An Efficient Key Distribution Scheme for Heterogeneous Sensor Networks

Sajid Hussain
Acadia University, Wolfville
Nova Scotia, Canada
sajid.hussain@acadiau.ca

Firdous Kausar and Ashraf Masood
College of Signals
National University of Science and Technology
Rawalpindi, Pakistan
firdous_3679@yahoo.com and
ashrafm@isb.comsat.net

ABSTRACT

Key distribution refers to the problem of establishing shared secrets on sensor nodes such that secret symmetric keys for communication privacy, integrity and authenticity can be generated. In a wireless sensor network, pre-distribution of secret keys is possibly the most practical approach to protect network communications but it is difficult due to the ad hoc nature, intermittent connectivity, and resource limitations of the sensor networks. In this paper, we propose a key distribution scheme based on random key pre-distribution for heterogeneous sensor network (HSN) to achieve better performance and security as compared to homogeneous network which suffer from high communication overhead, computation overhead, and/or high storage requirements. In a key generation process, instead of generating a large pool of random keys, a key pool is represented by a small number of generation keys. For a given generation key and publicly known seed value, a one-way hash function generates a key chain, and these key chains collectively make a key pool. Each sensor node is assigned a small number of randomly selected generation keys. The proposed scheme reduces the storage requirements while maintaining the same security strength.

Categories and Subject Descriptors

C.2.0 [**Computer Systems Organization**]: Computer-Communication Networks—*Security and protection*; D.4.6 [**Software Engineering**]: Security and Protection—*Authentication, Cryptographic controls*

General Terms

Security

Keywords

Key distribution, random key pre-distribution, heterogeneous sensor networks, security

IWCMC'07, August 12–16, 2007, Honolulu, Hawaii, USA.

1. INTRODUCTION

Due to recent advances in electronic industry, wireless sensors can be used in various ubiquitous and pervasive applications such as military, security, health-care[11, 13], industry automation, environmental and habitat monitoring [1, 15]. Wireless sensor networks (WSNs) consist of a large number of low power nodes, with limited processing, communication, and storage resources [2]. Due to limited resources of WSNs, it is challenging to incorporate basic security functions, such as authentication, access control, data integrity, privacy, and key distribution. For instance, asymmetric cryptography such as RSA or Elliptic Curve cryptography (ECC) is unsuitable for most sensor architectures due to high energy consumption and increased code storage requirements. To avoid the use of asymmetric cryptography, several alternative approaches have been developed to perform key management on resource-constrained sensor networks, such as random key pre-distribution schemes, plain text key exchange schemes, and transitory master key schemes.

In WSNs, hierarchical clustering provides scalability, self-organization, and energy efficient data dissemination [23]. A number of cluster formation protocols have been proposed but most existing protocols assume benign environments, and are vulnerable to attacks from malicious nodes.

Most existing research mainly considers homogeneous sensor networks, where all sensor nodes have identical capabilities in terms of communication, computation, sensing, and reliability; however, homogeneous WSNs are not scalable. Several recent works, on the other hand, investigate heterogeneous sensor networks (HSNs). Girod et al. [12] develop tools to support heterogeneous systems, and also to support the measurement and visualization of operational systems. Lazos and Poovendran [16] study the coverage problem in planar heterogeneous sensor networks and formulate the coverage problem as a set intersection problem. They formulated expressions in order to determine the required number of sensors for a field of interest. Ma et al. [18] propose a resource oriented protocol for heterogeneous sensor networks to build the network model that adapts according to the members' resources. Du and Lin [6] propose a differentiated coverage algorithm which can provide different coverage degrees for different areas; the algorithm is energy efficient since it only keeps minimum number of sensors in active state. Duarte-Melo and Liu [9] analyze the energy consumption and lifetime of HSN by providing periodic data from a sensing field to a remote receiver.

Security is very important for sensor networks applications such as military, homeland security, health-care, and industry automation. Secure and scalable WSN applications require efficient key distribution and key management mechanisms. For instance, pre-key distribution scheme is commonly used in WSNs [3], [19] , [10], [4], [24], [21], [5], [22]. In these approaches, with minimal resources, one can achieve a known probability of connectivity within a network. These efforts assume a deployment of homogeneous nodes, and therefore use a balance distribution of random keys among the nodes.

In this paper, however, we propose a key distribution scheme based on random key distribution for heterogeneous sensor networks. The proposed scheme reduces the storage requirements by using generation keys. The rest of paper is organized as follows: Section 2 provides the related work and Section 3 describes the proposed scheme. Section 4 gives the results and performance evaluation. Finally, Section 5 concludes the paper.

2. RELATED WORK

The key management problem is very active research area in WSNs. Eschenauer and Gligor [10] propose a probabilistic key pre-distribution technique to bootstrap the initial trust between sensor nodes. First, each sensor randomly picks a set of keys from a key pool before deployment. Then, in order to establish a pairwise key, two sensor nodes only need to identify the common keys that they share. Chan et al. [3] propose the q-composite key pre-distribution, which allows two sensors to setup a pairwise key only when they share at least q common keys. Chan et al. also developed a random pairwise keys scheme to handle node capture attacks. In [20] Perrig et al. propose SPINS, a security architecture specifically designed for sensor networks. In SPINS, each sensor node shares a secret key with the base station. Two sensor nodes cannot directly establish a secret key. However, they can use the base station as a trusted third party to set up the secret key. Oliveira et al [19] use random key pre-distribution for secure communication in hierarchical (cluster-based) protocols such as LEACH [14].

Du et al.[8] propose the asymmetric pre-distribution (AP) scheme for heterogeneous sensor networks which provides better security with low complexity and significant reduction on storage requirement. Lu et al. [17] propose a framework for key management schemes in distributed wireless sensor networks with heterogeneous sensor nodes.

3. PROPOSED SCHEME

In this section, we present our key distribution scheme designed for heterogeneous sensor networks. We assume an HSN consists of a small number of powerful High-end sensors (H-sensors) and a large number of Low-end sensors (L-sensors). H-sensors are more powerful nodes and have more computation, communication, energy supply and storage capability. L-sensors are ordinary sensor nodes with limited computation, communication, energy supply and storage capability.

We will consider the hierarchical structure of the HSN in which more powerful H-sensors act as cluster heads (CHs). Clustering of sensors enable local data processing, which reduces communication load in the network in order to provide scalable solutions.

A few terms used in the proposed scheme are as follows:

- *Key Pool*: A key pool K is a large pool of random symmetric keys.
- *Key Chain*: A key chain C is a subset of K. Each key chain is generated independently via a unique generation key and publicly known seed S by applying a keyed hash algorithm repeatedly. Publicly known seed value is same for every key chain. Each key chain has its unique ID namely, C_i and $i \in [0, M-1]$. M equal sized key chains in total form a complete key pool.
- *Key Ring*: A key ring R consists of randomly selected generation keys of corresponding key chains. Each sensor node is assigned a ring of R keys.

3.1 Key Pre-Distribution Phase

A key pool K consists of M different key chains:

$$K = C_o|C_1|\ldots|C_{M-1} \quad (1)$$

where $C_i \cap C_j = \phi(\forall i \neq j)$. As a key chain C_i is generated independently via a unique generation key g_i and publicly known seed S by applying a keyed hash algorithm repeatedly [22], the n-th key of the key chain C_i is computed as:

$$k_{C_i,n} = HASH^n(S, g_i) \quad (2)$$

The total number of keys in a key chain is N, where $N = \frac{K}{M}$. Each key in the key chain C_i is given as $C_{i,l}$, where $0 \leq i \leq M-1$ and $0 \leq l \leq N-1$, .

Before deploying the nodes, each node is loaded with its assigned key ring R, where R is the generation knowledge of a number of key chains. The assigning rules are as follows:

- Each L-sensor node is assigned with r randomly selected generation keys of corresponding key chains. From these r generation keys, $r \times N$ random keys can be calculated effectively.
- Each H-sensor node is pre-loaded with S randomly selected generation keys of corresponding key chains, where $S >> r$.

3.2 Cluster Formation Phase

During the cluster formation phase, all H-sensors broadcast Hello messages to nearby L-sensors with some random delay, in order to avoid collisions of Hello messages from neighboring H-sensors. The Hello message includes the ID of the H-sensor. The transmission range of the broadcast is large enough so that most L-sensors can receive Hello messages from several H-sensors. Then each L-sensor selects the H-sensor whose Hello message has the best signal noise ratio (SNR) as the cluster head. Each L-sensor also records other H-sensors from which it receives the Hello messages, and these H-sensors are listed as backup cluster heads in case the primary cluster head fails. The H-sensor acts as a cluster head (CH), and the L-sensors act as cluster members; the details of clustering scheme can be found in [7].

3.3 Cluster head based Shared Key Discovery Phase

The shared key discovery phase begins after cluster formation phase. First, each cluster member sends to its cluster

head a message, which includes its ID, the ids of the generation keys, and its neighboring nodes information. Second, this phase includes a sub-phase of neighborhood discovery, which could include the following: a) all L-sensors broadcast hello messages for a short range in order to discover neighbors, b) alternately, every L-sensor becomes a receiver to obtain the neighborhood information, c) the neighborhood discovery phases ends when all the L-sensors have obtained neighborhood information. Third, CH discovers the shared generation keys between neighboring L-sensors in its cluster.

As shown in Figure 1, in messages 1 and 2, L-sensors A and B send messages to CH, where messages contain their ids, ids of generation keys, and the list of their neighboring L-sensors ids. After discovering shared generation key between each pair of neighboring L-sensors, CH generates a random number n where $[0 \leq n \leq N]$ and disseminates the shared-key information to sensors in its cluster using shared-key messages, as shown in message 3 and 4 of Figure 1. In other words, L-sensors A and B share n-th key of C_m key chain. Further, L-sensors A and B also share the same n-th key of C_m key chain with their CH.

Some L-sensors may not share any pre-loaded generation key with their neighbors. For each pair of L-sensors (say X and Y) that do not share any generation key, CH obtains a shared-key between CH and X and a shared-key between CH and Y. Then, CH generates a pair-wise key for each pair (X and Y), and securely sends the key to them.

Figure 2 shows an example for neighboring L-sensors that do not share common pre-loaded generation key. CH first checks if it has a pre-loaded generation key shared with the L-sensors (e.g., X and Y). As CH is pre-loaded with a large number of generation keys, there is a high probability that CH can find at least one shared generation key with X and Y. CH generates random numbers p and q where $[0 \leq p, q \leq N]$, and send message 3,4, which means that CH share the p-th key of C_i key chain with node X and q-th key of C_j key chain with node Y. CH generates a new shared key between X and Y and sends this key to X and Y, encrypting with shared key between nodes (X,Y) and CH, as shown in messages 5 and 6.

1: $A \Rightarrow CH : (id_A, (id_{g_1}, id_{g_2}, \ldots id_{g_r}), List[neighbors])$
2: $B \Rightarrow CH : (id_B, (id_{g_1}, id_{g_2}, \ldots id_{g_r}), List[neighbors])$
3: $CH \Rightarrow A : (n, id_{g_m}, id_A, id_B)$
4: $CH \Rightarrow B : (n, id_{g_m}, id_A, id_B)$

Figure 1: Neighboring L-sensors with a common pre-loaded generation key.

1: $X \Rightarrow CH : (id_X, (id_{g_1}, id_{g_2}, \ldots id_{g_r}), List[neighbors])$
2: $Y \Rightarrow CH : (id_Y, (id_{g_1}, id_{g_2}, \ldots id_{g_r}), List[neighbors])$
3: $CH \Rightarrow X : (p, id_{g_i}, id_X)$
4: $CH \Rightarrow Y : (q, id_{g_j}, id_Y)$
5: $CH \Rightarrow X : (E_{K_{CH,X}}(K_{X,Y}))$
6: $CH \Rightarrow Y : (E_{K_{CH,Y}}(K_{X,Y}))$

Figure 2: Neighboring L-sensors without a common pre-loaded generation key.

Although in this paper, we have not discussed about the routing and data dissemination techniques, the pair-wise keys established between neighboring nodes can be used for several techniques such as: a) multi-hop tree based routing within a cluster, b) centralized (base station assisted) multi-hop routing techniques, and c) or any flat routing techniques.

4. PERFORMANCE EVALUATION

In this section, the proposed key distribution scheme is compared with other commonly used key distribution techniques. The results show that the proposed scheme can significantly reduce the storage requirements, while providing similar probability of key sharing among nodes.

The key pool size K is a critical parameter because in random key distribution schemes the amount of storage reserved for keys in each node is likely to be a preset constraint, which makes the size of the key ring R a fixed parameter. Once R is set then for larger values of K the probability that two L-nodes will share a key is small. Further the probability that a randomly chosen link is compromised when a node that is at neither end of the compromised link decreases by increasing the value of K . We want to find the largest key pool size K, such that the probability of key sharing between two L-sensors, as well as L-sensor and H-sensor is not less then the threshold p.

Let p be the probability that an L-sensor and H-sensor share at least one common key in their key ring.The number of possible key ring assignment for an L-sensor is

$$\frac{M!}{r!(M-r)!} \tag{3}$$

The number of possible key ring assignment for an H-sensor is

$$\frac{M!}{S!(M-S)!} \tag{4}$$

The total number of possible key ring assignment for an L-sensor and H-sensor is

$$\frac{M!}{r!(M-r)!} \times \frac{M!}{S!(M-S)!} \tag{5}$$

The probability that an L-sensor and H-sensor share a common key can be given as

$$p = 1 - \frac{(M-r)!(M-S)!}{M!(M-r-S)!} \tag{6}$$

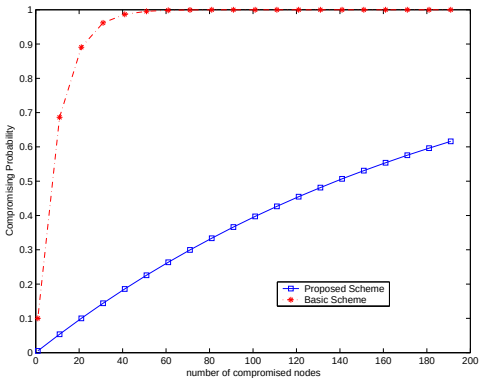

Figure 4: The Compromising Probability

Figure 3 shows probability of key sharing for different schemes. For different values of K, M, S and r we plot

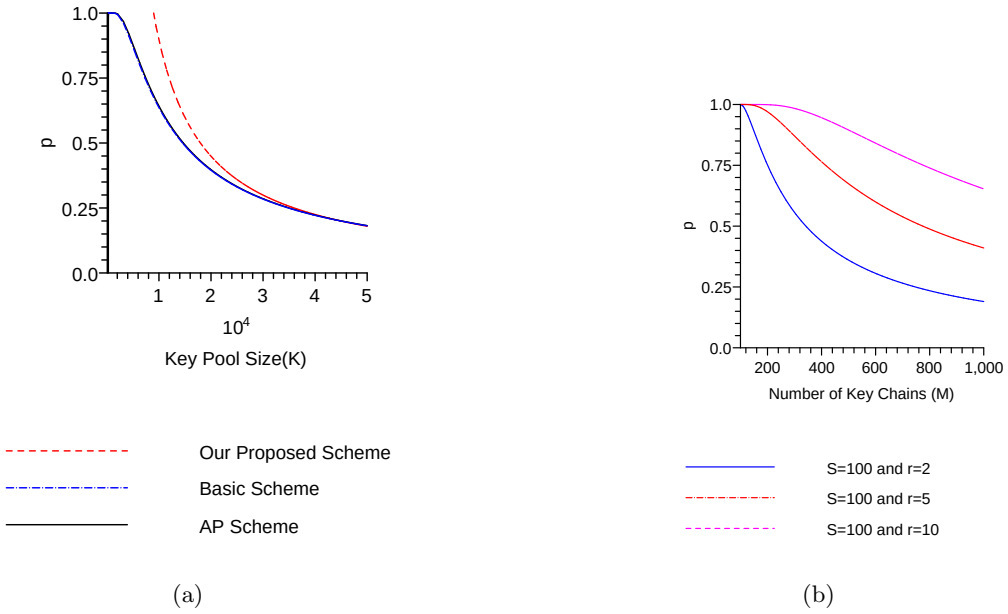

Figure 3: The Probability of Key Sharing

the probability of sharing at least one key, under our proposed scheme, the key pre-distribution scheme [10] which we will refer as basic scheme, and Asymmetric Pre-distribution scheme [8] which we will refer as AP scheme. In Figure 3(a), the key pool size ranges from 1,000 to 50,000 and key ring size is fixed to 100 for basic scheme. For AP scheme, H-sensor keys are 500 and L-sensor keys are 20. For our proposed scheme, the number of key chains (M) varies from 100 to 1000, S=90, and r=2. In other words, the number of key chains (M) is 0.02 times of the corresponding key pool size.

Figure 3(a) shows that for the proposed scheme, the same probability of key sharing among nodes can be achieved by just loading 2 generation keys in sensor node as compared to 100 keys in basic scheme [10] and 20 keys in AP scheme [8]. For instance, if there are 1000 L-sensors and 10 H-sensors in an HSN, where each L-sensor is pre-loaded with 2 generation keys and each H-sensor is pre-loaded with 100 generation keys, the total memory requirement for our proposed scheme is 2×1000+100×10=3000 (in the unit of key length). However, in AP scheme [8], if each H-sensor is loaded with 500 keys and each L-sensor is loaded with 10 keys, the total memory requirement for storing these keys will be 500×10+1000×20=25,000, which is 8 times larger than our proposed scheme.

Further, for a homogeneous sensor network with 1000 L-sensors, where each L-sensor is pre-loaded with 100 keys, the memory requirements will be 100×1000=100,000, which is 33 times larger than our proposed scheme.

Figure 3(b) shows that the probability of key sharing among nodes and CH increases by a very little increase in the number of pre-loaded generation keys in L-sensors. For instance, if pre-loaded keys are increased from 2 to 5, the key sharing probability increases from 0.5 to 0.8 approximately, for 400 key chains.

4.1 Security Evaluation

In this section, we investigate the security resilience of our proposed scheme against node compromise attack. Further, we calculate the expected number of compromised links due to key revealing of captured nodes.

Each L-sensor has a knowledge of $r \times N$ keys. The probability that a given key does not belongs to an L-sensor is $1 - \frac{r}{M}$. If there are n compromised nodes, the probability that a given key is not compromised is $(1 - \frac{r}{M})^n$. The probability of total number of compromised keys, where n number of L-sensors are captured, is as follows:

$$\overline{p} = 1 - \left(1 - \frac{r}{M}\right)^n \tag{7}$$

Figure 4 shows the compromising probability with respect to the number of compromised nodes. For the given parameters: M=1000, K=50,000, r=5, and m=100, the results show that when the compromised communication is 100 percent in basic scheme, the proposed scheme has compromised communication of only 12 percent (approximately).

5. CONCLUSION

In this paper, we propose a key distribution scheme for heterogeneous sensor networks based on random key pre-distribution. In our scheme, instead of storing all the assigned keys in a sensor node, we store a small number of generation keys. The results show that our scheme can significantly reduce the storage requirements as compared to other random key pre-distribution schemes. For instance, storage requirements can be reduced by 8 times as compared to AP [8], and 33 times as compared to basic scheme [10].

6. REFERENCES

[1] I. F. Akyildiz, W. Su, Y. Sankarasubramaniam, and E. Cayirci. A survey on sensor networks. *IEEE Communications Magazine*, August 2002.

[2] D. W. Carman, P. S. Kruus, and B. J. Matt. Constrains and approaches for distributed sensor network security. In *Technical report, NAI Labs*, 2000.

[3] H. Chan, A. Perrig, and D. Song. Random key pre-distribution schemes for sensor networks. In *IEEE Symposium on Security and Privacy*, pages 197–213, May 2003.

[4] H. Chan, A. Perrig, and D. Song. Random key pre-distribution schemes for sensor networkss. In *IEEE Symposium on Research in Security and Privacy*, 2003.

[5] Y. Cheng and D. P. Agrawal. Efficient pairwise key establishment and management in static wireless sensor networks. In *Second IEEE International Conference on Mobile ad hoc and Sensor Systems*, 2005.

[6] X. Du and F. Lin. Maintaining differentiated coverage in heterogeneous sensor networks. *EURASIP Journal on Wireless Communications and Networking*, (4):565–572, 2005.

[7] X. Du and Y. Xiao. Energy efficient chessboard clustering and routing in heterogeneous sensor network. *International Journal of Wireless and Mobile Computing*, 1(2):121–130, 2006.

[8] X. Du, Y. Xiao, M. Guizani, and H.-H. Chen. An effective key management scheme for heterogeneous sensor networks. *Ad Hoc Networks*, 5(1):24–34, 2007.

[9] E. J. Duarte-Melo and M. Liu. Analysis of energy consumption and lifetime of heterogeneous wireless sensor networks. In *Proceedings of IEEE Globecom*, 2002.

[10] L. Eschenauer and V. D. Gligor. A key management scheme for distributed sensor networks. In *ACM CCS 2002*, 2002.

[11] T. Gao, D. Greenspan, M. Welsh, R. R. Juang, and A. Alm. Vital signs monitoring and patient tracking over a wireless network. In *The 27th Annual International Conference of the IEEE EMBS*, Shanghai, China, September 2005.

[12] L. Girod, T. Stathopoulos, N. Ramanathan, J. Elson, D. Estrin, E. Osterweil, and T. Schoellhammer. A system for simulation, emulation, and deployment of heterogeneous sensor networks. In *2nd international conference on Embedded networked sensor systems*, 2004.

[13] L. Gu, D. Jia, P. Vicaire, T. Yan, L. Luo, A. Tirumala, Q. Cao, T. He, J. A. Stankovic, T. Abdelzaher, and B. H. Krogh. Lightweight detection and classification for wireless sensor networks in realistic environments. In *The 3rd ACM Conference on Embedded Networked Sensor Systems*, San Diego, USA, November 2005.

[14] W. R. Heinzelman, A. Chandrakasan, and H. Balakrishnan. Energy-efficient communication protocol for wireless microsensor networks. In *IEEE Hawaii Int. Conf. on System Sciences*, pages 4–7, 2000.

[15] J. Kahn, R. Katz, and K. Pister. Next century challenges: Mobile networking for smart dust. In *The ACM International Conference on Mobile Computing and Networking (MobiCom'99)*, Seattle, USA, August 1999.

[16] L. Lazos and R. Poovendran. Stochastic coverage in heterogeneous sensor networks. *ACM Transactions on Sensor Networks (TOSN)*, 2(3):325–358, August 2006.

[17] K. Lu, Y. Qian, and J. Hu. A framework for distributed key management schemes in heterogeneous wireless sensor networks. In *IEEE International Performance Computing and Communications Conference*, pages 513–519, 2006.

[18] Y. Ma, S. Dala1, M. Alwan, and J. Aylor. Rop: A resource oriented protocol for heterogeneous sensor networks. In *Virginia Tech Symposium on Wireless Personal Communications*, 2003.

[19] L. B. Oliveira, H. C. Wong, M. Bern, R. Dahab, and A. A. F. Loureiro. Sec leach: A random key distribution solution for securing clustered sensor networks. In *5th IEEE international symposium on network computing and applications*, pages 145–154, 2006.

[20] A. Perrig, R. Szewczyk, J. Tygar, Victorwen, and D. E. Culler. Spins: Security protocols for sensor networks. In *Seventh Annual Int'l Conf. on Mobile Computing and Networks*, July 2001.

[21] R. D. Pietro, L. V. Mancini, and A. Mei. Random key assignment secure wireless sensor networks. In *1st ACM workshop on Security of Ad Hoc and Sensor Networks*, 2003.

[22] K. Ren, K. Zeng, and W. Lou. A new approach for random key pre-distribution in large-scale wireless sensor networks. *Wireless communication and mobile computing*, 6(3):307–318, 2006.

[23] F. Zhao and L. Guibas. Wireless sensor networks. *Elsevier Inc*, pages 23–24, 2004.

[24] S. Zhu, S. Xu, S. Setia, and S. Jajodia. Establishing pairwise keys for secure communication in ad hoc networks: A probabilistic approach. In *11th IEEE International Conference on Network Protocols (ICNP'03)*, 2003.