Volume 3, Issue 7, July 2013 ISSN: 2277 128X

International Journal of Advanced Research in Computer Science and Software Engineering

Research Paper

Available online at: www.ijarcsse.com

A Novel Deterministic Key Pre Distribution Schemes for Wireless Sensor Network

Mahesh A. Khandke
Dept. of Info. Tech, Gharda Institute of Technology, Lavel , Ratnagiri, M.S., India

Sachin D. Babar
Dept. of computer eng. Sinhgad Institute Technology, Lonavala, Pune, M.S., India

Snehal R. Rane
Dept. of Info. Tech, Gharda Institute of Technology, Lavel, Ratnagiri, M.S., India

Rajkumar B.Pawar
Dept. of Info. Tech, Gharda Institute of Technology, Lavel, Ratnagiri,M.S.,India.

Suryakant J. Gavale
Software Engineer, PANOMTECH Ltd, Chilun, Ratnagiri, M.S.,India

Abstract: ***Wireless sensor networks (WSN) usually consists of a large number of tiny sensors with limited computation capability, memory space and power resource. Sensor networks are widely used for applications such as environmental monitoring, airports safety, health care, etc. The communication of a wireless sensor network can be captured quite easily, thereby it requires security. To achieve security in wireless sensor network, key pre-distribution is essential. Many key pre-distribution techniques have been developed recently to establish pair wise keys between sensor nodes in WSN. In this paper, we have proposed improved pairwise key management scheme based on deployment knowledge of the wireless sensor networks. Compared with previous proposed key pre-distribution schemes, the proposed method could significantly improve the performance and energy efficiency of the sensor nodes. It is very suitable for the sensor nodes that are limited in power, computational capacities, and memory. The proposed scheme is substantially more resilient against sensor nodes capture [7].***

Key Words — Key Words — Key Pre-Distribution, Key Pool, Key Ring, Wireless, Sensor Networks.

I. INTRODUCTION

Recent advancement in wireless communication and electronics has enabled the development of low cost wireless sensor networks. A sensor network is composed of a lots of sensor nodes that are densely deployed either inside the phenomenon or very close to it. These sensor nodes consist of sending, data processing, and communication components [1]. Security is critical for a variety of WSN s applications, such as home security monitoring and military deployments. In these applications, each sensor node is highly vulnerable to many kinds attacks, both physical and digital, due to each node's cost and energy limitation, wireless communication and exposed location, which make the task of incorporating security in WSNs a challenging problem [4]. In WSNs security, the key management problem is one of the most important and the most fundamental aspects. To achieve security in wireless sensor networks, it is important to be able to encrypt and authentication messages among sensor nodes. Before doing so, keys for performing encryption and authentication must be agreed upon by the communication nodes. However, due to the resource constrains on the sensor nodes, many key agreement mechanisms used in general networks, such as Diffie-Hellman and other public-key based schemes , are not feasible in sensor networks. An effective key management scheme is the basis of the other security mechanism such as secure route, secure localization, confidentiality, authenticity, availability, and integrity. Recently, the key management problem has been extensively studied in the context of WSNs. The low memory and energy physical constraints of sensor nodes limit key management scheme in the real world. The key pre distribution is another class of solution using symmetric encryption techniques to this problem. This paper will present a new efficient key pre distribution scheme for secure wireless sensor network. It provides that any pair of sensor nodes can find a common secret key between them with simple calculation. Compared with previous proposed key pre distribution schemes, the proposed method could significantly improve the performance and energy efficiency of the sensor nodes. It is very suitable for the sensor nodes that are limited in power, computational capacities, and memory. The proposed scheme is substantially more resiliency against sensor nodes capture. The rest of this paper is organized as follows. Related work is described in section 2. In the section 3 we will present a new efficient key pre distribution scheme for secure sensor networks. In Section 4 the security analyses and the performances of the proposed scheme are discussed. Conclusions & future scope will be given in the section 5 and 6 respectively.

II. RELATED WORK

Key pre distribution is an important topic that constitutes the basis of security in wireless sensor networks. Many security mechanisms such as encryption and authentication can be provided by accessing to shared keys. Several techniques are previously proposed to address this issue. The Extensive features about key distribution in sensor networks are given by L.

Eschenauer and V. Gligor [9], H. Chan. A. Perrig and D. Song [10], D. Liu and P. Ning [11] and Subash.T.D,Divya .C [2]. Eschenauer and Gligor's basic scheme [9] is taken as a framework for many techniques using probabilistic key sharing for key management.These studies compared themselves with the basic scheme as we did in this paper. Eschenauer and Gligor's basic scheme [9] proposed a probabilistic key sharing scheme similar to basic scheme. It provides a secure communication network can be formed with key sharing information between sensor nodes. but it is vulnerable to the node compromise attack. H. Chan. A. Pemg, and D. Song modified E-G scheme by only increasing the number of keys that two random nodes share from at least 1 to at least q. It increased vulnerability in large scale node compromise attack. D. Liu and P. Ning proposed a polynomial pool-based key pre-distribution scheme where any two sensors can definitely establish a pair-wise key when there are no compromised sensors. It has low resiliency. Subash.T.D,Divya .C used Pairwise key pre distribution scheme to improves the resilience of the network. it is used single hop communication. These above papers are compared which describe information about security issues in wireless sensor network. So in this papers author are given some key management scheme techniques such as probabilistic, q-composite randomize, pair wise and polynomial pool based scheme. Key pre distribution results in high security during adversarial attacks.

Key pre distribution algorithms are classified into two groups:

1) Deterministic key pre distribution where the key assignment follows a certain pattern.
2) Randomized key distribution, in which keys are assigned randomly from a large key pool and preloaded in the sensors.

On comparisons we concluded that pair wise scheme is better than other scheme because by using this scheme our communication become very secure as compared to other scheme because we are using pairwise keys in this technique so intruder cannot alter data because it contain combination of 2 keys, so if intruder knows all this 2 keys then he/she can only access our data otherwise not.

III. PROPOSED SCHEME

In this scheme, we are combining the scheme which is given in [1] and [2]. With help of algorithm given in the [1] we are assigning the predistribution keys to the each sensor nodes so that the sensor nodes can get the common keys ($k_{i,j} = k_{j,i}$) in between N_i and N_j. In the second step two separate communication links are established between the nodes. If one of the communication links gets compromised by an adversary, there exists another link for secure communication between the nodes. Thus the resilience of the sensor network can be improved.

Following steps are used to generate pre distribution keys for secure transmission which are given in [1].

Generation & distribution of predistribution keys:

1. First, the system randomly chooses a positive integer t and a base of form $\{1,t, t^2, , ,t^{n-1}\}$
2. The system randomly selects a pool of secret keys $k_{i,j} < t$ such that $k_{i,j} = k_{j,I}$ for i= 1,2,…,n and j= 1,2,…,n
3. According to the Theorem 1, the system could construct the secret information S_i of the form $S_i = k_{i,1} + k_{i,2}t + .. + k_n t^{n-1}$ for i= 1,2,…,n by using these n distinct secret keys $k_{i,1}$, $k_{i,2,..}k_{i,n}$
4. Finally, the system assigns the secret information S_i and t to each node *Ni* for i= 1,2,…,n Therefore, any pair of nodes N_i and Nj could compute $k_{i,j} = k_{j,i}$ using their secret information S_i and S_j. respectively. Thus, $k_{i,j} = k_{j,I}$ is a common key between N_i and N_j .

Establishment Path key:

After getting pre distribution keys from a key pool using above method we are going to send this keys by using two separate communication links. The idea behind using two separate communication links is that if one link fails then we can use another link for communication in between two nodes. Between the two neighboring nodes there is a chance of not finding a common key space. In this case, it is necessary to find a secure way to agree upon a common key. It can be observed that two neighboring nodes i and j, do not share a common key space; but still come up with a secret key between them. The secure channels are used that have already been established in the key-space sharing graph. As long as the graph is connected, two neighboring nodes can find a path in GKS [2]. To find a common secret key between i and j, f first generates a random key K Then, node i sends the key to $v_1$using the secure link between i and v1; forwards the key to using the secure link between v_1 and v2 so on until j receives the key from V_{ij}. Nodes i and j use this secret key K as their pair wise key. Since the key is always forwarded over a secure link, no nodes beyond this path can find out the key.

IV. ANALYSIS

The security of the presented scheme is based on the secret information S_i and t, for i= 1, 2,...,n. Without knowing S_i and t, the attacker cannot derive the secret common key $K_{i,j}$ between of nodes N_i *and* N_j. On the other hand, the system constructs the secret information $S_i = k_{i,1} + k_{i,2}t + k_{i,3}t^2 + ... + k_i,3t^{n-1}$ for i= 1, 2,...,n, by using these n distinct secret keys $k_{i,1}$, $k_{i,2}$, …$k_{i,n}$. It provides n-1 or fewer keys cannot reconstruct the information S_i In this situation, even if all n-1 keys $k_{i,j}$ have been compromised between N_i and N_j for j = 1, 2,...,n, $j \neq i$, they also cannot obtain the secret information S_i and other information S_j for j = 1, 2,...,n, $j \neq i$. Similarly, for the node *Ni*, it has the common keys $k_{i,j} = k_{j,i}$, between nodes *Ni and N j* for j = 1, 2,...,n

.it is very difficult to create other information: S$i = k_{i,1} + k_{i,2}\, t + k\ i,3t^2 + ... + k_{i,3}\, t^{n-1}$ for i= 1, 2,..., n, $j \neq i$. Without knowing the information S_j, the node *Ni* could not easily derive other keys. Then, no sensor can forge another sensor node to communicate and mutual authenticate to each others. Hence, the proposed scheme is secure [5].

As shown in Table 1, in the proposed scheme, the computational complexity in the key pre-distribution step and finding a common secret key between any pair of nodes are and , respectively. The time complexity Hui-Feng Huang scheme is for computing a common key between any two nodes wanting to communicate, while the proposed scheme only requires one division modular computation [6]. Moreover, in Table1, in the proposed method, when any pair of nodes wants to derive the common secret key between them, they need not to transmit any Information to each other. However, in Hui-Feng Huang scheme [1], they have to exchange some messages for computing a common key. Compared with Hui-Feng Huang scheme, it is obvious that the proposed method can reduce large amounts of computation & communications for both in the key pre-distribution step and computing a common secret key for any pair of nodes. Thus, our method is more efficient and uses fewer communications than those of existing key predistribution schemes for secure wireless sensor networks. It significantly improves the performance and energy efficiency of the sensor nodes [6].

Table I: Comparisons of Hui-Feng Huang scheme and the proposed scheme

	Hui-Feng Huang scheme	**proposed scheme**
Key pre-distribution step	n^2T_m	n^2T_d
Compute a common key for any pair of nodes	T_d	T_d
Total number of transmissions for finding all pair of common keys	0	0

V. CONCLUSION

In this paper we have studied a various key management scheme for wireless sensor networks that provides security. Here we have proposed improved pair wise key management scheme based on deployment knowledge of the wireless sensor networks. The proposed scheme is substantially more resiliency against sensor nodes capture. Our scheme has a number of appealing properties. First, our scheme is scalable and flexible. For a network that uses 64-bit secret keys, our scheme allows up to N = 264 sensor nodes. These nodes do not need to be deployed at the same time; they can be added later, and still be able to establish secret keys with existing nodes. Second, compared to existing key pre-distribution schemes, our scheme is substantially more resilient against attack. Our scheme provides efficient construction of a secure pair wise authentication scheme without relying on the random model.

VI. FUTURE SCOPE

We will concentrate on probabilistic scheme in future. we will try to increase Local connectivity between nodes by adding XOR operation in efficient key management scheme. In the future, this wide range of application areas will make sensor networks an integral part of our lives. However, realization of sensor networks needs to satisfy the constraints introduced by factors such as fault tolerance, scalability, cost, hardware, topology change, environment and power consumption. Since these constraints are highly stringent and specific for sensor networks, new wireless ad hoc networking techniques are required.

REFERENCES

[1] Hui-Feng Huang,"A New Design of Efficient Key Pre-distribution Scheme for Secure Wireless Sensor Networks", Proceedings of the Third International Conference on International Information Hiding and Multimedia Signal Processing (IIH-MSP 2007) -Volume 01, 2007.

[2] Subash.T.D, Divya .C ,"Novel Key Pre-distribution Scheme in Wireless Sensor Network", 978-1-4244-7926-9/11/$26.00 ©2011 IEEE.

[3] T.Kavitha, S. JenifaSubhaPriya, Dr. D.Sridharan, "Design of Deterministic key pre distribution using number theory", 978-1-4244-8679-3/11/$26.00 ©2011 IEEE.

[4] Shuai Yang, Jie Liu, Chunxiao Fan, Xiaoying Zhang , JunweiZou , "A new design of security wireless sensor network using efficient key management scheme".

[5] Murat Ergun and Albert Levi, "Combined Keying Materials for Key Distribution", Sabaci,Istanbul,Turkey.

[6] Tzu-Hsuan Shan and Chuan-Ming Liu ,"Enhancing the Key Pre-distribution Scheme on Wireless Sensor Networks".

[7] I.F. Akyildiz, W. Su*, Y. Sankarasubramaniam, E. Cayirci, "Wireless sensor networks: a survey".

[8] Marcos A.M. Vieira1, Ariano B. da Cunha2, and Di´ogenes C. da Silva Jr.2, "Designing Wireless Sensor Nodes".

[9] L. Eschenauer and V. D. Gligor. "A key-management scheme for distributed sensor networks", In Proc. of the 9th ACM CCS conference, pp. 41 – 47, 2002.

[10] H. Chan, A. Perrig, and D. Song, "Random key predistribution schemes for sensor networks".In Proc. of the IEEE Symposium on Security and Privacy, p. 197, 2003.

[11] D. Liu and P. Ning, "Establishing pairwise keys in distributed sensor networks," In Proc. ofthe 10th ACM CCS Conference, pp. 52 – 61. 2003

[12] W. Du, J. Deng, Y. S. Han, and P. K. Varshney. " A pair wise key pre-distribution scheme for wireless sensornetworks ". In Proc. of the 10th ACM CCS Conference, pp. 42– 51. 2003.

[13] Donggang Liu, PengNing, Wenliang Du, "Group Based Key Pre Distribution in Wireless Sensor Networks".

