April 2004.

[17] Laurent Eschenauer and Virgil D. Gligor. A key-management scheme for distributed sensor networks. In *CCS '02: Proceedings of the 9th ACM conference on Computer and communications security*, pages 41–47, New York, NY, USA, 2002. ACM Press.

[18] Dijiang Huang, Manish Mehta, Deep Medhi, and Lein Harn. Location-aware key management scheme for wireless sensor networks. In *SASN '04: Proceedings of the 2nd ACM workshop on Security of ad hoc and sensor networks*, pages 29–42, New York, NY, USA, 2004. ACM Press.

[19] David Hwang, Bo-Cheng Lai, and Ingrid Verbauwhede. Energy-memory-security tradeoffs in distributed sensor networks. In *ADHOC-NOW*, pages 70–81, 2004.

[20] Joengmin Hwang and Yongdae Kim. Revisiting random key pre-distribution schemes for wireless sensor networks. In *SASN*, pages 43–52, 2004.

[21] Takashi Ito, Hidenori Ohta, Nori Matsuda, and Takeshi Yoneda. A key pre-distribution scheme for secure sensor networks using probability density function of node deployment. In *SASN '05: Proceedings of the 3rd ACM workshop on Security of ad hoc and sensor networks*, pages 69–75, New York, NY, USA, 2005. ACM Press.

[22] Yee Wei Law, Ricardo Corin, Sandro Etalle, and Pieter H. Hartel. A formally verified decentralized key management architecture for wireless sensor networks. In *PWC*, pages 27–39, 2003.

[23] J. Lee and D. Stinson. A combinatorial approach to key predistribution for distributed sensor networks. IEEE Wireless Communications and Networking Conference, CD-ROM, 2005, paper PHY53-06, 6 pp, 2005.

[24] Jooyoung Lee and Douglas R. Stinson. Deterministic key predistribution schemes for distributed sensor networks. In *Selected Areas in Cryptography*, pages 294–307, 2004.

[25] Jooyoung Lee and Douglas R. Stinson. On the construction of practical key predistribution schemes for distributed sensor networks using combinatorial designs. Technical Report CACR 2005-05, Centre for Applied Cryptographic Research, University of Waterloo, November 2005.

[26] Donggang Liu and Peng Ning. Efficient distribution of key chain commitments for broadcast authentication in distributed sensor networks. In *NDSS*, 2003.

[27] Donggang Liu and Peng Ning. Establishing pairwise keys in distributed sensor networks. In *CCS '03: Proceedings of the 10th ACM conference on Computer and communications security*, pages 52–61, New York, NY, USA, 2003. ACM Press.

[28] Donggang Liu and Peng Ning. Location-based pairwise key establishments for static sensor networks. In *SASN*, pages 72–82, 2003.

[29] Donggang Liu, Peng Ning, and Rongfang Li. Establishing pairwise keys in distributed sensor networks. *ACM Trans. Inf. Syst. Secur.*, 8(1):41–77, 2005.

[30] Abedelaziz Mohaisen, YoungJae Maeng, and DaeHun Nyang. On grid-based key pre-distribution: Twoard a better connectivity in wireless sensor network. In *SSDU-07*, 2007.

[31] Abedelaziz Mohaisen and DaeHun Nyang. Hierarchical grid-based pairwise key predistribution scheme for wireless sensor networks. In *EWSN*, pages 83–98, 2006.

[32] Roberto Di Pietro, Luigi V. Mancini, and Alessandro Mei. Random key-assignment for secure wireless sensor networks. In *SASN '03: Proceedings of the 1st ACM workshop on Security of ad hoc and sensor networks*, pages 62–71, New York, NY, USA, 2003. ACM Press.

[33] M. Ramkumar and N. Memon. An efficient key predistribution scheme for ad hoc network security. *IEEE Journal on Selected Areas in Communications*, 23:611–621, 2005.

[34] Kay Römer and Friedemann Mattern. The design space of wireless sensor networks. *IEEE Wireless Communications Magazine*, 11(6):54–61, 2004.

[35] Patrick Traynor, Heesook Choi, Guohong Cao, Sencun Zhu, and Thomas F. La Porta. Establishing pair-wise keys in heterogeneous sensor networks. Technical Report NAS-TR-0001-2004, Network and Security Research Center, Department of Computer Science and Engineering, Pennsylvania State University, University Park, PA, USA, December 2004. Updated July 6, 2005.

[36] Jeffery Undercoffer, Sasikanth Avancha, Anupam Joshi, and John Pinkston. Security for sensor networks. CADIP Research Symposium, 2002.

[37] Johann Van Der Merwe, Dawoud Dawoud, and Stephen McDonald. A survey on peer-to-peer key management for mobile ad hoc networks. *ACM Comput. Surv.*, 39(1):1, 2007.

[38] Yun Zhou, Yanchao Zhang, and Yuguang Fang. Key establishment in sensor networks based on triangle grid deployment model. In *MILCOM 2005, IEEE Military Communications Conference*, 2005.

[39] Sencun Zhu, Shouhuai Xu, Sanjeev Setia, and Sushil Jajodia. Establishing pairwise keys for secure communication in ad hoc networks: A probabilistic approach. In *ICNP*, pages 326–335, 2003.