Mission-guided Key Management for Ad Hoc Sensor Network

Shaobin Cai, Xiaozong Yang and Jing Zhao

Harbin Institute of Technology, Department of Computer, Mail-box 320 Harbin Institute of Technology, Harbin, China, 150001
Phone: 86-451-6414093
csb@ftcl.hit.edu.cn

Abstract. Ad hoc Sensor Networks (ASNs) are ad-hoc mobile networks that consist of sensor nodes with limited computation and communication capabilities. Because ASNs may be deployed in hostile areas, where communication is monitored and nodes are subject to be captured by an adversary, ASNs need a cryptographic protection of communications and sensor-capture detection. According to that the ASN is deployed to carry out some certain tasks, we present a mission-guided key-management scheme. In our scheme, a key ring, which consisting of randomly chosen k keys from a sub-pool of a large offline-generated pool of P keys, is pre-distributed to each sensor node of a group. Compared with Laurent's scheme, our scheme improves the probability that a shared key exists between two sensor nodes of the same group, and doesn't affect its security.

Keyword Ad hoc Sensor Networks, Security, Key Management, Mission-guarded

1. Introduction

The last decade of last century has seen the advances in micro-electro-mechanical systems (MEMS) technology, wireless communications, and digital electronics have enabled ad hoc sensor networks (ASN) to monitor the physical world. When they are deployed in the hostile environments, their open architectures make potential intruder easy to intercept, eavesdrop and fake messages. Therefore, the ASN need strong security services.

Although some significant progress has been made in many aspects of ASN, which include topology management, routing algorithms, data link protocol and sensor data management [1], very little work is done on the security of ASN. Since proposals addressing security in general ad hoc networks [2][3][4] aren't suitable for ASN, the research into authentication and confidentiality mechanisms designed specifically for ASN is needed.

Most of the security mechanisms require the use of some kind of cryptographic keys that need to be shared between the communicating parties. The purpose of key management is to [5]: Initialize system users within a domain; Generate, distribute and install keying material; Control the use of keying material; Update, revoke and destroy keying material; Store, backup, recover and archive keying material. Key management is an unsolved problem in ASN.

The hardware resources of the sensor are so scarce that it is impractical for it to use typical asymmetric (public-key) cryptosystems to secure communications. For example, the Smart Dust sensors [6, 7] only have 8Kb of program and 512 bytes for data memory, and processors with 32 8-bit general registers that run at 4 MHz and 3.0V. Carman, Kruus, and Matt [8] report that on a mid-range processor, such as the Motorola MC68328, the energy consumption for a 1024-bit RSA encryption (signature) operation is much higher than that for a 1024-bit AES encryption operation. Hence, symmetric-key ciphers, low-energy, authenticated encryption modes [9, 10, 11], and hash functions become the tools for protecting ASN communications.

In order to reduce the usage of hardware resource, Laurent's scheme [12] distributes a key ring, which consisting of randomly chosen k keys from a large offline-generated pool of P keys, to each sensor node. Although, Lauren's scheme saves some hardware resources, its possibility that there is a secure link between any pair sensor nodes is low. According to that the sensors are deployed to perform certain tasks, we propose a mission-guided key management scheme. In our scheme, the sensors, which are deployed to perform a certain tasks, form a group. The scheme randomly chooses a key sub-pool from the large pool of P keys for the group according to the size of the group. And then, it distributes a ring of keys, which consists of randomly chosen k keys from the sub-pool, to each sensor node off-line. In the sensor network, most communications among sensors are among the sensors, which cooperate to accomplish assigned tasks. Therefore, our mission-guided key management scheme improves probability that a shared key exists between two sensor nodes. By the random graph analysis and simulation, we analyze the performance of both key management schemes.

The rest of the paper is organized as follow. First, we give an overview of our scheme in section 2. Secondly, we setup a mathematic model and analyze its performance in section 3. Thirdly, we analyze its performance by simulations in section 4. Finally, we draw a conclusion in section 5.

2. Overview of Our Scheme

Our scheme modifies Laurent's scheme according to that the actions of the sensor nodes are mission-guided. The difference between our scheme and Laurent's scheme is their key pre-distribution. Their shared-key discovery, path-key establishment, key revocation, re-keying and resiliency to sensor node capture are identical. In this section, we present how the keys are pre-distribute to the sensors according to the mission-guided scheme.

In the Laurent's scheme, a key ring, which consisting of randomly chosen k keys from a large offline-generated pool of P keys, is pre-distributed to each sensor node. According to the usage of ASN, most sensors of the ASN are deployed at the same time and to the same place for a special mission. Therefore, the sensors can be divided into groups for the sub-missions. Since most tasks of the mission are completed by the cooperation of the group members, most communications among sensors are happened among the number of a group. Therefore, our scheme can improve secure connectivity among the sensors, and reduce the path length between any pair of sensor nodes. The key pre-distribution phase of our scheme consists of the following six steps:

1. It first generates a large pool of P keys, which normally has 2^{17} - 2^{20} keys in Laurent's scheme, and their key identifiers offline;
2. It selects P_i ($P_i = \frac{l}{n} \times P$, l is the number of the sensors of the group and n is the number of the sensors of the ASN) keys from the pool to form a sub-pool, $Subpool_i$, for group G_i;
3. It randomly selects k keys from $Subpool_i$ to establish the key ring of a sensor of group G_i;
4. It loads the key ring into the memory of each sensor;
5. Its saves the key identifiers of a key ring and associated sensor identifier on a trusted controller node of the group;
6. It loads the i^{th} controller node with the key shared with the controller.

In the step 6, the key shared by a node with the i^{th} controller node, K^{ci}, can be computed as $K^{ci} = E_{K_x}(ci)$, where $K_x = K_1 \oplus, \ldots, \oplus K_k$, K_i are the keys of the node's key ring, ci is the controller's identity, and E_{K_x} denotes encryption section, with node key K_x. Hence, the keys shared by a node with controllers, which are only infrequently used, need not take any space on the key ring. However, in this case, the K^{ci} changes upon any key change on a ring.

Compared with Laurent's scheme, the advantage of our scheme is that the sensor nodes, which cooperate to accomplish some tasks, get their key ring from a sub-pool. Since the sub-pool is smaller than the pool, the possibility that there is a secure link between any pair sensor nodes of the same group increased. On the other hand, the key selection from the sub-pool doesn't affect randomicity of the key selection. Therefore, this scheme doesn't increase the possibility that an adversary decrypts a key.

3. Analysis

In this section, we compare the probability that a shared key exists between two sensor nodes in Laurent's scheme and our scheme.

In the sensor network, not only the security considerations but also the limits of the wireless communication ranges of sensor nodes preclude that the ASNs are fully connected by shared-key links between all sensor nodes. Therefore, it is impossible for the shared-key discovery phase to guarantee full connectivity for a sensor node with all its neighbors. Let p be the probability that a shared key exists between two sensor nodes, n be the number of network nodes, and $d = p \times (n-1)$ be the expected degree of a node of a fully connected network, in which d is the average number of edges connecting that node with its graph neighbors.

Since the wireless connectivity constraints limit sensor node neighborhoods, the a node has n' ($n' \leq$ n-1) neighbor nodes, which implies that the probability of sharing a key between any two neighbors becomes $p' = \frac{d}{n'} \geq p$. Hence, we set the probability that two nodes share at least one key in their key rings of size k chosen from a given pool of P keys to p', and then derive p' as a function of k. In the derivation, the size of the key pool, P, isn't a sensor-design constraint; the size of the key ring, k, is sensor design constraint.

The probability that two key rings share at least a key is 1 – Pr [two nodes do not share any key]. To compute the probability that two key rings do not share any key, we first compute the number of the possible key rings. Since each key of a key ring is drawn out of a pool of P keys without replacement, the number of possible key rings is:

$$\frac{P!}{k!(P-k)!}$$

After picking out the first key ring, the total number of possible key rings that do not share a key with this key ring is the number of key rings that can be drawn out of the remaining P - k unused key in the pool, namely:

$$\frac{(P-k)!}{k!(P-2k)!}$$

Therefore, the probability that no key is shared between the two rings is the ratio of the number of rings without a match by the total number of rings. Thus, the probability that there is at least a shared key between two key rings is:

$$p' = 1 - \frac{k!(P-k)!}{P!} \times \frac{(P-k)!}{k!(P-2k)!}$$

and thus

$$p' = 1 - \frac{((P-k)!)^2}{(P-2k)!P!}$$

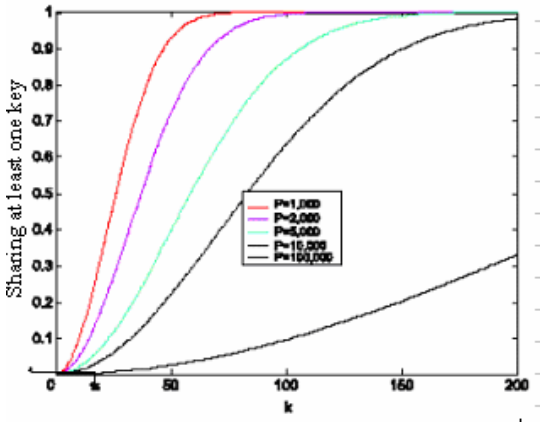

Fig. 1. Probability of sharing at least one key when two nodes choose k keys from a pool of size P (cited from Laurent's scheme)

In order to simplify the analysis of our scheme, we assume that there are only sensor nodes of the same group in the ASN. Therefore, the p' of our scheme between two sensors of the same group, whose sub-pool has P_i keys, is

$$p' = 1 - \frac{((P_i - k)!)^2}{(P_i - 2k)!P_i!}$$

Since P is very large, we use Stirling's approximation for

$$n! \approx \sqrt{2\pi}\ n^{n+\frac{1}{2}}\ e^{-n}$$

to simplify the expression of p', and obtain:

$$p' = 1 - \frac{(1-\frac{k}{P})^{2(P-k+\frac{1}{2})}}{(1-\frac{2k}{P})^{(P-2k+\frac{1}{2})}}$$

Since the size of sub-pool is much smaller than that of pool, the probability that a shared key exists between two sensor nodes of the same group is improved by our scheme. But, our scheme doesn't affect the probability that a shared key exists between two sensor nodes of the different group.

Figure 1 illustrates a plot of this function for various values of P. When a pool size P is 10,000 keys, and 75 keys are distributed to any sensor nodes, Laurent's scheme only makes any two nodes have the probability $p' = 0.5$ that they share a key in their key ring, our scheme can make any two nodes of the same group have the probability $p' \approx 1$ that they share a key in their key ring (we assume that there are 10 groups in the ASN, and each sub-pool has 1,000 keys).

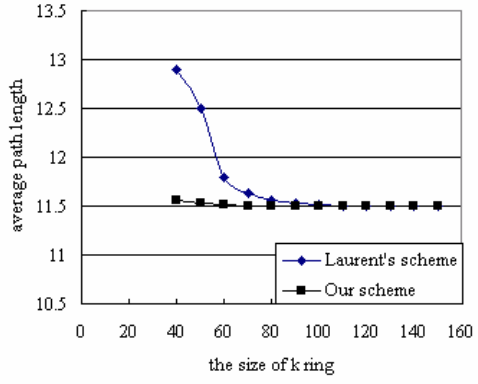

Fig. 2. Average path length at network layer

4. Simulations

We investigate the effect of the various parameters on ASN by the simulations. In our simulations, the ASN is made up of 1,000 nodes, each node averagely has 40 neighbor sensor nodes, and the pool of key has 10,000 keys. In our scheme, the sensor nodes are divided into 10 groups, and the movement of the nodes is guided by mission-guided mobility model. In the mission-guided mobility model, the movements of the nodes have three characters:

1. When a task is assigned to a group, all nodes of the group move to the assigned area at similar speed;
2. When a node of the group arrived at the assigned area, the node move according to the "random waypoint" in the assigned area;
3. When a group finishes its assigned task, it waits a new task in the previous assigned area.

4.1 Effect on the Network Topology

Whether two neighbor nodes share a key during the shared-key discovery phase means that whether a link exists or not between these two nodes from a network routers' point of view. Therefore, the probability that two nodes share a key in their key ring has an effect on the average path length between two nodes after shared-key discovery.

Figure 2 shows the relationship between the path length and the sizes of the key ring. From the figure we can see that the average path length of the network depends on the size of the key ring. The smaller k is, the higher the probability that a link does not have a key and, therefore, the longer paths need to be found between nodes. When k is too small, the network is disconnected. Since, the sensor group is deployed to perform certain tasks, most of them are in an assigned zone, and most

links between two sensor nodes are between two sensor nodes of the same group. From the analysis above, we can know that our scheme improves the probability, which a link has a key, and shortens the average path length.

Because some links may not be keyed, a node may need to use a multi-link path to communicate with one of its wireless neighbors. Although the schemes can encrypt this link by the path key procedure, the long path increases the delay and communication cost to setup a path key with a neighbor.

Figure 3 shows the path length of neighbors when the key ring of sensors has 75 keys. When neighborhood node cannot be reached via a shared key, the node must take at least two links to contact it. Since the structure of the ad hoc sensor network is unstable, a node has to setup the path key with its unreachable neighbors constantly. The effects waste the scare source of ASN. Therefore, if we can improve the probability of two nodes' sharing a key, then we can decrease the usage of path key procedure. In Laurent's scheme, only 45.3% of the neighbors are reachable over a single link, and other 17.8% of the neighbors are reachable over two-link paths. In our scheme, almost 100% of the neighbors of the same group are reachable over a single link. Although, some neighbors of different group aren't reachable over a single link, the 98.7% of the neighbors are reachable over a single link, and other 1.3% of the neighbors are reachable over two-link paths.

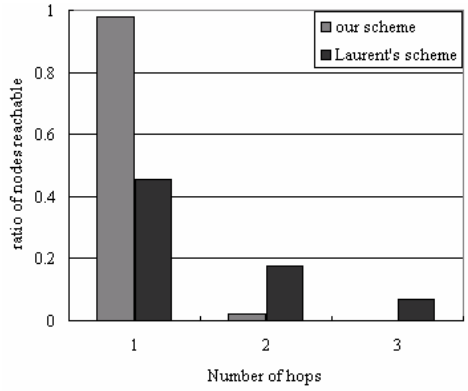

Fig. 3. Path length to neighbors

4.2 Resiliency to Sensor Node Capture

If an adversary captures a node, then they can acquire k keys, and the adversary can attack $\frac{k \times number\ of\ links}{P}$ links. Therefore, how many links are secured with the same key is an important factor that affects the resiliency to sensor node capture. From the simulation results, we can know that the usage of the keys of our scheme is similar with that of Laurent's scheme. Out of the pool of 10,000 keys, only about 50%

of the keys are used to secure links, only about 30% are used to secure one link, about 10% are used to secure two links, and only about 5% are used to secure 3 links. Therefore, the ability of both schemes to stand against the node capture is similar.

5. Conclusions

In this paper, we presented a new mission-guided key management scheme for large scale ASNs. In our scheme, the sensors, which are deployed to perform a certain tasks, form a group. The scheme randomly chose a key sub-pool from the large pool of P keys for the group according to the size of the group, and distributes a ring of keys, which consists of randomly chosen k keys from the sub-pool, to each sensor node off-line. By the analysis and simulations, we compare the difference between our scheme and Laurent's scheme. The results show that our scheme outperforms the Laurent's scheme.

References

1. I. Akyildiz, W. Su, Y. Sankarasubramaniam, E. Cayirci, "A survey on sensor networks", IEEE Commun. Mag. (August) (2002).
2. N. Asokan, P. Ginzboorg, "Key agreement in ad hoc networks", Comp. Commun., 23, pp. 1627 – 1637.
3. L. Zhou, Z.J. Haas, "Securing ad hoc networks", IEEE Networks 13 (6) (1999).
4. J. Kong, P. Zerfos, H. Luo, S. Lu, L. Zhang, "Providing robust and ubiquitous security support for mobile ad-hoc networks", IEEE ICNP (2001).
5. A. Menezes, P. van Oorschot, S. Vanstone, "Handbook of Applied Cryptography", CRC Press, 1997, ISBN 0849385237.
6. J. Hill, R. Szewczyk, A. Woo, S. Hollar, D. Culler, K. Pister, "System architecture directions for network sensors," Proc. of ASPLOS-IX, Cambridge, Mass. 2000.
7. J. M. Kahn, R. H. Katz and K. S. J. Pister, "Mobile Networking for Smart Dust", ACM/IEEE Intl. Conf. on Mobile Computing and Networking (MobiCom 99), Seattle, WA, August 17-19, 1999, pp. 271 - 278.
8. D. W. Carman, P. S. Kruus and B. J. Matt, "Constraints and Approaches for Distributed Sensor Network Security", dated September 1, 2000. NAI Labs Technical Report #00-010, available at http://download.nai.com /products/media/nai/zip/nailabs-report-00-010-final.zip
9. V.D. Gligor and P. Donescu, "Fast Encryption and Authentication: XCBC Encryption and XECB Authentication Modes", Fast Software Encryption 2001, M.Matsui (ed), LNCS 2355, Springer Verlag, April 2001.
10. C.S. Jutla, "Encryption Modes with Almost Free Message Integrity", Advances in Cryptology EUROCRYPT 2001, B. Pfitzmann (ed.), LNCS 2045, Springer Verlag, May 2001.
11. P. Rogaway, M. Bellare, J. Black, and T. Krovetz, "OCB: A Block-Cipher Mode of Operations for Efficient Authenticated Encryption", Proc. of the 8th ACM Conf. on Computer and Communication Security, Philadelphia, Penn., November 2001.
12. Laurent Eschenauer, Virgil D. Gligor "A Key Management Scheme for Distributed Sensor Networks" CCS'02, November 18–22, 2002, Washington, DC, USA.