Key Forwarding : A Location-Adaptive Key-Establishment Scheme for Wireless Sensor Networks

Ashok Kumar Das, Abhijit Das
{akdas,abhij}@cse.iitkgp.ernet.in
Surjyakanta Mohapatra
surjyakanta@gmail.com
Srihari Vavilapalli
hvpalli@yahoo.com

Department of Computer Science and Engineering
Indian Institute of Technology, Kharagpur 721 302, India

Abstract. In this paper we propose an improved alternative for the path key establishment phase of bootstrapping in a sensor network. Our scheme lets the network adapt to the deployment configuration by secure transmission of predistributed keys. This results in better connectivity than what path key establishment can yield. The communication overhead for our scheme is comparable with that for path key establishment. Moreover, the assurance of good connectivity allows one to start with bigger key pools, thereby improving resilience against node capture.

1 Introduction

Sensor networks are widely deployed in a variety of applications ranging from military to environmental and medical research. Chiefly for military applications, data collected by sensor nodes need be encrypted before transmission. Due to resource limitations in sensor nodes, it is not feasible to use public key routines. A symmetric cipher (like DES, RC5, IDEA, or AES) is the only viable option for encryption or decryption of secret data. However, setting up symmetric keys among communicating nodes continues to remain a challenge. Pairwise key establishment between neighboring sensor nodes in a sensor network is done by using a protocol which is popularly known as the *bootstrapping* protocol. A bootstrapping protocol involves several steps. In the key-predistribution phase, each sensor node is loaded with a set of pre-distributed keys. This is done before the deployment of the sensor nodes in a target field. After deployment, a direct key establishment (shared key discovery) phase is performed by the sensor nodes in order to establish direct pairwise keys between them. Path key establishment phase is an optional stage and, if executed, adds to the connectivity of the network. When two physical neighbors fail to establish a direct key during the shared key discovery phase, they attempt to find out a secure path to transmit a new pairwise key.

Key predistribution in sensor networks has received considerable research attention in recent years [1–6]. Eschenauer and Gligor [1] proposed the first basic random key predistribution called the EG scheme. Chan et al. [2] proposed several modifications of the EG scheme. Liu and Ning's polynomial-pool based key predistribution scheme [3] and the matrix-based key predistribution proposed by Du et al. [5] improve security considerably.

In this paper, we propose a modification of the existing bootstrapping framework. We introduce the concept of *key forwarding* as an alternative to the path key establishment phase. Our technique yields better connectivity at a cost comparable to (if not better than) that associated with path key establishment, and does not degrade the security of the network.

2 Location-adaptive key forwarding scheme

The deployment topology of a sensor network cannot usually be determined before the actual deployment of the nodes. If, however, an approximate deployment configuration is known a priori, a host of modifications can be incorporated in the key predistribution schemes so as to achieve substantially improved connectivity and high resilience against node captures. Such *location aware* schemes [4, 5] lose their performance enhancements as the error between the actual and the expected deployment locations of the sensor nodes increases. For sufficiently large errors, a location aware scheme essentially degrades to a random scheme without a priori knowledge of deployment configuration.

A *location adaptive* scheme, on the other hand, may or may not start with prior knowledge of the deployment configuration, but adapts to the geography of deployment, thereby improving local connectivity in the sensor network. The path key establishment phase is a location adaptive feature in the bootstrapping process. We propose an alternative to the path key establishment scheme, namely the *key forwarding scheme*, which leads to considerably better connectivity than the path key establishment scheme. Our scheme works on any geographic distribution of sensor nodes in the deployment area.

The key forwarding scheme is motivated by the following consideration. Consider the basic scheme (EG scheme) with each node capable of storing m (say 200) keys. Assume also that each node has at most d (for example, 100) physical neighbors. Even when a node is connected securely to all of these neighbors, at least $(m - d)$ keys remain unused in the node. Loading a key ring with more keys than the neighborhood size is necessitated by the desire to achieve decent local connectivity. Now imagine a situation where a node v is in the physical neighborhood of two other nodes u and w. Suppose that u and v share a predistributed key and so also do u and w, but not v and w. The nodes u and w may or may not be in the physical communication ranges of one another. The node u then forwards the key k shared between u and w to node v. Since u and v have a secure link between them, k can be forwarded securely. Once v receives k, a secure link between v and w is established by using either k or any other pairwise key set up using this key k. Each round of the key forwarding phase involves the following steps:

Algorithm KeyForwarding

```
1. for each node $v$ in the network:
2.   for each physical neighbor $w$ of $v$ with which $v$ does not share a key:
3.     $v$ broadcasts a request whether any of its neighbors shares a key with $w$
4.     if a neighbor $u$ of $v$ responds affirmatively and if $u$ and $v$ share a key,
5.       then $u$ securely forwards to $v$ a key $k$ shared between $u$ and $w$.
6.         $v$ generates a new pairwise key $k'$, encrypts $k'$ with $k$, and sends the
           encrypted key and the id of $u$ to $w$.
7.         $w$ retrieves $k'$ by decrypting using $k$.
8.         both $v$ and $w$ record $k'$ for future communication between them.
9.         $v$ deletes $k$ from its memory, if $k$ happens to occupy large space (like
           polynomial shares).
```

The above steps are to be carried out after the shared key discovery phase and can be repeated multiple times. In order to reduce communication overhead, the number of rounds of the key forwarding stage may be restricted to 2 or 3.

The security of the key forwarding stage is based on the assumption that bootstrapping is done securely, i.e., no nodes are captured during the initial key establishment phase. Incidentally, this is the assumption inherent in the path key establishment phase too.

Here we shall analyze our scheme applied only to the EG scheme [1] and the poly-pool scheme [3].

2.1 Network connectivity of key forwarding under the EG scheme

Let M be size of the key-pool, m the number of keys pre-distributed in each node, and p the probability that two physical neighbors share one or more keys in their key rings. It is easy to deduce (see [1]) that $p = 1 - \prod_{i=0}^{m-1} \frac{M-m-i}{M-i}$. Let us now calculate the theoretical probability p_r that a secure link exists between two physical neighbors v and w after r rounds of key forwarding. Let d denote the (average) physical neighborhood size of each node. After the direct key establishment phase, we have: $p_0 = p$.

For the derivation of p_1, let us take two physical neighbors v and w that do not share a key. A new pairwise key is established between v and w if there exists a neighbor u of v sharing a key with both v and w. The probability that a physical neighbor u of v has this property is p^2. So the probability that neither of the d neighbors of v can help to establish a secure v-w link is $(1-p^2)^d$. Thus among the $(1-p)d$ neighbors of v with whom v does not share a key, about $d(1-p)(1-p^2)^d$ links remain insecure. We then have $p_1 = 1-(1-p)(1-p^2)^d$. This analysis can be repeatedly generalized as: $p_r = 1-(1-p_{r-1})(1-pp_{r-1})^d$ for all $r \geq 1$.

The probabilities p_r are plotted in Figure 1 for $M = 100000, m = 100$ (so that $p = 0.0953$) and for several values of d. From the figure, it is clear that when the average number of neighbors increases, the connectivity also increases.

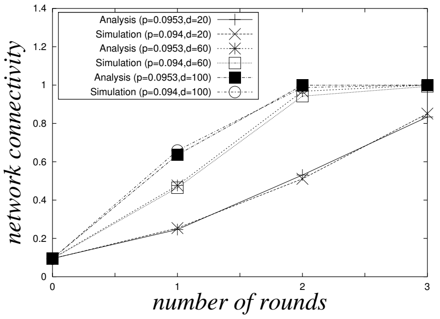

Fig. 1. Analysis and simulation of network connectivity for key forwarding under the EG scheme ($n = 10000$, $d = 20, 40, 60, 80, 100$, $M = 100000$, $m = 100$).

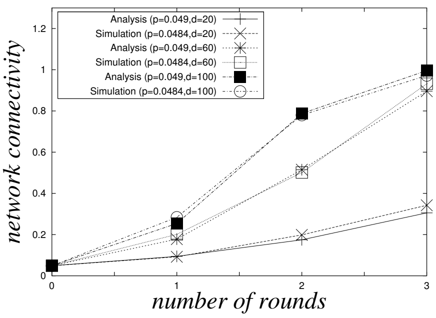

Fig. 2. Analysis and simulation of network connectivity for key forwarding under the poly-pool scheme ($n = 10000$, $d = 20, 40, 60, 80, 100$, $s = 500$, $s' = 5$).

This is expected, since the probability that two unconnected nodes v and w can establish a pairwise key between them increases with the number of nodes that can help in this process. The figure also illustrates that one obtains high network connectivity after two rounds of key forwarding.

2.2 Network connectivity of key forwarding under the poly-pool scheme

Let s be the polynomial pool size, and s' the number of polynomial shares given to each node. Analogous to the EG scheme, the local connectivity p can be computed as (see [3]) $p = 1 - \prod_{i=0}^{s'-1} \frac{s-s'-i}{s-i}$.

The probability p_r of two sensor nodes sharing a key after r rounds of key forwarding can be derived analogously as before and can be given by the equations: $p_0 = p$, $p_1 = 1 - (1-p)(1-p^2)^d$, $p_r = 1 - (1-p_{r-1})(1-pp_{r-1})^d$ for all $r \geq 1$.

For $s = 500$ and $s' = 5$, we have $p = 0.0492$, that is, the network is likely to remain disconnected with high probability after shared key discovery. From Figure 2, it is clear that after executing two to three rounds of key forwarding we expect to achieve high network connectivity.

3 Simulation results

3.1 Connectivity measurement

For the EG scheme, we have taken the parameters $n = 10000$, $M = 100000$, $m = 100$, $d = 20, 40, 60, 80, 100$. The theoretical and simulated connectivity probabilities are plotted in Figure 1. For the poly-pool scheme, we have considered the parameters: $s = 500$, $s' = 5$, $n = 10000$, $d = 20, 40, 60, 80, 100$. The theoretical and simulated probabilities are plotted in Figure 2. In Figures 3 and 4

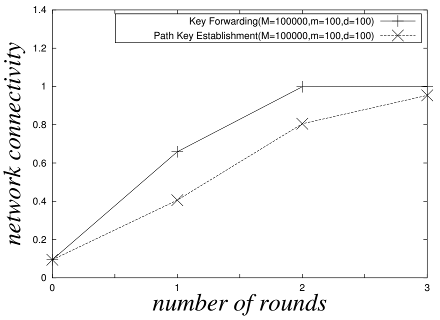

Fig. 3. Comparison of connectivity between key forwarding and path key establishment under the EG scheme ($n = 10000$, $d = 100$, $M = 100000$, $m = 100$).

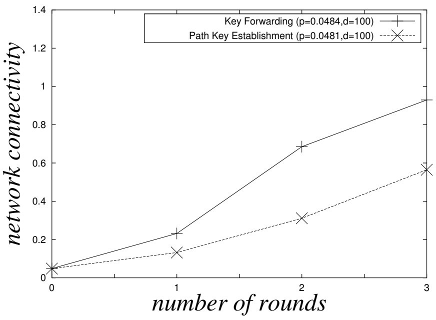

Fig. 4. Comparison of connectivity between key forwarding and path key establishment under the poly-pool scheme ($n = 10000$, $d = 100$, $s = 500$, $s' = 5$).

we compare simulated connectivity between key forwarding and path key establishment. Key forwarding is found to clearly outperform path key establishment, particularly for the poly-pool scheme. In fact, key forwarding may render an initially disconnected network connected, whereas path key establishment can never achieve this.

3.2 Resilience measurement

Following conventional practice, we measure the resilience of the network against node capture by the fraction of compromised links among uncaptured nodes and express this resilience as a function of the number of nodes captured. We assume that bootstrapping is done securely, i.e., no nodes are captured during bootstrapping. If the adversary also does not intercept any transmission during bootstrapping, the resilience of the network against node capture becomes the same as that of the original EG or poly-pool scheme under the given parameters. Since considerable connectivity is guaranteed by key forwarding, we can start with parameters leading to extremely high resilience.

So we assume now that an eavesdropper does not capture any node during bootstrapping but records every transaction made during bootstrapping. Later the eavesdropper manages to capture some nodes. The record of bootstrapping transactions reveals to the eavesdropper the following secret information: (i) All the pairwise keys resulting from the initial key predistribution based on captured keys or polynomial shares, (ii) All the pairwise keys established using forwarded keys or polynomial shares that are captured, (iii) For the poly-pool scheme, if more than t shares of a polynomial f are captured, any pairwise key established using any share of f during both shared key discovery and key forwarding.

Simulation results for resilience measurement under the EG scheme are shown in Figure 5 for various parameter values. Results for resilience measurement under the poly-pool scheme are shown in Figure 6 for various parameter values.

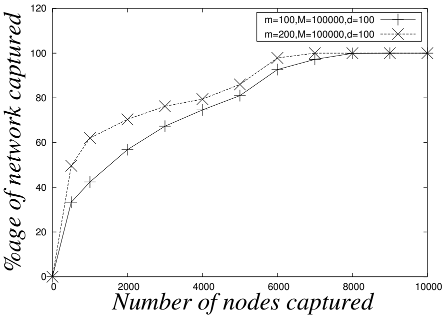

Fig. 5. Resilience measurement of key forwarding under the EG scheme ($m = 100$, 200, $M = 100000$, $n = 10000$, $d = 100$).

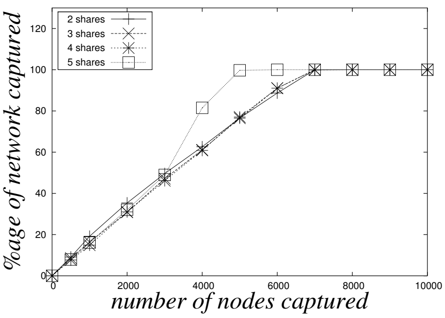

Fig. 6. Resilience measurement of key forwarding under the poly-pool scheme ($n = 10000$, $d = 100$, $s = 500$, $s' = 2, 3, 4, 5$).

4 Conclusion

In this paper, we have proposed an alternative to the path key establishment phase of bootstrapping in a sensor network. Our scheme offers markedly better connectivity compared to path key establishment. We have corroborated this claim both theoretically and by running simulations. Better connectivity lets one start with bigger networks and/or bigger pool sizes, both leading to better resilience against node captures. The extra communication overhead incurred by key forwarding is comparable with, if not better than, that associated with path key establishment.

References

1. Eschenauer, L., Gligor, V.D.: A key management scheme for distributed sensor networks. In: 9th ACM Conference on Computer and Communication Security. (2002) 41–47
2. Chan, H., Perrig, A., Song, D.: Random key predistribution for sensor networks. In: IEEE Symposium on Security and Privacy, Berkely, California (2003) 197–213
3. Liu, D., Ning, P.: Establishing pairwise keys in distributed sensor networks. In: Proceedings of 10th ACM Conference on Computer and Communications Security (CCS), Washington DC (2003) 52–61
4. Liu, D., Ning, P.: Location-based pairwise key estalishments for static sensor networks. In: ACM Workshop on Security in Ad Hoc and Sensor Networks (SASN '03). (2003)
5. Du, W., Deng, J., Han, Y.S., Chen, S., Varshney, P.K.: A key management scheme for wireless sensor networks using deployment knowledge. In: 23rd Conference of the IEEE Communications Society (Infocom'04), Hong Kong, China (2004)
6. Du, W., Deng, J., Han, Y.S., Varshney, P.K.: A pairwise key pre-distribution scheme for wireless sensor networks. In: ACM Conference on Computer and Communications Security (CCS'03), Washington DC, USA (2003) 42–51