International Journal of Science and Research (IJSR)
ISSN (Online): 2319-7064
Impact Factor (2012): 3.358

A Novel Secure Key Management Scheme for Wireless Sensor Networks Using Post Deployment Knowledge

R. Sharmila[1], V. Vijayalakshmi[2]

[1]Research Scholar, Department of ECE, Rajiv Gandhi College of Engineering & Technology, Puducherry

[2]Assistant Professor, Department of ECE, Pondicherry Engineering College, Puducherry

Abstract: ***The wireless sensor networks are resources constraint networks. The security is most major apprehension in wireless sensor networks. The traditional cryptographic schemes are not suitable for the resource constraints sensor networks. Many key management schemes are especially designed to overcome the constraints of wireless sensor networks. Each and every key management schemes are some tradeoff between limited resources and security. The most of the key management schemes are depends upon the deployment knowledge to improve the connectivity and resilience of the network. In this proposed hierarchical key management scheme, we divide the deployment field into tracks and sector and the keys are generated and distributed based on hop count, track and sector ID. For the construction of tracks and sectors, are carried out by base stations at the beginning of the network initialization. So the security as well as energy efficient key management scheme can be achieved. The proposed scheme dynamically generates keys among sensors based on sector and sensor location ID. Our improved scheme offers high resilience, connectivity and reduced energy consumption without any additional overhead.***

Keywords: Wireless Sensor Networks, Key Management Schemes, Deployment Knowledge, Resilience.

1. Introduction

The recent advancement in the field of wireless communication and MEMS technology, wireless sensor networks take part in an area of communication specifically to collect the data from the hostile environment. The nodes are deployed randomly or manually to gather the data in an environment and transmit to a base station or gateway. The base stations takes an appropriate decision based on the received information and communicates to outside world via satellite. The different applications of Wireless Sensor Networks are agriculture farming, battlefield surveillances, military application, habitat monitoring etc. The sensor nodes are resources constraint device; it has limited transmission range ,computational capability , limited memory and limited energy .In spite of limited resources these sensor nodes are used in a different applications like to sense the surrounding, process the sensed data including data aggregation and send it to destination. The wireless sensor nodes are widely deployed in hostile environment like military, tracking an object etc. A traditional cryptographic algorithm has a massive computation complexity, large processing, more storage space, large bandwidth and energy source. So, it does not suitable for the resource constraint tiny sensor nodes. Instead of using such complex algorithms, a light weight security protocols are needed to provide secure communication in wireless sensor network because of the resource constrained. These difficulties are overcome by means of light weight scheme called key Management schemes; it is especially designed for wireless sensor network designed for secure communication in wireless sensor networks. The key management schemes are classified depends upon encryption, deployment knowledge and rekeying mechanism. The factor influence the secure relation with neighbor sensor nodes during network formation are connectivity, resilience, computation.

Most of the security protocols are concentrating in single layer only, for example link layer or physical layer or network layer. It does not provide complete security solution to all the layers in the wireless sensor nodes. This paper endeavors to incorporate services provided to the network layer and application layer to provide solution to multilevel security services. In this paper, a novel integrated protocol for civilizing both the energy efficiency and security based on post deployment knowledge. The proposed protocol increases the survivability of the network by reducing unwanted communication. The topology used in this paper is based on the deployment knowledge. In this proposed method, the base station divides the area into sector and level based on communication range or power level of the sensor nodes. Using the deployment knowledge of sensor nodes, the base station assigns the keys for sensor node. The keys are generated by using the sector ID and level number. The rest of the paper is organized as follows.

2. Related Works

The most straightforward key distribution possible is to have a single network-wide key [1]. Such simplicity results in a high level of efficiency and flexibility, requiring minimal memory for the storage of keys no matter the size of the network. However, the network-wide key approach has serious security vulnerabilities; the capture of a single node discloses the common key, compromising all the nodes in the network.

To defend against the node capture, the full pairwise scheme adopts the extreme opposite approach. In this case, each of

the 'n' nodes in network receives n−1 pairwise keys to communicate with every other node.

The full pairwise scheme assures a high security level against node capture. However, this solution hasa great memory overhead and a bad scalability; the introduction of new nodes in the network is possible only if their keys are preloaded from the beginning.

The random key pre-distribution (RKP) scheme [2] preloads each node with a subset of keys, called a key ring, that are randomly selected from a large pool of keys. Any two neighbor nodes able to find a common key within their respective key rings can use the common key to establish a secure link. Based on the random graph theory, the size of the key pool and the size of the key ring are carefully chosen in order for the secure links to form a connected graph with a high probability. As the existence of a secure link between two neighbor nodes is guaranteed probabilistically, the RKP scheme belongs to probabilistic key sharing. The-composite RKP (y) scheme [3] requires that a pair of nodes have at least q common keys to establish a secure link. Theq-composite RKP scheme is more resilient than the RKP scheme when a small number of nodes are compromised. A key distribution scheme combining the probabilistic key sharing with the threshold secret sharing is given in [4]. Besides the probabilistic approach, there are a variety of approaches to the key management in WSNs.

Resilience in WSNs refers to the resistance of key distribution schemes against node capture. When sensor nodes are deployed in hostile areas (e.g., battle surveillance),an adversary can mount a physical attack on a sensor node and recover secret information from its memory. The resilience can be evaluated by computing the fraction of total network communications that are compromised by a capture of x nodes, excluding the communications in which the compromised nodes are directly involved. Whereas the authors of the RKP scheme [2] does not give a formal analysis of resilience.

3. System Description

The post deployment nature of WSN helps in improving the features of the security by means of dynamic key assignment. WSN are any derived form of mobile ad -hoc network in which all the nodes deployed are of the same hierarchy.

When we do generally speak about post deployment, it deals with the independent architectural construct when everything can be changed day in and day out.

Architecture framing involves the initialization o the random deployment of the sensors. Once done so a node is considered to be the gateway which the user wishes .On scenarios of area of deployment, paradigms, and the terrain and so on deployment arena is divided into various sectors and level. This methodology used is to implement divide and conquer technique so the routing of information and also the key management is found to be reliable.

On basis of post deployment a random distribution scheme is adopted to ensure a practical simulative environment which would the picture in real time .With the help of the gateway node an initial set of keys for its peers. This is to ensure the pinging phenomenon so that they make a single network.

Physical separations in the region are made by considering the worst case range of information transmission depending upon the mote used. Sensors used are generally unidirectional. With the help of a dynamic key change algorithm it makes extremely difficult for any illegal tapper to tap the confidential information. This is possible by means of using a play way encapsulation or morphing techniques. The algorithm for the same has been given below and also a brief view upon the detection failure algorithm is also given to have an insight of the detection of failure nodes:

3.1 Algorithm to initialize and to change keys

Step1: By default each node is loaded with Identification Number which may be of numerical and alphabet or both.
Eg. Id No: 25
Step 2: Initialize the sector and level number for each node after the deployment.
Eg. S=1 L=4.
Step 3: Get the text 1, text2 and text3 for generating encrypted key.
E.g.. Text1=Apple
Text2=Ball
Text3=cat.
Step 4: Read No. Of letters in the given text
Eg. Text1 size=5
Text2 size=4
Text3 size =3
Step5: Switch the value of sector for better PROBABLITY for the key matching criteria.
The value of i and j are in random probability.

Step6: Switch the value of level no. For better encryption
The value of k and l are in random probability.
Step 7: Generate key using the function
Enc1= txt3size^sector mod txt1siz
Enc2= txt3size^sector mod txt2siz
Step8: Secure the id no by using the fuction idsecure= id+txt3siz
Step 9: Generate the key in the respective order
Value of i | Value of j | value of K | Value of L| encoded no from the text | Encoded no form the text | secure id
E.g.: 76593045

3.2 Algorithms to detect nodal failures

Step 1: Remote Assignment Of The Nodes.
Step 2: Check for the Failure Of Nodes After Every Iteration.
Step 3: If Found To Be True Go For The Election Of Next Cluster Head.
Step 4: If No Abnormalities Are Found Then Continue the Same Process Recursively
Once the architectural formulation is done then emphasis is given towards the key matching. The sample key to be

78|23|ab|49|
The above given key is to visually represent the key generation where set pair of keys do match perfectly by key pool initialization. Once done the keys can be changed in the same manner.

4. Results and Discussions

4.1. Overall Failure rate Assessment

Number of study cases: 25
Threshold fixed: 0.68
Number of combinations of the keys: 100
The reliability under controlled simulation environment is100%

4.2 Key Generation

Enter the Sector No. of the Node (Sensor):1
Enter the Level No. of the Node (Sensor):3
Enter the id No of sensor : 45
Enter the Text1 for Encapsulation: 'apple'
Enter the Text2 for Encapsulation: 'ball'
Enter the Text3 for Encapsulation: 'cat'
Processing Key
1
3
45
5
4
3
Key Generated
7
6
8
1
2
4
51

4.3 Key Matching

Enter the Generated Key
7
6
8
1
2
4
51
Enter the Text1 used for Encryption: 'apple'
Enter the Text2 used for Encryption: 'ball'
Enter the Text3 used for Encryption: 'cat'
Sector No. of the Node:
1
Level No. of the Node:
3
Unique ID of the Node
45

4.4 Comparison of energy consumption of existing and proposed scheme

Hence the below mentioned table gives a clear picture of the consumed energy between the proposed and existing probabilistic methods. Inference showed the this scheme is far more superior is consumption of energy.

Table 1: Comparison of energy consumption

Number of Nodes	Conventional Random Method Energy Consumption In (Joules)	Proposed Method Energy Consumption In (Joules)
10	52.748 (u)	(u)
50	735.87 (m)	45.44 (m)
100	2744.45	137.89 (m)
200	14403.74	243.1(m)
500	39407.37	560.65(m)
1000	84891.52	1328.90(m)

5. Conclusion

This work aims to serve as the guideline for the student and researchers that want to validate in Mat lab environment own algorithm proposed for the WSN applications. We have showed how to proposed and visualize WSN topology and how to route data through the multi hop paths. We have also proposed energy model that can be used for transformation of the communication cost to the energy consumption. The ideas in proposed energy model were supported by the analysis of the real sensor network. We notify, that only simplified energy model was stated here. The nodes spent most of time in the sleep mode and thus the significant attention should be devoted to this factor.

6. Future Work

Thenceforth the above proposed methodology can be applied in defense oriented applications where more emphasis is given to security in transmission of information. Hence this method on implementation will contribute to increasing the credentialed of the information. Also by enhancing the raw energy conservation scheme the consumption for the same can also be reduced. This novel system will have huge impact when refined and implemented.

References

[1] G.D. Abowd, J.P.G. Sterbenz, Final report on the interagency workshop on research issues for smart environments, *IEEE Personal Communications* (October 2000) 36–40.
[2] J. Agre, L. Clare, An integrated architecture for cooperative sensing networks, *IEEE Computer Magazine* (May 2000) 106–108.
[3] I.F. Akyildiz, W. Su, A power aware enhanced routing (PAER) protocol for sensor networks, *Georgia Tech*

Technical Report, January 2002, submitted for publication.

[4] A. Bakre, B.R. Badrinath, I-TCP: indirect TCP for mobile hosts, *Proceedings of the 15th International Conference on Distributed Computing Systems*, Vancouver, BC, May 1995, pp. 136–143.

[5] P. Bauer, M. Sichitiu, R. Istepanian, K. Premaratne, The mobile patient: wireless distributed sensor networks for patient monitoring and care, *Proceedings 2000 IEEE EMBS International Conference on Information Technology Applications in Biomedicine*, 2000, pp. 17–21.

[6] M. Bhardwaj, T. Garnett, A.P. Chandrakasan, Upper bounds on the lifetime of sensor networks, *IEEE International Conference on Communications ICC'01*, Helsinki, Finland, June 2001.

Author Profile

R. Sharmila graduated B.E (Electronics and Communication Engineering) from Annamalai University in the year 2006.She obtained her Master degree in Computer and Communication Engineering from Dr.Pauls Engineering College, Anna University in the year of 2010.At Present, she is working as Assistant Professor in the Department of Electronics and Communication Engineering, Rajiv Gandhi College of Engineering and Technology, Puducherry. Presently, she is working towards PhD in Pondicherry Engineering College, Puducherry, India .Her current area of research is network security issues in wireless sensor networks. She is a member of ISTE.