IOSR Journal of Computer Engineering (IOSR-JCE)
e-ISSN: 2278-0661,p-ISSN: 2278-8727, Volume 16, Issue 5, Ver. VII (Sep – Oct. 2014), PP 121-124
www.iosrjournals.org

Providing efficient measurable key by using unital based key pre-distribution scheme for wireless sensor networks

A. Manoj kumar [1,] P. Jaya prakash[2,] Dr.M.Giri[3]
M.Tech Scholar[1], Assistant professor[2]
[1,2] Research Scholar in Vel Tech, Dr RR & Dr SR Technical University, Chennai.
[3]Professor & Head, Department of Computer Science and Engineering
Sreenivasa Institute of Technology and Management Studies Chittoor, Andhra Pradesh, India

Abstract: *Resource limitations and potential WSNs application and key management are the challenging issues for WSNs. Network scalability is one of the important things in designing a key management scheme. So we are proposed a new scalable key management scheme for WSNs; by this we will achieve a good secure connectivity. For this purpose we used one theory that is called Unital design theory. We have to show mapping from unital to key pre-distribution, by this mapping we will achieved high network scalability and sharing probability. So, that they have extended their work still more by finding another theory that is Unital based key pre-distribution scheme, by using this they achieved high network scalability and sharing probability. They had conducted some of the analysis and simulation and the results had been compared with that of the existing system, by using different criteria such as,*
1. Storage overhead
2. Network scalability
3. Network connectivity
4. Average secure path length
5. Network resiliency
So, the system had shown good network scalability and sharing probability.
Keywords: *Network scalability, Key management, secure connectivity, Unital Design, Sharing probability*

I. Introduction

Unital Design:

Resource limitations are challenging issues for WSNs. WSNs are suffering from reduced storage capacity. Due to this reason it is essential to develop some techniques. By implementing techniques they can build blocks of keys that are placed on the nodes to secure the network links. In the existing system they used key rings that are strongly related to network size. By using key rings they suffer from low scalability and degrade other performance metrics which include
1. Secure connectivity
2. Storage overhead.
So by this they had designed the Unital design theory which allowed to build the blocks with unique feature and which allowed
1. High scalability.
2. Network connectivity.

They explained the mapping from unital design to key pre-distribution and do not degrade the other performances. To achieve high scalability and network connectivity they have proposed another theory that is unital-based scheme.

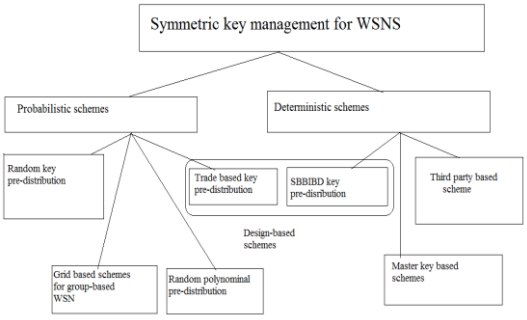
Unital:

In geometry, a unital is a set of n3 + 1 points arranged into subsets of size n + 1 so that every pair of distinct points of the set are contained in exactly one subset. $n \geq 3$ is required by some authors to avoid small exceptional cases.[1] This is equivalent to saying that a unital is a 2-(n3 + 1, n + 1, 1) block design. Some unitals may be embedded in a projective plane of order n2 (the subsets of the design become sets of collinear points in the projective plane). In this case of embedded unitals, every line of the plane intersects the unital in 1 or n + 1 points. In the Desargues an planes, PG (2, q2), the classical examples of unitals are given by non-degenerate Hermitian curves.

Classical unitals:

We give some terminology used in projective geometry. A correlation of a projective geometry is a bijection on its subspaces that come containment. In particular, a correlation exchanges points and hyperplanes.A correlation of arrangement two is called a polarity.A polarity is called nitary polarity if its combined with sesquilinearform s with companion automorphism α satisfies: $s(u,v) = s(v,u)\alpha$ for all vectors u, v of the particular vector space.A point is called absolute point of a polarity if it is on the image of itself under the polarity.Theabsolute points is a unitary polarity of the projective geometry PG(d,F), for some $d \geq 2$, is a nondegenerateHermitian variety, and if d = 2 this variety is called a nondegenerateHermitian curve.In PG(2,q2) for some prime power q, the set of points of a nondegenerateHermitiancurve form a unitalwhich is called a classical unital.Let be a non-degenerate Hermitian curve in for some prime power . As all non-degenerate Hermitian curves in the same plane are projectively equivalent, can be described in terms of homogeneous coordinates as follows:

II. System Architecture



Symmetric key management for WSNS:

Symmetric key management is divied into two types they are Probabilistic schemes and Deterministic schemes these are again divided four and three types they are

Probabilistic Schemes:

1.Random key pre-distribution.
2.Trade based key pre-distribution.
3.Random polynominal pre-distribution.
4.Grid based scheme.

Deterministic schemes:

1.SBBIB key pre-distibution.
2.Third party based scheme.
3.Master key based scheme.

Ree-unitals:

Another family of unitals, based on Ree groups was built by H. Luneburg.[6] Let Γ = R(q) be the Ree group of type 2G2 of order (q3 + 1)q3(q - 1) where q = 32m+1. Let P be the set of all q3 + 1 Sylow tree subgroups of Γ. Γ acts transitively on this set by conjugation. For any S and T in P, the pointwise on ΓS, T is cyclic of order q - 1, and thus it had a unique involution, μ. Each such involution fixes correctly q + 1 points of P. Built a block design on the points of P whose blocks are the fixed point sets of these various involutions μ. Since Γ acts transitively on P, this will be 2-design with parameters 2-(q3 + 1, q + 1, 1) called a Reeunital. Lüneburg also showed that the Reeunital scan not be embedded in projective planes of order q2 (Desarguesian or not) such that the auto Orphism group Γ is induced by a collineation group of the plane. For q = 3, Grüning proved that a Reeunitalcan not be embedded in any projective plane of order 9.

Isomorphic versus equivalent unitals:

Since unitals are block designs, the unitals are said to be isomorphic if there is a design same between them, a bijection between the point sets which maps blocks to blocks. This concept does not take into concerdationt the property of embed ability, so we say that unitals, embedded in the same ambient are equivalent if there is a collineation of the plane which maps one unital to the other.

Embeddable versus non-embeddable:

There are precisely four projective planes of order 9: the Desarguesian plane PG, the Hall plane of order 9, the dual Hall plane of order 9 and the Hughes plane of order 9. An exhaustive computer search by Penttila and Royle found 18 unitals (up to equivalence) with n = 3 in these four planes. Two in PG (2, 9), four in the Hall plane, and so other four in the double Hall plane, and eight in the Hughes plane. However, 1-unitals in the Hall plane is self-doubled, and so, gets counted again in the double Hall plane. Thus, there are 17 different embeddableunitals with n = 3. On the other hand, a non-exhaustive computer search found over 900 mutually nonsame designs which are unitals with n = 3.

Security Key pre-distribution in wireless sensor networks:

Key distribution is an important issue in wireless sensor network (WSN) design. It is a newly developed field due to the recent improvements in wireless communications. Wireless sensor networks are small, battery-powered, memory-constraint devices named sensor nodes points, which have the capability of wireless communication over a controlled area. Due to memory and power constraints, they have to be well arranged to build a fully functional network.

Security Key distribution schemes:

Key pre-distribution is the method of distribution of keys onto nodespoints beforedeployment. Therefore, the node points build up the network using their secret keys after deployment, when they reach their target position. Key pre-distribution schemes are various methods that have been developed by academicians for a better maintenance of key management in WSNs. Key pre-distribution scheme has three phases:

1. Key distribution
2. Shared key discovery
3. Path-key establishment

During these phases, secret keys are generated, placed in sensor node points, and each sensor node searches the area in its communication range to find another node to communicate. A secure link will be established when two nodes discover one or more common keys, and communication is done on that link between those two node points. After that paths are established connecting these links, to build a connected graph. Thefinal result is a wireless communication network functioning in its own way, according to the security key pre-distribution scheme used in creation. There are a number of aspects of WSNs on which key pre-distribution schemes are competing to achieve a better result. The most difficult ones are: local and global connection, and same. Local connectivity means chance that any two sensor node points have a common key with which they can establish a secure link to communicate. Global connectivity is the fraction of node points that are in the largest connected graph over the number of all nodes. Resiliency is the number of links that cannot be compromised when a number of nodes are compromised. So it is the quality of resistance against the attempts to hack the network. Other than these, two other critical issues in WSN design are computational cost and hardware cost. Computational cost is the amount of valuation done during these phases. Hardware cost is the cost of the memory and battery in each node points. There is a most-cited security keypredistribution scheme which is usually called "the main scheme" that introduced the ideas of random key pre-distribution, whereby the factor drastically improves resiliency.

Pre-distribution:

Pre-distribution (also written as Pre-distribution) is a neologism coined by Yale University Professor Jacob Hacker in a paper called The Institutional Foundations of Middle Class Democracy published by the think tank Policy Network. Pre-distribution is the idea that the state should try to prevent inequalities occurring in the first place rather than ameliorating inequalities through the tax and benefits system once they have occurred as occurs under redistribution. Associated with the Campaign for Co-operative Socialism including a set of five articles published in Winter 2009/2010 by 'The CCPA Monitor' and then, in May 2010, as a collection: 'CCPA Readings on Co-operative Socialism'. In addition, the term 'pre-distribution' has been used by authors James Robertson and Joseph Huber in the book, 'Creating New Money' and, then, in various publications.

Economic theory:

In the United Kingdom, Labour Party leader Ed Miliband has shown interest in the concept telling a Policy Network seminar at the London Stock Exchange that "Pre-distribution is about saying we cannot allow ourselves to be stuck with permanently being a low-product economy". The concept has seen as resulting from a recognition that were Labour to return to government they would not be able to reverse all Coalition cuts and implement traditional redistributive policies due to the poor state of the economy and instead need to focus on policies that make "work pay" for the poorest in society. Tristram Hunt, an influential Labour MP, called for

pre-distribution in his chapter in The Purple Book as a way to reform the economy whilst having fiscal restraint and fellow Purple Book contributor Rachel Reeves used the term in a June 2012 Progress article. Lord Wood of A field, an adviser to Ed Miliband, has argued that "pre-distribution" agenda is necessary because "In the face of rising inequality, coming down social mobility and standing real wages for middle-income earners, there are some restriction to what redistribution can achieve on its own". In an article in The Guardian, Hacker described the three major themes of pre-distribution in a UK environment: getting the macro economy right, particularly by encouraging long-term investment providing good quality public services, particularly healthcare and investing in skills of the young discovering new ways to control the market-economy, such as worker empowerment, steps beyond the minimum wage such as the right to know what co-worker groups earn, and the formation of worker groups other than unions.

Criticism:

There has been some criticism of whether pre-distribution is practical. BBC Political Correspondent Ian Watson argues that a pre-distributive policy might, for instance, require a business (when bidding for a government contract) to pay the living wage rather than the national minimum wage, something that may be difficult during times of austerity although Watson's argument has been countered by the independent Commission on Living Standards. Some commentators have gone so far as to suggest that the concept of pre-distribution has simply been invented, and lacks any real substance. Neil O'Brien, director of the conservative think tank Policy Exchange, criticized the term 'pre-distribution' as "the sort of stupid made-up word that only a policy wonk could love" before going on to say that the idea itself has merit.

III. Conclusion:

We proposed, in this work, a scalable key management scheme which ensures a good secure coverage of large scale WSN with a low key storage overhead and a good network communication resiliency. We make use of the theory unital design .we showed that a basic mapping from unitals to key pre-distribution allows to achieve high network scalability while giving allow direct secure connectivity coverage. We proposed then an efficient scalable unital-based key pre-distribution scheme pro-viding high network scalability and good secure connectivity coverage. We discuss the solution parameter and we propose adequate values giving a very good trade-off between network scalability and secure connectivity. We conducted analytical analysis and simulations to compare our new solution to existing ones, the results showed that our approach ensures a high secure coverage of large scale networks while providing good overall performances.

References:

[1]. J. M. Kahn, R. H. Katz, and K. S. J. Pister, “Next century challenges: Mobile networking for smart dust,” in Proceedings of the 5th Annual ACM/IEEE Internation Conference on Mobile Computing and Networking (MobiCom), 1999, pp. 483–492.
[2]. Hunt, T. 'Reviving our sense of mission: Designing a new political economy' in The Purple Book, R. Philpot (ed.), p. 65
[3]. BBC News - Ed Miliband unveils 'pre-distribution' plan to fix economy.
[4]. I.F. Akyildiz, W. Su, Y. Sankarasubramaniam, and E. Cayirci, "A survey on sensor networks", IEEE Communications Magazine, vol.40, no.8, pp. 102-114, August 2002.
[5]. L. Eschenauer and V.D.Gligor, "A key management scheme for distributed sensor networks", in Proceedings of the 9the ACM conference on Computer and communications security, Washington DC, USA, November 18–22, 2002, 41-47.
[6]. Assmus, Jr., E. F.; Key, J. D. (1992), Designs and Their Codes, Cambridge Tracts in Mathematics #103, Cambridge University Press, ISBN 0-521-41361-3
[7]. Barwick, Susan; Ebert, Gary (2008), Unitals in Projective Planes, Springer, doi:10.1007/978-0-387-76366-8, ISBN 978-0-387-76364-4.
[8]. WalidBechkit, YacineChallal, AbdelmadjidBouabdallah, and VahidTarokh-“ A Highly Scalable Key Pre-Distribution Scheme for Wireless Sensor Networks”- IEEE TRANSACTIONS ON WIRELESS COMMUNICATIONS, VOL. 12, NO. 2, FEBRUARY 2013
[9]. Y. Zhou, Y. Fang, and Y. Zhang, “Securing wireless sensor networks: asurvey,” IEEE Commun. Surv.Tuts., vol. 10, no. 1–4, pp. 6–28, 2008.
[10]. H. Chan, A. Perrig, and D. Song, “Random key predistributionschemesfor sensor networks,” in IEEE SP, pp. 197–213, 2003.
[11]. C. Castelluccia and A. Spognardi, “A robust key pre-distribution pro-tocol for multi-phase wireless sensor networks,” in Proc. 2007 IEEESecurecom, pp. 351–360.
[12]. S. Ruj, A. Nayak, and I. Stojmenovic, “Fully secure pairwise andtriple key distribution in wireless sensor networks using combinatorialdesigns,” in Proc. 2011 IEEE INFOCOM, pp. 326–330.