ISSN No. 0976-5697

Volume 3, No. 7, Nov-Dec 2012

International Journal of Advanced Research in Computer Science

REVIEW ARTICLE

Available Online at www.ijarcs.info

Low Power Key Management Protocol for Wireless Sensor Network

Santosh L Deshpande
Professor Department of Computer Science and Engineering
B V B College of Engineering and Technology
Hubli. Karnataka India
sld@bvb.edu

Abstract: Wireless sensor networks are highly sensitive to the energy consumed as they consume more power in communication and routing the data across each other also The energy cost of transmitting 1 Kb a distance of 100 m is approximately the same as that for the executing 3 million instructions by 100 million instructions per second/W processor. In the current work the authors have thought upon the energy aspects such that the un-scaled i.e raw value of the data shall be used instead of the converted value. The material defects and aging factors will also be used to hide the actual value of the data. Also complete use of symmetric key ensures that power saving happens at every aspect. The use of swarm intelligence for the generation of the keys also provides dynamic security. Several symmetric-key pre-distribution protocols have been investigated recently to establish secure links between sensor nodes, but most of them are not scalable due to their linearly increased communication and key storage overheads. Furthermore, existing protocols cannot provide sufficient security when the number of compromised nodes exceeds a critical value. To address these limitations, we propose an improved key management mechanism for large-scale wireless sensor networks. A highly unexposed area of non-scaled data has been chosen as one of the parameters along with an innovative method called graph based key management integrated with each others to solve this problem.

Keywords: Key management, Wireless sensor networks, cryptography , symmetric key algorithms, Scaling of sensors.

I. INTRODUCTION

All Wireless sensor networks are inherently collaborative environments in which sensor nodes self-organize and operate in groups that typically are dynamic and mission-driven. Secure communications in wireless sensor networks under this collaborative model calls for efficient group key management. However, providing key management services in wireless sensor networks is complicated by their ad-hoc nature, intermittent connectivity, large scale, and resource limitations. To address these issues, this paper proposes a new energy-efficient key management scheme for networks consisting of a large number of commodity sensor nodes that are randomly deployed. In the presented methodology the author has tried to use the materialistic problems present in the sensors that vary from sensor to sensor due to material defects also as a one of the major parameters to identify the sensor correctly for the self authentication purpose. The graph based key management scheme is used to share a large numbers of keys instead of one secret key. This graph will be used for the key generation and this will change for time to time such that compromising the sensor nodes will be highly impossible. This innovative method is energy efficient as well as fast. A protocol also is designed that can stop the man in middle attack also. To overcome the relay attack the synchronized clock of base station and sensor nodes are used.

II. SYSTEM AT A GLANCE

A. Initial setup:

Pre distribution of keys is the common activity that is followed in any wireless sensor networks. The sensors are configured and necessary data is installed that can be initial transmission of the keys before deployment of these at the remote locations. This is treated as the first key transmitted between the sensors and the base station where the aggregation of the data from such several sensors will happen. The idea is to do the maximum processing at the base stations than the sensor node.[1] The graph is installed at these sensor nodes so that the key generation can happen in the following way. All the pubic key generation algorithms deal with the problems like factorization and discrete mathematics of higher values of the prime numbers.

These methods are highly time consuming and vulnerable to the attacks. Thus, the mathematical functions used above are other than discrete and factorization type. [2] This is being to avoid longer computational time and possible intrusion as is being done in earlier methods discussed above. The graph so designed will solve the problem as it can use any function that is sensitive to the input values like logarithmic and hyperbolic functions. These functions are invoked when that node is traversed while generating the key value. The ant colony algorithm [3,4] to solve the TSP will use such graphs. With this the functions at the nodes will generate the keys and will be stored in the tabu_list of the ants. After the global optimization the final list of key values will be available in the tabu_list. The discussion is represented through the

figure 1 In the figure 1, a small portion of the shared graph is shown that is chosen to select the keys.

ABCDE are the nodes of one tour. The designed graph says that every node is a function and edge has some weight generated randomly. The key will be generated as follows. If the user chooses the source node as B and destination node as node E then key will be

Key = fe(fd(fc(fb(BC),CD),DE)) …….. 1

In the above formula the suffix of f's are the functions associated with individual nodes.

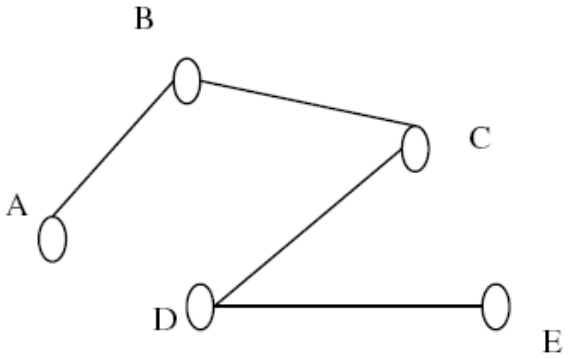


Figure 1 The chosen Path

These functions will collectively generate the value of a key, which is unique and highly sensitive to its seed value as the chosen functions are logarithmic and hyperbolic. The method reduces the power consumption as encryption and decryption of the RSA is very high for the sensor nodes to deal with. The strength of the generated keys is also calculated for NIST standards. [5] After seeing up the communication after deployment of the sensors will take place. The sensor will transmit the nodes chosen along and encrypt the data using Blow Fish along with the sensor identity.

At the base station upon reception of this data it will be decrypted with same keys as the keys related to that nodes is available with the base station. The data related to scaling is also available in the base station this will be used to extract the information from the raw un-scaled data. B. Using the techniques of scaling of the sensors the sensor is a device that converts an analog quantity with the equivalent digital code. The sensor follows a specific equation which is used by the sensor to map this value to the digital equivalent code.

In the conventional systems the sensor node itself calculates the digital real time equivalent but in the presented method in this paper purposely avoids this conversion that will act as one more level of encrypting the data. In spite of man in middle attack the attacker will not be in a position to gain the digital equivalent.

System Protocol

Esh Shared key for communication by both Base Station and Sensor Node

BSid Base-Station identification number

SENid Sensor Node identification number

RA Random Number generated by Base-Station

RB Random Number generated by Sensor-Node

KR Session Random Key

a. Base Station to Sensor Node: Base Station sends Encryption message which include Base-Station identification number , Sensor Node identification number, its Random Number ,along with the Time Stamp .:Esh (BSid , SENid , RA ,TB)
b. Sensor Node to Base Station: same message along with the its random number in Encryption format using Esh.: Esh (BSid , SENid , RA,TB, RB)
c. Decrypts the message at Base station and confirm that RA and TB values as it did in step (a) Base Station sends the two messages to Sensor Node , the first is all information as said above along with random session key all encrypted with the Esh. The second is key bench encrypted with the session random key (KR) Esh (BSid , SENid , RA,TB, RB, KR)

KR (Key bench data()

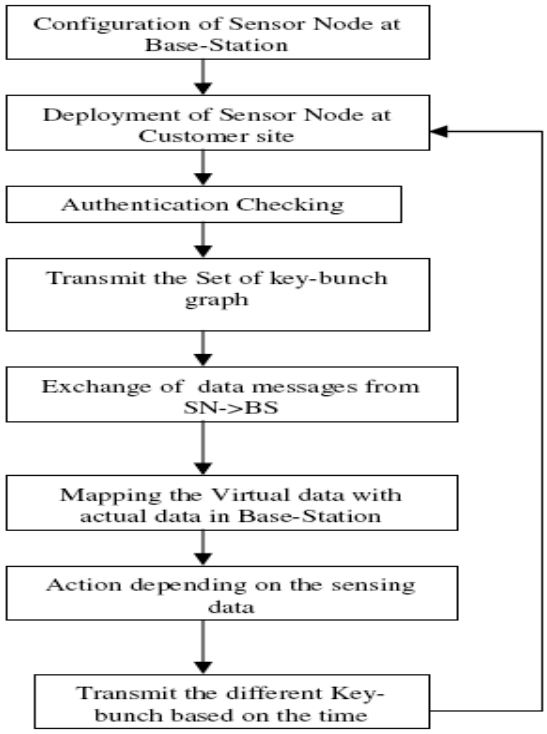


Figure 2 Protocol at a glance

Table: 1 Need of WSN w.r.t. Applications 5 being the best

WSN Type	Scalability	Resilience	Storage	Power	Communication
Military	5	5	4	5	4
Disaster	2	4	3	2	4
Industry	4	4	3	4	5
Agriculture	2	3	2	4	4
Environment	4	3	3	4	4
Bio medical	4	5	3	4	4
Transport	3	4	4	3	4

Type Style and Fonts
Two messages are sent to Sensor Node

d. At Sensor node The first message is decrypted by Esh and extract the value of KR and with the help of KR it extract the Key bunch data.

III. RESULTS AND ANALYSIS

The key generation and management was done using the presented methodology called as swarm intelligence and Blowfish was the symmetric key algorithm used use of logical blocks in symmetric key algorithm improves the power efficiency of the secured communication also the strength of the keys was measured using tests of NIST and produced promising results.

Swarm intelligence [6] is an area of research that over the last decade has experienced a boom in interest. Inspired by the seemingly intelligent behavior of swarms of primitive animals, swarm intelligence has proven to be a promising field of research in many different areas. By observing and modeling the processes that occur in natural ants when working in their natural domain, it is possible to use this as inspiration to create a 'colony' of artificial ants, working in an environment represented by a graph and potentially experience a similar emergent intelligence. In fact, researchers in the field of biology have developed good theories on how ants communicate as a group and attempts to adapt these theories to a simulated domain in a computer have verified that it is possible to obtain emergent intelligent behavior from colonies of artificial ants. The use of the Ant colony algorithm applied to solve a problem like traveling sales person problem with the use of long period random number generator and Polynomial based random number generator functions applied at the nodes [7].

The Ant colony algorithm is executed at its worst case complexity that is n3. There after it takes only linear complexity [8]. As the TSP is getting solved for transitively closed graph the list of intermittent nodes is obtained in the linked list. Each value of the graph edge is operated on the random number generator functions like simple and fast random bit generator (SFRNG) and Long period random number generator (LPRNG). The combination of these operated on the graph value will generate a sound cryptographic key. Use of multiple functions in multiple rounds will ensure a perfect cryptographic key that can be used for encryption. The graph is shared at both the legitimate users using public key crypto system and these mirror images of the graphs at both the systems will make sure that the same key is generated at any point of time.

The uses of LPRNG and SFRNG have produced promising results that are shown in the graphs below. The NIST test of frequency and runs test for both generators are as follows.

The probability (under the null hypothesis of randomness) that the chosen test statistic will assume values those are equal to or worse than the observed. The P-value is frequently called the "tail probability." A P-value 0.01 would mean that the sequence would be considered to be random with a confidence of 99 %. The results on a large sample of data and various combinations of seed produced following results.

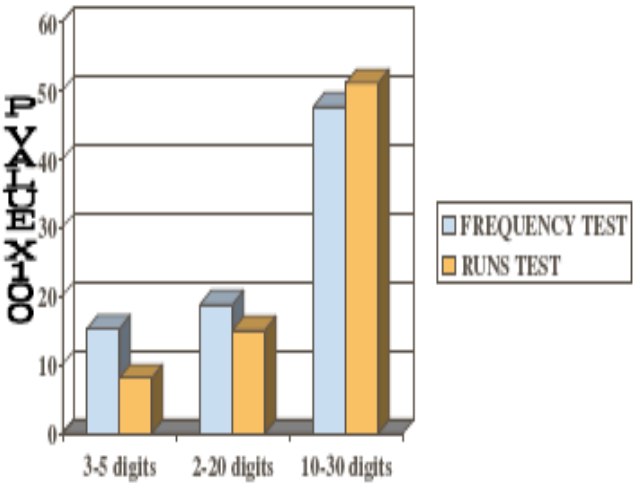


Figure: 3

PRNG graph for the sample up to 30 digits number

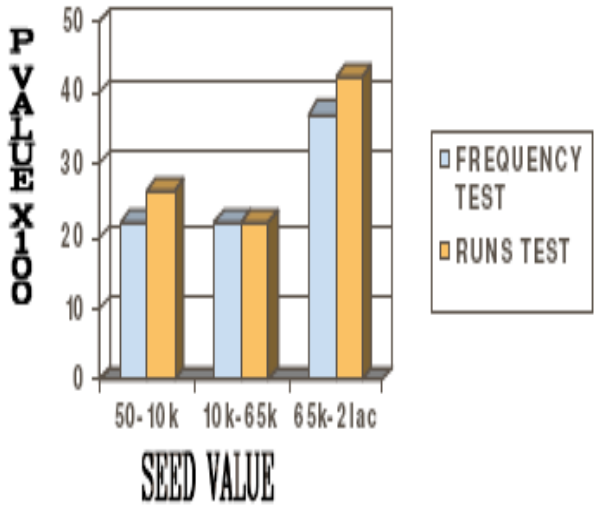
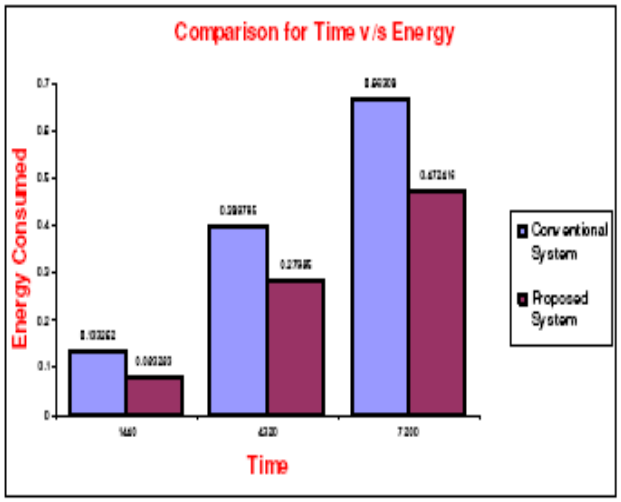


Figure: 4

FRNG graph for the sample up to 2 lack samples

For LPRG
Average p values observed:
0.4708 for frequency test
0.5173 for runs test.
Failure rate observed:
0.38% for frequency test.
1.53% for runs test.
Collision rate observed: 2.8%
For SFRG
Average p values observed:
0.3724 for frequency test
0.4207 for runs test.
Failure rate observed:
4.64% for frequency test.
3.5% for runs test.
Collision rate observed: 0.53%



Comparison for Time Vs Energy consumed for Ten Sensors

Figure:5

In any wireless sensor networks based on applications following parameters are required. Looking in to the table1 all the application areas need enhancement on the communication and power through this paper the same can be achieved. However more emphases on security and key management related aspects are done. Apart from this the work was carried out such that every mathematical instruction was counted with the logical one and observed the following in terms of energy saving as shown in the following graph.

It is observed that proposed system consumes average 22% less power compared to the existing system.

IV. CONCLUSION

Overall the solution to the problem to get a better and faster key management scheme for the sensor networks is achieved. To achieve this new scheme proposed that uses the ant colony model's swarm intelligence to exchange the keys between the legitimate users. The complete key management life cycle is achieved. That takes less time as well as its power efficiency makes it ideal for the scenario of wireless sensor networks.

V. ACKNOWLEDGMENT

The author S L Deshpande acknowledges the help and encouragement shown by their respective heads of the institute and managements in carrying out this work.

VI. REFERENCES

[1]. Ankit Mehta, Deepak T. J, Arpit Mehta Compendium of Applications For Wireless Sensor Network" All the three authors were summer interns at TCS Chennai in summer 2005

[2]. Wenliang Du., Jing Deng., Yunghsiang S. Han, Shigang Chen, and Pramod K.Varshney . "A Key Management Scheme for Wireless Sensor" Department of Electrical Engineering and Computer Science Syracuse University, Syracuse, NY 13244-1240, IEEE INFOCOM 2004.

[3]. Pierre Delisl, Michaël Krajecki, Marc Gravel, Caroline Gagné "Parallel Implementation of an Ant Colony Optimization Metaheuristic with OPENMP" MIC2005. The 6th Metaheuristics International Conference Vienna, Austria, August 22–26, 2005.

[4]. K Roberto Di Pietro , Luigi V. Mancini , Sushil Jajodia "Providing secrecy in key management protocols for large wireless sensors networks"Available online www.elsevier.com/locate/adhoc 27 May 2007.

[5]. NIST Special Publication 800-22 (with revisions dated May 15, 2001) on Randomness by Andrew Rukhin, Juan Soto, James Nechvatal, Miles Smid, Elaine Barker, Stefan Leigh, Mark Levenson, Mark Vangel, David Banks,Alan Heckert and James Dray, San Vo

[6]. Pierre Delisl, Michaël Krajecki, Marc Gravel, Caroline Gagné "Parallel Implementation of an Ant Colony Optimization Metaheuristic with OPENMP" MIC2005. The 6th Metaheuristics International Conference Vienna, Austria, August 22–26, 2005.

[7]. Richard Crandall and Carl Pomerance, "Prime Numbers", Springer publication 2 edition.

[8]. Marco Dorigo Universit´e Libre de Bruxelles, "The Ant Colony Optimization Metaheuristic: Algorithms, Applications, and Advances Technical Report" IRIDIA-2000 pp10-32