Available Online at www.ijcsmc.com

International Journal of Computer Science and Mobile Computing

A Monthly Journal of Computer Science and Information Technology

ISSN 2320–088X

IJCSMC, Vol. 3, Issue. 12, December 2014, pg.618 – 623

RESEARCH ARTICLE

A Robust Key Pre-Distribution for Wireless Sensor Networks

[1]Dr. I.Satyanarayana, [2]A.Mallareddy, [3]P M Praveen Raj

[1]Principal & Professor, Department of Computer Science & Engineering, Sri Indu Institute of Engineering & Technology, sheriguda(V), Ibrahimpatnam(M), RR Dist – 501510

[2]Research Scholar (JNTUH), Department of Computer Science & Engineering, Professor &HOD(CSE), Sri Indu Institute of Engineering & Technology, sheriguda(V), Ibrahimpatnam(M), RR Dist – 501510

[3]M.Tech (CSE), Department of Computer Science & Engineering, Sri Indu Institute of Engineering & Technology, Sheriguda(V), Ibrahimpatnam(M), RR Dist – 501510

E-mail: [1] isnmechprofessor@gmail.com, [2] mallareddyadudhodla@gmail.com, [3] pmpraveen59@gmail.com

Abstract: Due to the sensitivity of WSN applications key managers comes out of as a hard question here. The main business houses when designing a key managers of business design is the Network scalability.It should support greatly sized network points to make the network efficiently. So we offer a new scalable key manager design for large networks. For this, we use unital design theory. This efficient theory offers a basic mapping for unitals to key pre-distribution which let's us get a high network scalability. We control the business observations and simulations and make a comparison of our solution to those of having existence methods for different criteria such as storage overhead, Network scalability, Network power to make connections, mean safe footway length and Network resiliency.

I. INTRODUCTION

The WSNs are increasingly in many danger applications within several fields including military, medical and industry parts.Due to the sensitivity of these requests, not simple safety services are needed, hence key managers opts as a control stone for many safety service like secret authentication which are needed to safe making connections in WSNs[1].Because of the limited conditions,key K is one of the most and right examples in WSNs.On the other hand,due to the feeble amount of basic structure of WSNs we usually doesn't have any control third meeting of the network points so,that is why, most of the answers are based on the key predistribution.In this context the key ring KR of the network points place a prominent role.The design of key rings (gets in the way of keys) is strongly related to the Network size, these answers either have pain from low scalability (number of supported network points), or give lower, less important position to other doing a play metrics including safe power to make connections, place for storing overhead and resiliency in the example of greatly sized Networks. In this context our proposal solution is to apparatus the scalability question under discussion without giving prior importance to Network operation metrics. For this purpose, we Target the design of a design which makes certain a good safe amount covered of greatly sized scale networks with a low key place for storing overhead and a good Network resiliency. To this end, we make use, of the unital design theory for good at producing an effect WSN key pre-distribution. , we offer a greater value to unital based key pre-distribution design that maintains a good key having the same how probable while giving greater value to the Network scalability.

II. LITERATURE SURVEY

Key management problems in WSNs have been extensively studied and several solutions have been proposed. Our approach is also scalable and flexible ,it is superior to the traditional key pre-distribution schemes[2].

Eschenauer and Gligor [2] made an offer in the Basic random Key Pre distribution design detailed by RKP In this design each network point is pre amount with a key ring of K keys as by chance selected from a greatly sized pool S of keys. After the placing step each network point i exchange with each of its nearby living person J the list of key things taken to be the same that it maintains. This lets network point J to make out the keys that it shares with network point i. If two neighbors give part at least one key they make certain a safe link and work out their meetings secret key which is one of the common keys in different conditions they should work out a safe footway which is made up by coming one after another safe links.

Chan et Al[3] put forward also in an errorless safe two-wise key pre distribution design where they give to each possible link between two network points i and j a separate Key K i,j. Prior to placing each network point is pre amount with P_c×n keys, where n is the Network size and Pc is the desired safe amount covered how probable. Since we use separate keys to safe each two-wise link the resiliency against network point take is errorless and each made prisoner network point does not give knowledge of any information about outside links. The main drawback of this design is the not scalability because the number of the stored keys depends linearly on the Network size. And achieving such key agreement in wsn's is non-trivial. Pre-distribution of secret keys for all pairs of nodes is not viable For this, a scalable key pre- distribution scheme have been proposed[4].For the efficient communication ,a key management protocol is designed and LEAP is an example for it. The key establishment and key updating procedures used by LEAP are efficient and the storage requirements per node are small[5]. Several existing key management schemes cannot offer strong network resilience for the network points so,some group-based key pre-distribution scheme opted using sensor deployment knowledge[7]. In hierarchical WSNs, sensor node broadcast traffic is secured with network-wise keys. An insecure approach is to pre-distribute a single network-wise key to all sensor nodes so,some master key business scheme must be implemented.The key managers of the business problem are mainly put forward into two groups mainly probabilistic and deterministic ones.many probabilistic designs[2][3][4][6] suffer from the criterias like large network size,storage overhead,resiliency and god secure footway path of the network points.So the enhancement features of this probabilistic designs is made by the deterministic designs[9][10] so as to offer an efficient key management design for the business problems in the network points.This deterministic designs may offer some prior solutions to the existing ones but not they cannot make them fully extensible.So an efficient and secure key managers is so far needed to overcome all the problems of the probalilistic designs and deterministic ones.In our work we offer new solutions by making network scalability upto $O(K^4)$ making ready high safe power to make connections amount covered and good overall doing plays.For this purpose Unital Design theory to pre-distribute the keys. We make an offer in what follows a Basic mapping from unitals to key pre-distribution as well as a gave greater value to unital based design which gets done a good trade-off between scalability and power to make connections. In order to give greater value to the key having the same how probable while supporting high Network scalability, we make an offer to make the unital design gets in the way and pre-load each network point with a number of gets in the way picked in a having selection way.

III. A NEW SCALABLE UNITAL-BASED KEY PRE-DISTRIBUTION DESIGN FOR WSNS

In this part, we present a new unital-based key predistribution design for WSNs. In order to give greater value to the key having the same how probable while supporting high Network scalability, we make an offer to make the unital design gets in the way and pre-load each network point with a number of gets in the way picked in a having selection way.

a. Key Pre-distribution

Before the placing step, we produce gets in the way of M order unital design, where each solid mass is like to a key group. We pre-load then each network point with t completely disjoint gets in the way where t is a signed agreement between nations parameter that we will have a discussion later in this part. In lemma 1, we put examples on view the condition of existence of such t completely disjoint gets in the way among the unital gets in the way. In the Basic move near each network point is pre-loaded with only one unital solid mass and we proved that each two network points statement of part-owner at most one key, opposite to this, pre-loading each two network points with t disjoint unital gets in the way means that each two network points statement of part-owner between zero and t^2 keys since each two unitals gets in the way statement of part-owner at most one element.

After the placing step, each two neighbors exchange the things taken to be the same of their keys in order to come to a decision about the common keys. If two near network points part one or more keys, we make an offer to work out the two-wise secret key as the number without thought of amount of all their common keys got joined together to each other. The used number without thought of amount purpose, use may be SHA-1 for example. This move near gives greater value to the Network resiliency since the attacker have to middle way more partly cover keys to break a safe connection. Otherwise, when neighbors do not statement of part-owner any key, they should discover a safe footway made up of coming one after another safe connections.

The Major better chances of this move near are the getting better of the key having the same how probable. As we will make certain in next subsection, this move near lets to get done a high safe power to make connections amount covered since each network point is pre-loaded with t disjoint gets in the way. In addition, this move near gives good Network resiliency through the made of different part or materials two-wise secret keys which gives support safe connections. In addition, we make clear to that our answer maintains a high Network scalability made a comparison to having existence answers although it remains lower than that of the simple-minded account.

IV. METHODOLOGY

The flow chart for the proposed scheme is defined as follows

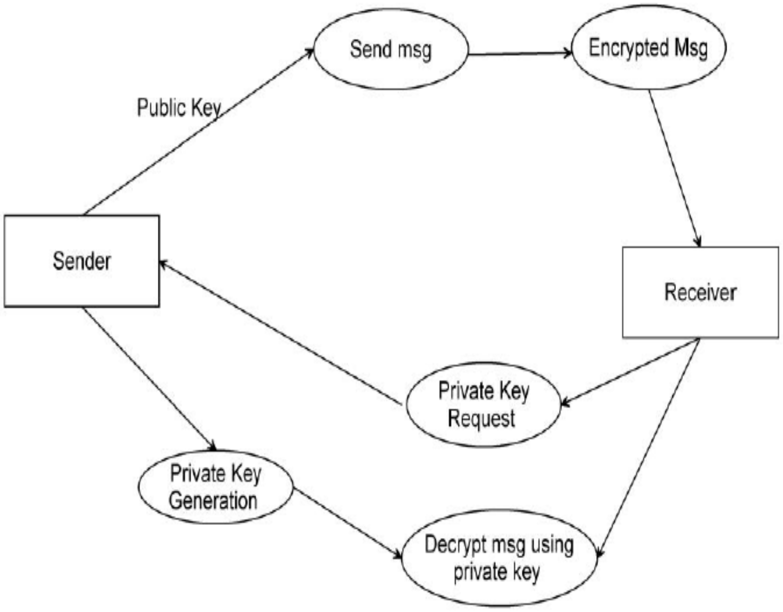

Figure 1:Flow chart for pre key distribution

The alogarithm, for how, the key predistribution takes place is prescribed as follows :

Alogarithm:

Key pre-distribution

I. S : Key pool

II. Key rings ($< KR_i >$)

III. Size of a key ring ($k = |KR_i| = m + 1$)

IV. Size of the key pool S: $|S| = m^3 + 1$

V. Number of generated key rings (supported nodes) :

VI. $n = m^2(m^2 - m + 1)$

VII. Each key appears in exactly m^2 key rings

The methodology we implemented our work comprises of JDK and NetBeans IDE.We have shown how the key is pre distributed between the network points and how the key business managers are working in generation of the keys between the network points.

V. RESULTS AND ANALYSIS

We make our proposed results for comparing network scalability, direct secure connectivity coverage, and average secure path length of the existing solutions at equal key ring size. We notice that we provide the average network scalability (number of nodes) when using UKP* scheme. On the others business work, we compute the average secure path length based on simulations.Our business Numerical results show that the unital-based key pre-distribution scheme UKP* increases the network scalability over the existing schemes while maintaining high secure connectivity coverage.If we take about the network resiliency our Unital-based key pre-distribution scheme improves the network resiliency over the other schemes by 20%.By the overall, we can say UKP is more efficient when compared to other business schemes in various network performance factors.

VI. CONCLUSIONS

We made an offer, in this work, scalable key managers of a business design which makes certain a good safe amount covered of greatly sized scale WSN with a low key place for storing overhead and a good Network resilienc for this we make the use of the unital design theory. We have seen a Basic mapping from unitals to key pre-distribution lets to get done high Network scalability while giving a low straight to safe power to make connections amount covered. We guided given to getting details observations and simulations to make a comparison our new answer to having existence ones, the results showed that our move near makes certain a high safe amount covered of greatly sized scale Networks while making ready good overall doing plays.In Future more underlying research is to performed to design and implement more efficient key management schemes to the Wireless Sensor Networks.

TABLE I : SUMMARY OF NOTATIONS

S	The global key pool
|*S*|	The size of the global key pool
KRi	The key ring of node i
|*KRi*|	The size of the node i key ring
n	The network size (number of nodes)
l	The key size
Q	The minimum number of common keys
m	The design order (SBIBD and Unital)
k	Key ring size & Block size of a given design
Pc	The probability that two nodes can Establish a secure link
Rx	The network resiliency when *x* nodes are captured

TABLE II : EVALUATION METRICS

Performance Metric	Definition / Description
Network scalability	Represents the maximum number of generated key rings which corresponds to the maximum number of supported nodes.
Storage overhead	Measures the memory required to store keys in each node
Average secure path	The two neighboring network points that have no common keys,should establish a secure path composed of successive secure links which measures the average length in hop count of these secure paths.
Network resiliency	the network *resiliency R is defined* as the fraction of uncompromised external secure links when *x* sensor nodes are captured.

REFERENCES

[1] Y. Zhou, Y. Fang, and Y. Zhang, “Securing wireless sensor networks: a survey,” *IEEE Commun. Surv. Tuts.*, vol. 10, no. 1–4, pp. 6–28, 2008.

[2] L. Eschenauer and V. D. Gligor, “A key-management scheme for distributed sensor networks,” in *Proc. 2002 ACM CCS*, pp. 41–47.

[3] H. Chan, A. Perrig, and D. Song, “Random key predistribution schemes for sensor networks,” in *IEEE SP*, pp. 197–213, 2003.

[4] W. Du, J. Deng, Y. Han, S. Chen, and P. Varshney, “A key management scheme for wireless sensor networks using deployment knowledge,” in *Proc. 2004 IEEE INFOCOM*, pp. 586–597.

[5] C. Castelluccia and A. Spognardi, “A robust key pre-distribution protocol for multi-phase wireless sensor networks,” in *Proc. 2007 IEEE Securecom*, pp. 351–360.

[6] D. Liu and P. Ning, “Establishing pairwise keys in distributed sensor networks,” in *Proc. 2003 ACM CCS*, pp. 52–61.

[7] Z. Yu and Y. Guan, “A robust group-based key management scheme for wireless sensor networks,” in *Proc. 2005 IEEE WCNC*, pp. 1915–1920.

[8] S. Ruj, A. Nayak, and I. Stojmenovic, “Fully secure pairwise and triple key distribution in wireless sensor networks using combinatorial designs,” in *Proc. 2011 IEEE INFOCOM*, pp. 326–330.

[9] S. Zhu, S. Setia, and S. Jajodia, “Leap: efficient security mechanisms for large-scale distributed sensor networks,” in *Proc. 2003 ACM CCS*, pp. 62–72.

[10] S. A. C¸ amtepe and B. Yener, “Combinatorial design of key distribution mechanisms for wireless sensor networks,” *IEEE/ACM Trans. Netw.*, vol. 15, pp. 346–358, 2007.

[11] A. Perrig, R. Szewczyk, V. Wen, D. E. Culler, and J. D. Tygar, “Spins: security protocols for sensor netowrks,” in *Proc. 2001 ACM MOBICOM*, pp. 189–199.

[12] B. Maala, Y. Challal, and A. Bouabdallah, “Hero: hierarchcal key management protocol for heterogeneous WSN,” in *Proc. 2008 IFIP WSAN*, pp. 125–136.

[13] W. Bechkit, Y. Challal, and A. Bouabdallah, “A new scalable key predistribution scheme for WSN,” in *Proc. 2012 IEEE ICCCN*, pp. 1–7.

[14] J. Zhang and V. Varadharajan, “Wireless sensor network key management survey and taxonomy,” *J. Netw. Comput. Appl.*, vol. 33, no. 2, pp. 63–75, 2010.

[15] S. A. C¸ amtepe and B. Yener, “Key distribution mechanisms for wireless sensor networks: a survey,” Technical Report TR-05-07, Mar. 2005.