IJETST- Vol.||02||Issue||02||Pages 1815-1818||February||ISSN 2348-9480 2015

Open access Journal International Journal of Emerging Trends in Science and Technology

Literature Survey on Establishing Wireless Sensor Networks Using Otway Rees Protocol

Authors

Delona James[1], Jintu J Babu[2], Sushitha Susan Joseph[3]

[1,2]Student, Department of CSE, Mar Baselios Christian College of Engineering and Technology, Kerala, India

[3]Assistant Professor, Department of CSE, Mar Baselios Christian College of Engineering and Technology, Kerala, India

Emails: [1]*delona93@gmail.com*, [2]*jintujbabu1993@gmail.com*, [3]*sushisusan64@gmail.com*

ABSTRACT

Wireless sensor network has many application such as environment sensing, building safety monitoring, earthquake prediction etc. Security is critical issue in sensor networks. A fundamental security service is to establish pairwise key shared between two sensor nodes, which is basis of other security such as encryption and authentication. The prime problem in key management is to establish secure keys between the sensor nodes. To avoid this pairwise key establishment is used. This scheme consists of two key pools. One key pool is hashed value of keys in another key pool. With the one-way hash function, this scheme can make attackers get less key information from the compromised sensor nodes. Along with this Otway Rees protocol is used to provide integrity and authenticity. If direct path between two sensors are not present, then by using this protocol it is easy to find key with the help of intermediate node.

Keywords- *wireless sensor networks; key management;hash function*

I. Introduction

Wireless sensor networks (WSNs) are adhoc-network and it is a collection of node into a cooperative network. The application of wireless sensor networks are building safety monitoring, environment sensing, earthquake prediction, military uses, etc. The Application domains of Wireless Sensor Network are diverse due to the availability of micro-sensors and low-power wireless communications. The primary concern in WSN is security and also establishing a security connectivity between sensor nodes. A fundamental security service is to establish pair wise key shared between two sensor nodes, which is the basis of other security such as encryption and authentication. For enhancing the security. We are using pairwise key establishment using Otway Rees protocol. It consist of two key pools. By using this scheme we can achieve integrity and authenticity.

II. Literature Review

In [1] Eschenauer and Gligor was purposed schemes based on key pre-distribution. which is refer to EG scheme. It generates a large pool consist of random keys. From a large key pool each sensor node is preconfigured a random subset of keys before deployment of the network. To agree on a pairwise key for communication, two nodes are communicate with a common key. This scheme consists of three phases: key pre-distribution, shared-key discovery, and path-key establishment.

There exist a number of key pre-distribution schemes. let all the nodes carry a *master* secret key. To Achieve key agreement and obtain a new pairwise key, Any pair of nodes can use this global master secret key. If one node compromised, this scheme does not exhibit desirable network resilience: the security of the entire sensor network will be compromised. Some existing studies suggest storing the master key in tamper-resistant hardware to reduce the risk, but this increases the cost and energy consumption of each sensor. Consider each sensor carry N-1 secret pairwise keys, each of which is known only to this sensor and one of the other $N - 1$ sensors. The resilience of this scheme is perfect because compromising one node does not affect the security of communications among other nodes; however, this scheme is impractical for sensors with an extremely limited amount of memory because N could be large.

The disadvantage of the EG scheme is, From the same key pool all pre-load keys are selected .then next problem is the fraction of the affected keys increases quickly as a result of number of compromised sensor nodes increases. As a result, a small number of compromised nodes may affect large fraction of the secure link.

In [2] Based on Eschenauer -Gligor scheme, Chan, Perrig and Song proposed a q-composite random key pre-distribution scheme. Instead of just one common key to establish a secure connection ,It requires that two sensor nodes share at least *q* (q>1) keys.The *q*-composite scheme increase the network resilience against node captures, but it is only advantageous when there is few captured sensor nodes.

A generalization of this is the “q-composite” scheme it increase the resilience of the network (for the same amount of key storage) and requires an attacker to compromise many more nodes in order to compromise additional communication links. The difference between this scheme and the previous one is that the q-composite scheme requires two nodes to find q (with q > 1) keys in common before deriving a shared key.. Network resilience against node capture is improved for certain ranges of other parameters, by increasing the value of q. This scheme also have disadvantage, i.e. large number of key is needed and also it can be used when the number of sensor node is less.

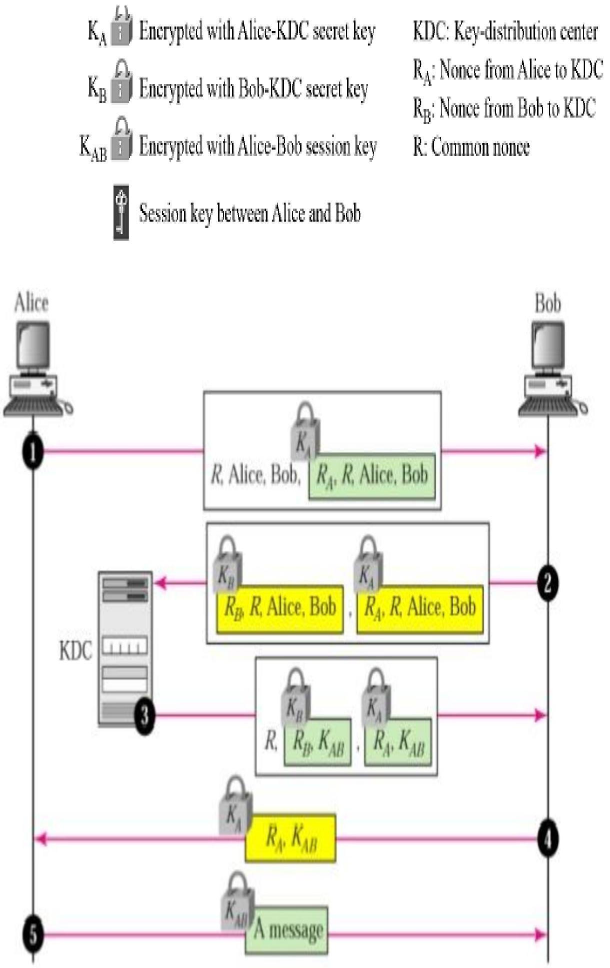
In [3] Du et al [3] proposed the multiple-space key pre-distribution scheme. In[3] each key is replaced by a special key space and many more people came with certain modifications to the existing scheme. All these schemes assume a random node deployment model where each sensor node has direct pair-wise keys shared with only portion of the neighbors, and depends on the multi hop or the path which is established in order for the nodes to communicate with long distance nodes.

In [4] we discuss the problem of designing a key predistribution scheme (KPS). The analysis of the [4] shows it has high global connectivity and resilience against nodes’ compromise. The KPS can be constructed and flexibly tuned in a wide range of design parameters. Most important characteristics of KPS are storage, connectivity, resilience , complexity. In this paper, we present a deterministic key predistribution scheme which is a combination of two different KPSs: the one based on a special class of combinatorial designs, called affine planes, and the well-known Blom’s scheme. This paper provides a modification to the original Blom’s scheme and presents a solution to reduce computation overhead and memory cost. The security parameter of the scheme is c, if more than c numbers of nodes are compromised, the whole network will be compromised

In[5] A polynomial-based key distribution scheme in which every sensor node is preloaded with coefficients of a symmetric bivariate polynomial evaluated at one of its variables using its identification value and the symmetry property of a polynomial allows every sensor node to establish a pairwise key with every neighbour sensor node or any node in the network evaluated at their ID value.In these key pre-distribution schemes, as the number of number of compromised nodes increases, the fraction of affected pairwise keys increase quickly.

In [6] Chan & ferriq was first to propose grid based key pre-distribution key ,in this scheme they placed the nodes of network in square grid this scheme is known as PIKE scheme. In this each node will have a secret pairwise key with the nodes which lie in the same row or same column the disadvantage of this scheme is high communication overhead.

In addition that we are proposing a new scheme using Otway Rees protocol. When there is no direct path, then use intermediate node for the key establishment. But if any attacker is present then they corrupts the key exchanged between source and destination. Normally it is difficult to identify this. With the help of Otway Rees protocol (ORP) it is easy to find whether correct key is exchanged between two sensors.



K_A Encrypted with Alice-KDC secret key
K_B Encrypted with Bob-KDC secret key
K_{AB} Encrypted with Alice-Bob session key
Session key between Alice and Bob
KDC: Key-distribution center
R_A: Nonce from Alice to KDC
R_B: Nonce from Bob to KDC
R: Common nonce
Alice
Bob
KDC
1
R, Alice, Bob,
K_A
R_A, R, Alice, Bob
2
K_B
R_B, R, Alice, Bob
K_A
R_A, R, Alice, Bob
3
R,
K_B
R_B, K_{AB}
K_A
R_A, K_{AB}
4
K_A
R_A, K_{AB}
5
K_{AB}
A message

Fig: Otway Rees Protocol

When sensor1 needs to communicate with sensor3, there is no direct path. So sensor2 act as the intermediate node. Sensor1 send (source, destination, R) to sensor3. Along that (source, destination, R, R_A) which is encrypted using K_A is send. At sensor3 it can see (source, destination, R) and add R_B i.e (source, destination, R, R_B) which is encrypted using K_B. This is send to sensor2. Sensor2 know K_A and K_B. So this can decrypt it. Sensor2 select one key R_{AB} for communication between sensor1 and sensor3. This key is encrypted using K_A and K_B. Sensor2 sends (R_A, R_{AB}) which is encrypted using K_A and (R_B, R_{AB}) which is encrypted using K_B to sensor3. Sensor3 decrypt (R_B, R_{AB}) using K_B and send (R_A, R_{AB}) to sensor1 which is decrypted using K_A. By this Sensor1 and sensor3 get R_{AB} as the key and then using that key they exchange another key which is used as the key between sensor1 and sensor3. By checking R , R_A ,R_B value we can know that any attacker is present or not. If any change to the value occurs then attacker is present otherwise sensors are secure. In the presence of attacker value of *R* , R_A ,R_B value is not same. The working of Otway Rees Protocol can be seen from the Above figure. Alice represents sensor1. Bob represent sensor3 and KDC represent sensor2.

III. CONCLUSION

In this paper, we proposed a novel key management scheme for wireless sensor networks. The scheme is based on EG scheme and use one-way hash function to generate a new key pool from a given key pool. With the one-way hash function, the proposed scheme can make attackers get less key information from the compromised sensor nodes. Compared to exiting key predistribution schemes, our schemes is substantially more resiliency against sensor nodes capture. .Along with this Otway Rees protocol is used to provide integrity and authenticity.

ACKNOWLEDGEMENT

We would like to thanks all the reference authors for the completion of this paper.

REFERENCE

1. I.F. Akyildiz, W. Su, Y. Sankara subramanian. A survey on wireless sensor networks. IEEE Communication Magazine, 2002, 38(8): 102~114

2. L. Eschenaure and V.D. Gligor, “A key-management scheme for distributed sensor networks”. in: Proc. of the 9the ACM Conference on Computer and Communications, Washington DC, USA, pp.41-47, Nov. 2002
3. J.Zhang, Q.Cui, X.Liu. An Efficient Key Management Scheme for Wireless Sensor Networks in Hostile Environments. in: International Conference on Multimedia Information Networking and Security, 2009, Hubei, pp.417-420, Nov.2009
4. H. Chan, A. Perrig and D. Song, “Random kcnney predistribution schemes for sensor networks”, in: Proc. 20003 IEEE Symposiumon Security and Privacy, pp.197-313, May 2003
5. D. Liu, P. Ning, and R. Li, “Establishing pairwise keys in distributed sensor networks”. ACM Transactions on Information and System Security, vol.8, pp.41-77, Feb. 2005
6. C. Blundo, A. D. Santis, A. Herzberg. S. Jutten, U. Vaccaro, and M. Yung. “Perfectly secure key distribution for dynamicconference”, Information and Computation, vol.1, pp.1-23 , Jan.1995

BIOGRAPHY

Delona James is currently pursuing her B.Tech Degree in Computer Science and Engineering in Mar Baselios Christian College of Engineering & Technology, Peermade, Kerala. Her areas of interest are networks, software engineering and data privacy.

Jintu J Babu is currently pursuing her B.Tech Degree in Computer Science and Engineering in Mar Baselios Christian College of Engineering & Technology, Peermade, Kerala. Her areas of interest are data privacy, object oriented programming and database management.

Sushitha Susan Joseph (M.E.,2012, Anna University, Chennai; B.Tech, 2009, Mahathma Gandhi University, Kottayam) is an assistant professor in the Department of Computer Science and Engineering, MBCCET, Peermade, Kerala. Her main research interests focus on artificial intelligence, data mining, wireless sensor networks.