Key Establishment Schemes against Storage-Bounded Adversaries in Wireless Sensor Networks

Shi-Chun Tsai, Wen-Guey Tzeng, and Kun-Yi Zhou

***Abstract*—In this paper we re-examine the attacking scenario about wireless sensor networks. It is generally assumed that the adversary picks up all radio communications of sensor nodes without any loss and stores the eavesdropped messages for later use. We suggest that in some situations the adversary may not be able to pick up all radio communications of sensor nodes. Therefore, we propose the storage-bounded adversary model for wireless sensor networks, in which the adversary's storage is bounded.**

We propose two key establishment schemes for establishing shared keys for neighboring sensor nodes in the storage-bounded adversary model. The first scheme needs special beacon nodes for broadcasting random bits. In the second scheme, some sensor nodes play the role of beacon nodes. Our results are theoretical in some sense. Nevertheless, we can adjust them for realistic consideration.

***Index Terms*—Bounded-storage model, key establishment, unconditional security, wireless sensor network.**

I. Introduction

A WIRELESS sensor network usually consists of a large number of small autonomous sensor nodes. Each sensor node has some level of computing power, a limited size of storage, a set of sensors for exploring the environment and a small antenna for communicating with the outside world. One way of deploying a wireless sensor network is to scatter senor nodes in the field randomly. Then, these sensor nodes form a network autonomously via their built-in programs. Due to restriction of small antenna, each sensor node can communicate with its geographic neighbors only. We say that two sensor nodes are *neighbored* if they can communicate with each other via radio directly. In some situations, we may deploy a set of special nodes, called *beacon nodes*, for broadcasting instructions and data to the sensor nodes. A beacon node is more powerful so that its radio signal could cover a larger area.

There are some security issues about wireless sensor networks, such as, communication security, message authentication, node authentication, etc. We are concerned about the key establishment problem, which is to establish a shared (secret) key for two neighboring sensor nodes via the public radio link. The established key is later used for secure communication (encryption) or authentication. The key establishment problem for wireless sensor networks has been studied actively. In this paper we re-examine the attacking scenario about wireless sensor networks. It is generally assumed that the adversary picks up all radio communications of sensor nodes without any loss and stores the eavesdropped messages for later use. We suggest that this may not be the case. For example, the radio quality of a sensor node is not very good and its coverage area is small. It is hard for the adversary to get all communications between sensor nodes. Therefore, we propose the *storage-bounded adversary* model for wireless sensor networks to capture the essence of *incomplete eavesdropping*. In this model, the adversary cannot eavesdrop all communications of the sensor nodes. We could conceptually think that the adversary's storage is limited so that it cannot store all communications. The storage-bounded adversary model has been studied in the cryptographic field for its advanced view. It explores the possibility of encryption in the era of quantum computation. We bring the model to wireless sensor networks for exploring an alternative adversary model.

By considering the storage-bounded adversary, we propose two key establishment schemes. The first scheme needs some special beacon nodes for broadcasting random bits. In the second scheme, some sensor nodes play the role of beacon nodes. Our results are theoretical in some sense. Nevertheless, we can adjust them for realistic consideration.

Our key establishment schemes have the following properties. Firstly, they do not pre-load secrets to sensor nodes. This saves quite a lot of setup work before sensor nodes are deployed to the field. Secondly, the connectivity rate of neighboring sensor nodes is very high and the probability of repeated keys is very low. Thirdly, even if the adversary captures a large fraction of the deployed sensor nodes, almost all of the shared keys of un-compromised links remain secure. We note that most key pre-distribution schemes allow only a small fraction of sensor nodes to be compromised by the adversary. Finally, the shared keys in the first scheme are unconditionally secure. Furthermore, since all shared keys are generated in the field without pre-loaded secrets in sensor nodes, shared keys can be updated from time to time.

We do not consider the adversary that applies other types of attacks, such as node impersonation, node replication, etc. There have been many proposed countermeasures [5]–[7]. If we need them, we can simply use them without too much effort.

Related work. Maurer [8] first proposed the storage-bounded adversary model. Cachin and Maurer [2] proposed a complete solution for encryption under the storage-bounded adversary model.

For key pre-distribution, Blom [1] proposed a scheme for

Manuscript received August 6, 2008; revised October 2, 2008; accepted November 8, 2008. The associate editor coordinating the review of this paper and approving it for publication was D. Wu.

The authors are with the Computer Science Department, National Chiao Tung University, Hsinchu, Taiwan 30050 (e-mail: {sctsai, wgtzeng, kyzhou}@cs.nctu.edu.tw). Corresponding author: W.-G. Tzeng.

This research was supported in part by projects NSC-96-2628-E-009-011-MY3, NSC-97-2221-E-009-064-MY3 NSC-97-2219-E-009-006 (TWISC), and MoE-97W803.

Digital Object Identifier 10.1109/TWC.2009.081048

multiple parties to establish pairwise keys. Eschenauer and Gligor [6] proposed to assign a random subset of the key space to each sensor node. They showed that two neighboring nodes can establish a shared key from their own key pools with a reasonable probability. Chan, et al. [3], Du, et al. [5], and Liu and Ning [7] improved the basic random key pre-distribution scheme of Eschenauer and Gilgor by using multiple random key pools for each sensor node. Ren, et al. [12] discussed how to pre-distribute keys in large scale.

Miller and Vaidya [9] proposed a key pre-distribution scheme by assuming that the communication channels between sensor nodes use the orthogonal frequency-division multiplexing technology. They considered that these channels cannot be eavesdropped all together. Thus, each sensor node broadcasts its pre-loaded secrets to its neighboring nodes through these channels randomly. Due to the characteristics of the channels, only a part of broadcasted secrets are obtained by the adversary. Then, two neighboring sensor nodes can use the uncompromised secrets to establish their shared key. The essence of their assumption is similar to *incomplete eavesdropping*. But, they used it in designing a key pre-distribution scheme. Our schemes are not key pre-distributed. Furthermore, our analysis technique is quite different.

II. Preliminaries

We assume that the sensor nodes are scattered to the field randomly. Each sensor node has no post-deployment knowledge about the other sensor nodes. All it can do is to use its antenna to communicate with its neighboring sensor nodes.

The adversary can eavesdrop all communications of sensor nodes. But, due to storage limitation it can store only a fraction of the eavesdropped messages. After that, the adversary compromises a fraction of the sensor nodes (compromised sensor nodes) and gets the secrets inside them. Then, the adversary tries to infer the shared key held by two neighboring sensor nodes that are not compromised.

Our first key establishment scheme is called *Key Establishment with Beacons in the Storage-Bounded Model*, denoted as KeB-Sb. The beacon nodes are deployed like the sensor nodes, but with a much less number. Each beacon node broadcasts random bits that are received by the sensor nodes within its radio range. Then, two neighboring sensor nodes use the received bits to establish their shared key.

The second key establishment scheme is called *Key Establishment in the Storage-Bounded Model*, denoted as Ke-Sb. Ke-Sb needs no beacon nodes. Each sensor node can play the role of a beacon node. Unlike KeB-Sb, a sensor node that broadcasts random bits establishes shared keys with its neighboring sensor nodes.

The used parameters and notations of the schemes are shown in Table I.

In our analysis, we use a Chernoff bound to derive a closed form for approximating security probabilities [11]. Let X_i be identical and independent Boolean random variables with expectation $E(X_i) = \theta$, $1 \le i \le t$. Then, almost all values of $\sum_{i=1}^{t} X_i$ are around its mean $E(\sum_{i=1}^{t} X_i) = t\theta$, that is, for any $0 < \epsilon \le 1$,

$$\Pr[\sum_{i=1}^{t} X_i \ge (1+\epsilon)t\theta] \le e^{-t\theta\epsilon^2/3}.$$

TABLE I
The used parameters and notations.

- n: the number of deployed sensor nodes in a wireless sensor network. Assume that the sensor node set is $\{V_1, V_2, \ldots, V_n\}$.
- α: the number of broadcasted random bits by a beacon node.
- β: the number of stored bits, with respect to each beacon or beaming node, by the adversary.
- γ: the number of broadcasted random bits by a beaming node.
- κ: the length of the shared keys established among neighboring sensor nodes. Typically, κ is 128-bit long.
- $\mu = 2\sqrt{\kappa\alpha}$: the number of randomly stored bits of a sensor node for each beacon node in the KeB-Sb scheme.
- $K_{i,j}$: the shared key computed by sensor node V_i for its neighbor V_j within a bacon or beaming node.
- $p_{complete}$: the probability of forming a complete network.
- H: a cryptographic hash function with κ-bit output.
- G: a pseudorandom generator that stretches a short random bit string to a very long pseudorandom bit string.
- $|S|$: the number of elements in set S.
- $a \ll b$: a is much smaller than b.

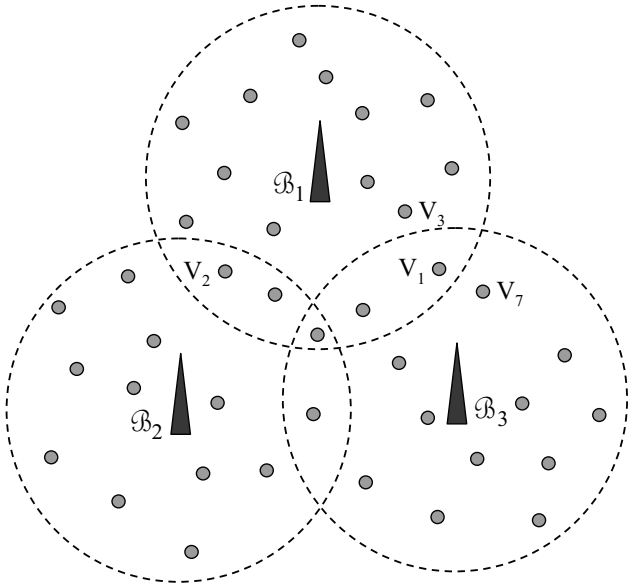

Fig. 1. Deployment of sensor and beacon nodes in a field. Each beacon node uses a different frequency to broadcast random bits and each sensor receives and stores some of them.

III. Scheme: KeB-Sb

Assume that the field deployment of sensor and beacon nodes is like that in Figure 1, in which a dot is a sensor node and a triangle is a beacon node. We assume that there are z beacon nodes $\mathcal{B}_1, \mathcal{B}_2, \ldots, \mathcal{B}_z$. We shall determine an appropriate z later. Without loss of generality, we only present steps for beacon node $\mathcal{B}_1$ and sensor nodes $V_1, V_2, \ldots, V_m$ within its radio range. The adversary gets a fraction δ of the broadcasted random bits of $\mathcal{B}_1$.

The Scheme. The sensor nodes within $\mathcal{B}_1$ use the steps in Figure 2 to establish their shared keys. Those within other beacon nodes do the same thing. The idea is that $\mathcal{B}_1$ broadcasts

1) $\mathcal{B}_1$ generates and broadcasts α random bits on the fly.
2) Each V_i, $1 \leq i \leq m$, randomly stores μ bits $r_{i_1} r_{i_2} \cdots r_{i_\mu}$. Let $S_i = \{i_1, i_2, \ldots, i_\mu\}$.
3) Each V_i, $1 \leq i \leq m$, does the following:
   a) Exchange S_i with each of its neighbors V_j via their direct radio link;
   b) Let $S_{i,j} = S_i \cap S_j = \{s_1, s_2, \ldots, s_l\}$. If $|S_{i,j}| = l \geq \kappa$, compute $K_{i,j} = H(r_{s_1} r_{s_2} \cdots r_{s_l})$.
   c) Erase the stored bits $r_{i_1} r_{i_2} \cdots r_{i_\mu}$ from its memory.

Fig. 2. KEB-SB: Steps of establishing shared keys between neighboring sensor nodes within the radio range of the beacon node $\mathcal{B}_1$.

α random bits and each sensor node randomly stores μ bits. Then, two neighboring sensor nodes exchange the indices of their stored bits and find their common bits. Finally, they compute the shared key from the common bits by taking the hash value of the common bits. It is easy to check that $K_{i,j} = K_{j,i}$ since V_i and V_j found their common bits from the publicly exchanged indices.

It is critical that some sensor nodes V lie within the radio coverage areas of many beacon nodes, say, $\mathcal{B}_1, \mathcal{B}_2, \ldots, \mathcal{B}_\tau$. Assume that $\mathcal{B}_i$'s use different frequencies for broadcasting so that they won't interfere with each other. In this case, V establishes shared keys with its neighboring sensor nodes within various beacon nodes $\mathcal{B}_k$, $1 \leq k \leq \tau$. Thus, a network that connects all sensor nodes can be formed. For example, the sensor node V_1 has a shared key $K_{1,3}$ with V_3 within $\mathcal{B}_1$ and a shared key $K_{1,7}$ with V_7 within $\mathcal{B}_3$. V_1 plays as a connecting node between the sensor nodes within $\mathcal{B}_1$ and the sensor nodes within $\mathcal{B}_3$.

Probability of Establishing Shared Keys. In the scheme each sensor node within a beacon node stores $\mu = 2\sqrt{\kappa\alpha}$ broadcasted bits randomly. Two neighboring sensor nodes within a beacon node will have 4κ common bits on average. Furthermore, the probability that two neighboring sensor nodes have at least κ common bits is $1 - e^{-\kappa/4}$ at least. For $\kappa = 128$, $1 - e^{-\kappa/4} \approx 1$. The following lemma shows this fact, where S and T are the sets of indices of stored bits by two neighboring sensor nodes, respectively.

Lemma 1 ([4]): If S and T are randomly chosen from the $2\sqrt{\kappa\alpha}$-element subsets over $\{1, 2, \ldots, \alpha\}$, then, for sufficiently large α,

$$\Pr_{S,T}[|S \cap T| < \kappa] < e^{-\kappa/4}.$$

Security of Shared Keys. Assume that the adversary stores $\beta = \delta\alpha$ bits of the broadcasted α bits, where $\delta < 1$ is a constant. The security of shared keys depends on δ and κ. Two neighboring sensor nodes within a beacon node have $l = 4\kappa$ common bits on average and the adversary gets a fraction δl of them on average. Although the number l of common stored bits is a random variable, we take the average $l = 4\kappa$ for simplifying analysis. We show that the probability that the adversary gets up to $(\delta + \epsilon)l$ common bits is very low, where $\delta + \epsilon < 1$.

Let $A \subset \{1, 2, \ldots, \alpha\}$ be the set of indices of the stored bits by the adversary, $|A| = \beta$, and B the set of indices of the commonly stored bits by two neighboring sensor nodes, $|B| = l$. We fix A first. The probability that the adversary stores $(\delta + \epsilon)l$ common bits is, for $\delta + \epsilon < 1$ and integer $l(\delta + \epsilon)$,

$$\Pr_B[|A \cap B| \geq (\delta + \epsilon)l] = \sum_{i=(\delta+\epsilon)l}^{l} \frac{\binom{\beta}{i}\binom{\alpha-\beta}{l-i}}{\binom{\alpha}{l}}.$$

It is hard to derive a closed form for the above equation. Nevertheless, we can compute a pretty tight upper bound. In the above computation the elements in B are randomly chosen one by one from $\{1, 2, \ldots, \alpha\}$ *without replacement*. However, if α is much larger than l, we can think that the elements are randomly chosen one by one *with replacement*. Let B' be a multi-set with l elements randomly chosen one by one from $\{1, 2, \ldots, \alpha\}$ *with replacement*. Since α is indeed much large than l in our schemes, we can safely say that

$$\Pr_B[|A \cap B| \geq (\delta + \epsilon)l] \approx \Pr_{B'}[|A \cap B'| \geq (\delta + \epsilon)l],$$

which is bounded by the following lemma.

Lemma 2: Let A be a fixed subset of $\{1, 2, \ldots, \alpha\}$ with $|A| = \beta$ and B', $|B'| = l \ll \beta$, a multi-subset randomly chosen from $\{1, 2, \ldots, \alpha\}$ with replacement. It holds that

$$\Pr_{B'}[|A \cap B'| \geq (\delta + \epsilon)l] \leq e^{-l\epsilon^2/(3\delta)}.$$

Proof: Let X_i be the indicator random variable for whether the ith chosen element of B' is in A, $1 \leq i \leq l$. We have $|A \cap B'| = \sum_{i=1}^{l} X_i$ and $E(\sum_{i=1}^{l} X_i) = \delta l$. Since X_i's are independent, by the Chernoff bound, we have

$$\begin{aligned}\Pr_{B'}[|A \cap B'| \geq (\delta + \epsilon)l] &= \Pr[\sum_{i=1}^{l} X_i \geq (\delta + \epsilon)l] \\ &= \Pr[\sum_{i=1}^{l} X_i \geq \delta l(1 + \epsilon/\delta)] \leq e^{-\delta l(\epsilon/\delta)^2/3} \\ &= e^{-l\epsilon^2/(3\delta)}.\end{aligned}$$

■

Since the above holds for any fixed A, the probability holds no matter how the adversary stores broadcasted bits. For $\kappa = 128$, $\delta = 2/3$, $\epsilon = 1/4$, we have

$$\Pr_{B'}[|A \cap B'| \geq (11/12)l] < e^{-16}.$$

In this case, the adversary does not know at least $(1-\delta-\epsilon)l \approx 43$ common bits of two neighboring sensor nodes within a beacon node.

Probability of Complete Connectivity. We now compute the number of beacon nodes that are needed for high $p_{complete}$. The most important factor for $p_{complete}$ is the size of the overlapping area of radio coverage since the sensor nodes within the overlapping area connect sensor nodes within different beacon nodes. Let R be the radius of the field and r be the radius of the radio coverage of a beacon node. Recall that there are z beacon nodes. We take a very conservative and ideal estimate for the required z. Here, we assume that each overlapping area is shared by three beacon nodes. For each beacon node, the overlapping area of coverage is at least

$$(\pi r^2 z - \pi R^2)/2z,$$

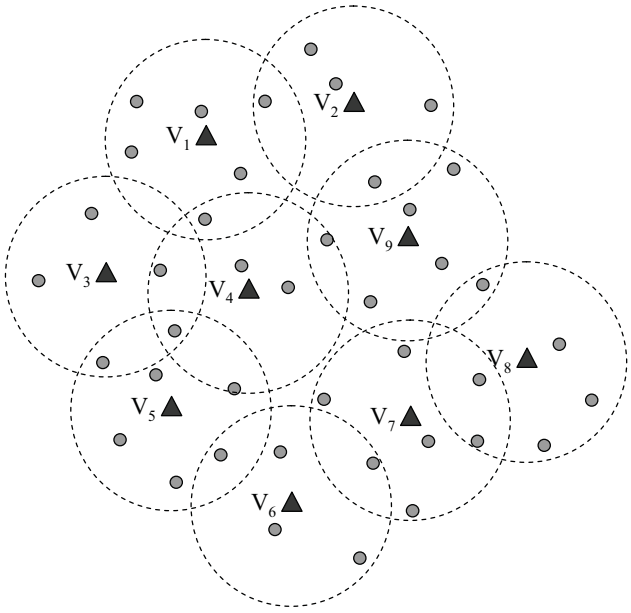

Fig. 3. Deployment of sensor nodes in a field. Some sensor nodes become beaming nodes for broadcasting random bits.

where $r^2z - R^2 > 0$. If we want the number of sensor nodes within the overlapping area of a beacon node to be at least c, we need

$$\frac{n}{\pi R^2}\left(\frac{\pi r^2 z - \pi R^2}{2z}\right) \geq c,$$

which implies

$$z \geq \frac{nR^2}{nr^2 - 2cR^2} \tag{1}$$

With these c connecting sensor nodes within each beacon node, the probability that the sensor nodes within the beacon node are isolated from the whole network is at most $(2e^{-\kappa/4})^c$.

There are n/z sensor nodes within each beacon node on average. The probability that any one of them fails to connect to another sensor node is at most $(n/z)e^{-\kappa/4}$. Since there are z beacon nodes, the probability $p_{complete}$ that all sensor nodes are connected is at least

$$1 - z((n/z)e^{-\kappa/4} + (2e^{-\kappa/4})^c),$$

which is very close to 1 for a relatively large n, say, $n = 1000$.

Our analysis is based on idealistic assumptions, such as a good frequency management and the coverage of the random deployment is reasonably well. For practical consideration, please see, e.g., [10].

IV. Scheme: Ke-Sb

In the situation that no beacon nodes exist, we let some sensor nodes play the role of broadcasting random bits. We call these sensor nodes as *beaming nodes*. Assume that each sensor node becomes a beaming node with probability p independently, where p will be determined later. The choice of p is to have enough beaming nodes to cover the whole field. A field deployment is shown in Figure 3, in which V_1 to V_9, denoted as triangles, are the beaming nodes. Note that since a beaming node uses a seed to generate pseudorandom bits, the adversary's computing power should be polynomial-time bounded, instead of unboundedness.

- Each V_i, $1 \leq i \leq n$, randomly acts a beaming node with probability p. Without loss of generality, let $V_1, V_2, \ldots, V_\tau$ be the beaming nodes and $V_{\tau+1}, V_{\tau+2}, \ldots, V_n$ be the non-beaming sensor nodes.

1) Each beaming node $V_j, 1 \leq j \leq \tau$, generates a secret seed s_j randomly and broadcasts γ pseudorandom bits $G(s_j) = r_{j,1}r_{j,2}\cdots r_{j,\gamma}$.
2) Each non-beaming sensor node $V_i, \tau+1 \leq i \leq n$, does the following. Assume that V_i is within radio range of beaming nodes $V_1, V_2, \ldots, V_\rho$, wlog.
   a) Randomly store 4κ bits $r_{j,j_1}r_{j,j_2}\cdots r_{j,j_{4\kappa}}$ from each $V_j, 1 \leq j \leq \rho$. Let $S_{i,j} = \{(j,j_1),(j,j_2),\ldots,(j,j_{4\kappa})\}$, $1 \leq j \leq \rho$.
   b) Send $S_{i,j}$ to V_j, $1 \leq j \leq \rho$.
   c) Compute the shared key $K_{i,j} = H(r_{j,j_1}r_{j,j_2}\cdots r_{j,j_{4\kappa}})$ with V_j, $1 \leq j \leq \rho$.
3) Each beaming node V_j, $1 \leq j \leq \tau$, computes the shared key $K_{j,i} = H(r_{j,j_1}r_{j,j_2}\cdots r_{j,j_{4\kappa}})$ by $S_{i,j}$ with each of its *neighboring* sensor nodes V_i, where $r_{j,j_1}r_{j,j_2}\cdots r_{j,j_{4\kappa}}$ is re-computed from its random seed s_j.
4) Each beaming node V_j erases its random seed s_j from its memory, $1 \leq j \leq \tau$.

Fig. 4. Ke-Sb: Steps of establishing shared keys between beaming nodes and their neighboring sensor nodes.

The Scheme. The Ke-Sb scheme is shown in Figure 4. A beaming node V_j broadcasts γ pseudorandom bits $G(s_j) = r_{j,1}r_{j,2}\ldots r_{j,\gamma}$ and each sensor node V_i within its radio range stores 4κ bits of them randomly. Then, the sensor node V_i sends the indices $(j,j_1),(j,j_2),\ldots,(j,j_{4\kappa})$ of the stored bits to V_j and computes the shared key $K_{i,j}$ which is the hash value of its stored bits. V_j computes the stored bits of V_i from the random seed s_j and the shared key $K_{j,i}$ in the same way. It is necessary that a beaming node uses a pseudorandom generator to generate pseudorandom bits since these pseudorandom bits are used later for computing shared keys with its neighboring sensor nodes.

Security of Shared Keys. The security analysis of a shared key is the same as that of the KeB-Sb scheme. Recall that an adversary has a storage of β bits. By Lemma 2, the probability that the adversary gets $l(\delta+\epsilon)$ of the stored bits of a sensor node is less than

$$e^{-4\kappa\epsilon^2\gamma/(3\beta)}.$$

Density of Beaming Nodes. The larger p is, the higher $p_{complete}$ is. Nevertheless, we want to have a smaller p so that the expected number np of beaming nodes is as small as possible. Assume that r is the radius of radio range of a beaming node and R is the radius of the deployment field. Note that this r is smaller than that of a beacon node in the KeB-Sb scheme. The expected number of beaming nodes is np, which is equivalent to z, the number beacon nodes. By

Equation (1), we need

$$z = np \geq \frac{nR^2}{nr^2 - 2cR^2},$$

where c is the expected number of connecting nodes in the overlapping area of two beaming nodes. Thus, we have

$$p \geq \frac{R^2}{nr^2 - 2cR^2}.$$

V. Discussion

Our schemes are designed on an abstract model of wireless sensor networks. Many details are omitted. Comparison between the conventional and storage-bounded adversary model is uncalled-for since their basic assumptions are fundamentally different. Even though our schemes are theoretical, we can use some techniques to improve their performance on energy consumption, storage requirement and computation cost.

1) No re-send: It is possible that a sensor node does not receive some random bits from beacon or beaming nodes. The sensor node can simply ignore a lost bit and continues to wait for the next one. This does not affect its functionality since only a very small fraction of broadcasted bits are stored by each sensor node. Thus, the beacon and beaming nodes can broadcast in a "raw" mode.
2) Sleeping: In our schemes, random bits are broadcasted for a relatively long period of time. But, the sensor nodes do not store all of them. Thus, the sensor nodes can use the random sleeping technique to reduce energy consumption. Each sensor node stays in a state of very low energy consumption for most time and wakes up to receive bits from time to time.
   Furthermore, when a sensor node needs to receive broadcasted random bits from different beacon or beaming nodes in different frequencies, it can switch to a different frequency in each wake-up. Thus, the beacon or beaming nodes can broadcast random bits at different frequencies without worrying about whether their neighboring sensor nodes can receive them simultaneously.
3) Pseudorandomness: In our schemes, all kinds of nodes need some random bits. Beacon and beaming nodes need to generate random bits for broadcasting and sensor nodes need to generate random indices for picking up broadcasted random bits. In fact, pseudorandom bits can replace random bits for better efficiency. A node can sample a short random seed s from the environment and uses the pseudorandom bit generator G to generate pseudorandom bits $G(s)$.
   It should be noted that if we use pseudorandom bits in the scheme, the storage-bounded adversary should be polynomial-time bounded also, instead of computing-unboundedness. This is because a computing-unlimited adversary can search the seed by the eavesdropped pseudorandom bits and the pseudorandom generator G.

In reality, an adversary may jam the media to block the process of key establishment. It is hard for wireless communications to resist this kind of denial of service attacks. Due to sensor nodes' low hardware profile, it is not practical for them to receive the random bits from a satellite. In the above we only discuss how to establish shared keys for the sensor nodes that are within the radio range of beacon and beaming nodes. For others that are neighbored can establish direct link through the path-key finding process.

VI. Conclusions

We have introduced the storage-bounded adversary model to wireless sensor networks and proposed two key establishment schemes in this model. We are interested in improving efficiency of the schemes for practicability in the future. We are also interested in proposing different kinds of security schemes for wireless sensor networks in this model.

References

[1] R. Blom, "An optimal clas of symmetric key generation systems," in *Proc. EUROCRYPT 84*, pp. 335–338, 1984.
[2] C. Cachin and U. M. Maurer, "Unconditional security against memory-bounded adversaries," in *Proc. CRYPTO 97*, pp. 292–306, 1997.
[3] H. Chan, A. Perrig, and D. Song, "Random key predistribution for sensor networks," in *Proc. IEEE Symposium on Security and Privacy 03*, pp. 197–213, 2003.
[4] Y. Z. Ding, "Oblivious transfer in the bounded storage model," in *Proc. CRYPTO 01*, pp. 155–170, 2001.
[5] W. Du, J. Deng, Y. S. Han, and P. Varshney, "A pairwise key predistribution scheme for wireless sensor networks," in *Proc. ACM CCS 03*, pp. 42–51, 2003.
[6] L. Eschenauer and V. D. Gilgor, "A key-mamnagement scheme for distributed sensor networks, in *Proc. ACM CCS 02*, pp. 41–47, 2002.
[7] D. Liu and P. Ning, "Eatablishing pairwise keys in distributed sensor networks," in *Proc. ACM CCS 03*, pp. 52–61, 2003.
[8] U. M. Maurer, "Conditionally-perfect secrecy and a provably-secure randomized cipher." *J. Cryptology*, vol. 5, no. 1, pp. 53–66, 1992.
[9] M. J. Miller and N. H. Vaidya, "Leveraging channel diversity for key establishment in wireless sensor networks," in *Proc. IEEE INFOCOM 06*, pp. 1–12, 2006
[10] S. Meguerdichian, F. Koushanfar, M. Potkonjak, and B. Srivastava, "Coverage problems in wireless ad-hoc sensor networks," in *Proc. IEEE INFOCOM 01*, pp. 1380–1387, 2001.
[11] M. Mitzenmacher and E. Upfal, *Probability and Computing: Randomized Algorithms and Probabilistic Analysis*. Cambridge University Press, 2005.
[12] K. Ren, K. Zeng, and W. Lou, "A new approach for random key predistribution in large scale wireless sensor networks," *Wireless Commun. and Mobile Computing*, vol. 6, no. 3, pp. 307–318, 2006.