INTERNATIONAL JOURNAL OF RESEARCH
In Advanced Engineering Technologies

Volume 2, Issue 3 OCT 2014

KEY PRE-DISTRIBUTION USING UNITAL DESIGN FOR WIRELESS SENSOR NETWORK

[1] V. NARESH, [2] N.V. VINOD KUMAR

[1]M.Tech Student, Department of CSE.

vemananaresh554@gmail.com

[2]Assistant Professor, Department of CSE

vinnu.nukala55@gmail.com

ABSTRACT:

Key pre-distribution is a well-kenned technique for ascertaining secure communication via encryption among sensors deployed in an ad-hoc manner to compose a sensor network. . Sensor networks are commonly utilized for applications like environmental monitoring, airports safety, health care. The communication of a wireless sensor network can be captured quite facilely, thereby it require security. To achieve security in wireless sensor network, key pre-distribution is essential. To solve the key pre-distribution quandary, two elegant key pre-distribution approaches have been proposed recently.

In this paper, we propose an incipient key pre-distribution scheme, which substantially amends the resilience of the network compared to the subsisting schemes. Our scheme exhibits a nice threshold property: when the number of compromised nodes is less than the threshold, the possibility that any nodes other than these compromised nodes is affected is near to zero (0). This desirable property lowers the initial payoff of more diminutive scale network breaches to an adversary, and makes it necessary for the adversary to assail a significant proportion of the network. We withal present an in depth analysis of our plan in terms of network resilience and associated overhead.

Index Terms—Wireless sensor networks, security, key management, network scalability, resource optimization.

1. INTRODUCTION

Nowadays, wireless sensor networks (wsn) are increasingly utilized in numerous fields such as military, medical And industrial sectors; they are more and more involved In several sensitive applications which require sophisticated Security accommodations. Due to the resource constraints, subsisting security solutions for conventional networks could not Be utilized in wsn. So, the security issues became then one of The main challenges for the resource constrained environment of wsn. Key management is a corner stone accommodation For many security accommodations such as confidentiality and Authentication which are required to secure communications In wsn. The establishment of secure links between nodes Is then a conundrum in wsn. The public key Predicated solutions, which provide efficient key management Accommodations in conventional networks, are unsuitable for wsn Because of resource constraints. Some public key schemes Have been implemented on authentic sensors, however Most researchers believe that these techniques are still Too heavyweight over authentic sensors' technology because They induce a consequential communication and computation Overhead. Symmetric key establishment is then one Of the most congruous paradigms for securing exchanges in Wsn. Because of the lack of

infrastructure in wsn, we Have customarily no trusted third party which can attribute Pairwise secret keys to neighboring nodes, that is why most Subsisting solutions are predicated on key pre-distribution.The key establishment technique for a secure application must Minimally incorporate authenticity, confidentiality, integrity, Scalability, and flexibility.

1.1 Main contributions of our scheme

In this paper, we propose an incipient key pre-distribution scheme. The main contributions of this paper are as follows:

1. Substantially amended network resilience against node capture over subsisting schemes.

2. Pairwise keys that enable authentication.

3. Thorough theoretical analysis of security, and communication and computation overhead analysis.

Our scheme builds on Blom's key pre-distribution scheme and coalesces the arbitrary key pre-distribution method with it. Our results show that the resilience of our scheme is substantially more preponderant than Blom's scheme as well as other desultory key pre-distribution schemes. Blom proposed a key pre-distribution scheme that sanctions any dyad of nodes to find a secret pairwise key between them. Compared to the (N − 1)-pairwise-key pre-distribution scheme, Blom's scheme only utilizes λ+1 recollection spaces with λ much more minuscule than N. The tradeoff is that, unlike the (N − 1)-pairwise-key scheme, Blom's scheme is not impeccably resilient against node capture. Instead it has the following λ-secure property: as long as an adversary compromises less than or equipollent to λ nodes, uncompromised nodes are impeccably secure; when an adversary compromises more than λ nodes, all pairwise keys of the entire network are compromised. The threshold λ can be treated as a security parameter in that cull of a more immensely colossal λ leads to a more secure network. This threshold property of Blom's scheme is a desirable feature because an adversary needs to assail a significant fraction of the network in order to achieve high payoff. However, λ additionally determines the amount of recollection to store key information, as incrementing λ leads to higher recollection utilization. The goal of our scheme is to increment network's resilience against node capture without utilizing more recollection. Blom's scheme uses one key space for all nodes to ascertain that any dyad can compute its pairwise key in this key space. Motivated by the arbitrary key pre-distribution schemes presented in [11, 7], we propose an incipient scheme utilizing multiple key spaces: we first construct ω spaces utilizing Blom's scheme, and each sensor node carries key information from τ ($2 \leq \tau < \omega$) desultorily culled key spaces. According to Blom's scheme, if two nodes carry key information from a prevalent space, they can compute their pairwise key from the information; when two nodes do not carry key information from a mundane space, they can conduct key acquiescent via other nodes which portion pairwise keys with them. Our analysis has shown that utilizing the same amount of recollection, our incipient scheme is substantially more resilient than Blom's scheme and other key pre-distribution schemes.

2. BACKGROUND: UNITAL DESIGN

In combinatorics, the design theory deals with the existence and construction of systems of finite sets whose intersections have specified numerical properties. Formally, A t-design (v, b, r, k, λ) is defined as follows : Given a finite set X of v points (elements), we construct a family of b subsets of X, called blocks, such that each block has a size k, each point is contained in r blocks and each

$$\begin{pmatrix}
1 & . & . & . & . & 1 & 1 & . & . & . & 1 & . \\
. & . & . & . & . & 1 & . & 1 & 1 & 1 & . & . \\
. & . & 1 & 1 & . & . & 1 & 1 & . & . & . & . \\
1 & . & . & 1 & 1 & . & . & . & 1 & . & . & . \\
. & . & . & . & 1 & . & 1 & . & . & 1 & . & 1 \\
. & . & 1 & . & . & . & . & . & 1 & . & 1 & 1 \\
. & 1 & 1 & . & 1 & 1 & . & . & . & . & . & . \\
1 & 1 & . & . & . & . & . & 1 & . & . & . & 1 \\
. & 1 & . & 1 & . & . & . & . & . & 1 & 1 & .
\end{pmatrix}$$

Fig. 1. Example of incidence matrix of a 2-(9,3,1) hermitian unital

t points are contained together in exactly λ blocks. For instance, the Symmetric Balanced Incomplete Block Design (SBIBD) presented above is a (v, b, r, k, λ) design, where v = b = m2 + m + 1, r = k = m + 1 and λ = 1. A Unital design is a Steiner 2-design which consists of b = m2 (m3 + 1)/(m + 1) blocks, of a set of v = m3 + 1 points [21]. Each block contains m + 1 points and each point is contained in r = m2 blocks. Each pair of points is contained together in exactly one block. We note the Unital as a 2−design(m3+1, m2 (m3+1)/(m+1), m2 , m+1, 1) or as (m3 + 1, m + 1, 1) for

simplicity sake. Without loss of generality, we focus in this paper on Hermitian Unitals which exist for all m a prime power. Other construction for m not necessarily a prime power exist in literature [21]. Some Hermitian unital construction approaches were proposed in the literature [22] [23]. We refer in this paper to the construction proposed in [23]. A unital may be represented by its v × b incidence matrix that we call M. In this matrix, rows represent the points Pi and columns represent blocks Bj . The matrix M is then defined as:

$$M_{ij} = \begin{cases} 1 & \text{if } P_i \in B_j \\ 0 & \text{otherwise} \end{cases}$$

We give in figure 1 an incidence matrix of a 2-(9,3,1) hermitian unital. It consists of 12 blocks of a set of 9 points. Each block contains 3 points and each point occurs in 4 blocks. Each pair of points is contained together in exactly one block.

3. KEY PRE-DISTRIBUTION PHASE

During the key pre-distribution phase, we require to assign key information to each node, such that after deployment, neighboring sensor nodes can find a secret key between them. Assume that each sensor node has a unique identification, whose range emanates from 1 to N. We withal cull the security parameters τ, ω, and λ, where $2 \leq \tau < \omega$. These parameters decide the security and performance of our scheme, and will be discussed later in the paper. Our key pre-distribution phase contains the following steps: Step 1 (Generating G matrix): We first cull a primitive element from a finite field GF(q), where q is the most minuscule prime more immensely colossal than the key size, to engender an engenderer matrix G of size (λ+1)×N. Let G(j) represent the jth column of G. We provide G(j) to node j. albeit G(j) consists of (λ+1) elements, each sensor only needs to recollect one seed (the second element of the column), which can be habituated to regenerate all the elements in G(j). Therefore the recollection utilization for storing G(j) at a node is just a single element. Since the seed is unique for each sensor node, it can withal be utilized for node id. Step 2 (Generating D matrix): We engender ω symmetric matrices D1,. . ., Dω of size (λ + 1) × (λ + 1). We call each tuple Si = (Di, G), i = 1, . . . , ω, a key space. We then compute the matrix Ai = (Di • G) T . Let Ai(j) represent the jth row of Ai. Step 3 (Selecting τ spaces): We arbitrarily cull τ distinct key spaces from the ω key spaces for each node. For each space Si culled by node j, we store the jth row of Ai (i.e. Ai(j)) at this node. This information is secret and should stay within the node; under no circumstance should a node send this secret information to any other node. According to Blom's scheme, two nodes can find a mundane secret key if they have both picked a prevalent key space. Since Ai is an N × (λ + 1) matrix, Ai(j) consists of (λ + 1) elements. Therefore, each node needs to store (λ+ 1)τ elements in its recollection. Because the length of each element is equipollent to the length of secret keys, the recollection utilization of each node is (λ + 1)τ times the length of the key.

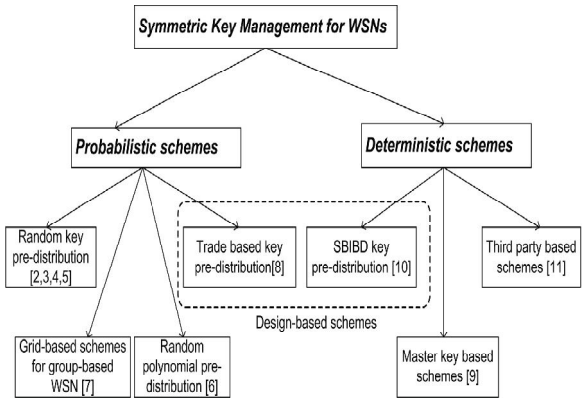

Fig2.system architecture

4. CONCLUSION & FUTURE WORK

We proposed, in this paper, an incipient highly scalable key pre-distribution scheme for WSN. We make use, for the first time, of the unital design theory. We showed that a

rudimentary mapping from unitals to key pre-distribution sanctions to achieve a profoundly high network scalability while degrading the key sharing probability. We proposed then an enhanced unital-predicated construction which gives birth to an incipient key management scheme providing high network scalability and good key sharing probability. We conducted analytic calculation and intensive simulations to compare our solutions to subsisting ones which showed that our approach enhances significantly the network scalability when providing good overall performances. As future work, we orchestrate to deepen the analysis of our parameter cull in order to suggest values given the best tradeoff. In integration, we attend to analyze more network performances of our solution like the network resilience against node capture attacks.

REFERENCES

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

[2] 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.

[3] 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.

[4] F. J. MacWilliams and N. J. A. Sloane. The Theory of Error-Correcting Codes. New York, NY: Elsevier Science Publishing Company, Inc., 1977.

[5] D. Malkhi, M. Reiter, A. Wool, and R. N. Wright. Probabilistic quorum systems. Information and Computation, (2):184–206, November 2001.

[6] B. C. Neuman and T. Tso. Kerberos: An authentication service for computer networks. IEEE Communications, 32(9):33–38, September 1994.

[7] H. Chan, A. Perrig, and D. Song, "Random key predistribution schemes for sensor networks".In Proc. of the IEEE Symposium on Security and Privacy, p. 197, 2003.

[8] D. Liu and P. Ning, "Establishing pairwise keys in distributed sensor networks," In Proc. ofthe 10th ACM CCS Conference, pp. 52 – 61. 2003

[9] W. Du, J. Deng, Y. S. Han, and P. K. Varshney. " A pair wise key pre-distribution scheme for wireless sensornetworks ". In Proc. of the 10th ACM CCS Conference, pp. 42– 51. 2003.

[10] Donggang Liu, PengNing, Wenliang Du, "Group Based Key Pre Distribution in Wireless Sensor Networks".

[11] Amos Fiat and Moni Naor. Broadcast encryption. In Advances in Cryptology – CRYPTO '93, volume 773 of Lecture Notes in Computer Science, 1994.