ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 2, Issue 4, April 2014

Analysis and Design of Various Key Pre-Distribution Schemes

Divya C [1], Jagannathan J [2] , Sathish Kumar C [3], Krishnan N [4]

Assistant Professor, Centre for Information Technology and Engineering, Manonmaniam Sundaranar University, India[1]

P.G. Student, Centre for Information Technology and Engineering, Manonmaniam Sundaranar University, India [2,3]

Professor, Centre for Information Technology and Engineering, Manonmaniam Sundaranar University, India [4]

ABSTRACT: The real emerging challenge in the field of Wireless Sensor Networks is to prevent sensor nodes by providing security and conserving scarce resources. Sensors are inexpensive, very low power devices which have limited resources and works on battery power. To provide security secret key plays a vital role, which is generated through some key pre-distribution schemes for providing a secure channels among sensor nodes in Wireless Sensor Networks. In this paper, we compare the proposed new key pre-distribution scheme called SHI-KPD Scheme with the existing key pre-distribution schemes based on some evaluation metrics such as resilience.

KEYWORDS*:* SHID, HASH, Poly Pool, SBIDB, TRADE-KP, WSN

I. INTRODUCTION

Wireless Sensor Networks are used in many real time applications such as environment monitoring, health monitoring, military applications, industrial monitoring, etc. Sensors are small in size, and have wireless communication range capability within short distances. A distinctive sensor node contains a sensing unit, power unit, a storage unit, a wireless transceiver and a processing unit. A WSN composed of large figure of sensor nodes with communication capabilities, computation, storage and limited power. Environments, where sensor nodes deployed are controlled such as home, office, warehouse, forest, etc. and uncontrolled such as hostile areas, disaster areas, toxic regions, etc. However, manual deployments become infeasible and even impossible as the number of the nodes increases. At a certain spots it is possible to provide denser sensors, but it may not be possible to control all the nodes. Thus, earlier the network topology cannot be defined exactly. Though the information of topology can be obtained by the way of sensor nodes and self-deployment protocols, for large scale wireless sensor network this may not be possible.

Six Security challenges in WSN are: (i) nature of Wireless communication, (ii) limitation of resource on sensor nodes, (iii) very dense and large WSN, (iv)lack of infrastructure fixed, (v) prior to deployment network topology is unknown, (vi) to unattended sensors high risk of physical attacks. In certain cases sensor nodes are require to operate under harmful condition. Security of such conditions is based on the efficient key pre-distribution scheme. To visit large amount of sensor nodes, and change their configuration in uncontrolled environments it is infeasible, or even impossible. In addition, using single shared key for the whole network may lead to obtain the key from the advisor. Thus, to establish the secure network, the sensor network must adopt the environment by using the pre-distributed keys, inorder to exchange the information with their immediate neighbors. In WSN Key distribution and management problem difficult one, and the new approaches are required. Motivation of this paper is to design the efficient key pre-distribution scheme and to compare it with the existing algorithms to prove that it is efficient than other schemes. This paper deals with related work in section II. The comparative study of various existing and proposed scheme with its performance analysis is made in section III. Finally it is concluded in section IV.

II.RELATED WORKS

The problems in Key management WSNs have been extensively studied in the literature and the key pre-distribution solutions have been compared with the proposed SHI-KPD's scheme.

Eschenauer and Gligor [1] proposed a random key pre-distribution scheme called RKP. In this scheme each node is pre loaded randomly with k keys from S pool. This scheme yields a high connectivity and not resilient against node capture since the capture of one node can compromise the whole network.

Chan et al. proposed in [2] a protocol called Q-composite scheme that enhances the resilience of RKP. Two nodes can establish a secure link only if they share at least Q keys. The pairwise session key is calculated as the hash function of: $K_{i,j}$ = Hash(K_{s1}||K_{s2}||…..||$K_{sq'}$) where K_{s1}, K_{s2}, ...$K_{sq'}$ are the q' shared keys between the two nodes i and j (q'≥ Q). This approach enhances the resilience against node capture attacks because the attacker needs more overlap keys to break a secure link.

Blom [3] proposed a λ-secure symmetric key generation system in which uses two matrices public G matrix and private A matrix, where G matrix are known to all adversaries and for each node a unique row from the private matrix A=(G.S) is allotted, where G,S be the public vandermone and secret symmetric matrix respectively. The pairwise keys are generated by $K_{i,j}=G.A^T$

Ruj et al. [5] proposed a Trade Based Key Management Scheme which consists a finite set X of v elements, a Steiner trade t − (v, k) is defined to be two disjoint groups $T_1$and T_2 of k-elements blocks of X such that each set of t elements from X occurs in exactly the same number of blocks of T_1 as of T_2. After deployment each node can establish a direct link if they share exactly two common keys which can be used for computing pairwise session key. And have proved that each pair of keys occur exactly two nodes in T_1 and T_2 respectively or no nodes.

Du et al. [6] proposed a scheme called enhanced random scheme assuming node before deployment knowledge. Every nodes are assigned with key from the regional key pools. The key pools are formed in a way that neighbouring keys from the corresponding key pool.

Camtepe and Yener [7] proposed key pre-distribution scheme named as Symmetric Balanced Incomplete Block Design (SBIBD). The proposed mapping from this scheme to key pre-distribution has to construct m^2+ m+1 key rings from a key pool S of m^2+ m +1 keys. The pairwise keys are generated by each contain k=m+1 keys.

III.COMPARATIVE STUDY

The key distribution scheme is used for the communication between the sensor nodes for the passing of information from the sensor node to the end user through wireless communication without interrupt from the external elements such node failure, from snoopers and more. So for preventing from the snoopers from the active and passive attacks we are going for an key distribution scheme by which the nodes can be prevented by generating keys for the key pre-distribution scheme. Thus the generated keys should not be captured by the attackers for solving these problems we propose a novel key pre-distribution scheme called SHID-KPD scheme for improving the resilience.

A. HASH FUNCTION ALGORITHM

In this scheme a part of original keys will be converted into derivate keys and they are assigned to every sensor before sensor nodes deployment. After the pairwise keys establishment between sensor nodes the original keys in every sensor nodes are then converted into derivative keys. Then all original keys will be then erased from the sensor memory. Because it is computational impossible to revert the Hash function, attackers can't get other sensor nodes information from any compromised sensor nodes.

Let the number of total captured sensor nodes be x. Hence, we have the probability P_b, that any secure link between two uncompromised sensor nodes is compromised when x sensor nodes have been captured is

$$P_b = 1-\left(1-\frac{t-s}{w}\right)^x \qquad (1)$$

Where t is the number of keys assigned to sensor nodes, s is the number of derivative keys in every sensor

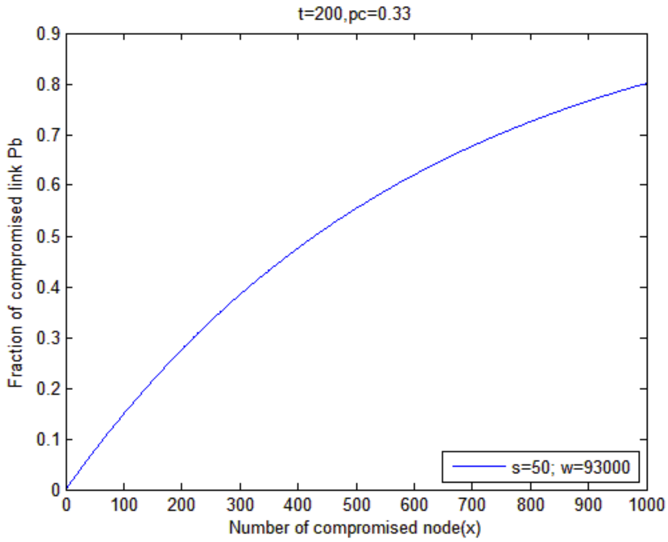

Fig.1 Resiliency of HASH Function Algorithm

Figure 1 shows the resiliency of the HASH Function algorithm during pairwise key establishing. The performance analysis of hash function is shown in figure 1. It is observed that if 500 nodes get compromised then P_b is 0.5.From this we understand that the resilience become stronger when the number of derivative key increase.

B. POLYNOMIAL POOL-BASED KEY PREDISTRIBUTION SCHEME

In polynomial pool-based key pre-distribution scheme the key setup server randomly generates bivariate t-degree polynomials with coefficients over a finite field GF(λ), where λ is a prime number large adequate to accommodate a cryptographic key.

A pool of |S| random bivariate polynomials, each with a unique id, namely, degree t, and a pool of $|S_k|$ random generation keys each with a unique identification. Prior to network deployment, for every sensor node u, the setup server randomly picks a subset of s polynomials out of $|S_p|$ and assigns polynomial shares of these s polynomials to the sensor node. In addition, for every sensor node u, the setup server randomly selects a subset of k(k<s) generation keys out of $|S_k|$ and assigns them to the sensor node u.

The poly pool-based key pre-distribution scheme uses the below equation for calculating the probability of resilience against the number of compromised node

$$R_x=\left(1-\frac{\binom{|S_p|}{2s}.\binom{2s}{s}}{\binom{|S_p|}{2s}^2}\right).\left(1-\frac{\binom{|S_k|-k}{m}}{\binom{|S_k|}{m}}\right) \qquad (5)$$

C. Symmetric BIBD

SBIBD is called Symmetric BIBD or Symmetric Design. The SBIBD has four properties:
1) Each block contains k=r objects
2) Every object occurs in r=k blocks
3) Every pair of objects occurs in λ block
4) Every pair of blocks intersects on λ objects.

The SBIBD scheme of order m, the network resiliency when x nodes are captured is

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 2, Issue 4, April 2014

$$R_x=\left(\frac{\binom{m^2}{x}}{\binom{m^2+m+1}{x}}\right) \quad (6)$$

D. Unital Design for Key Pre-Distribution in WSN

A Unital design is a Steiner t-design which consists of b = $m^2(m^2-m+1)$ blocks, of a set of v = m^3+1 points. Each block contains m + 1 points and each point is contained in r = m^2 blocks. Each pair of points is contained in exactly one block together. We denote the Unital by t-design(m^3+ 1, $m^2(m^2-m+1)$, m^2, m + 1, 1) or by (m^3+ 1, m + 1, 1)design for simplicity sake.

Unital scheme of order m, the network resiliency when x nodes are captured is

$$R_x=1-\sum_{i=1}^{t^2}(1-\left(\frac{\binom{m^3(m-1)}{x*t}}{\binom{m^2(m^2-m+1)}{x*t}}\right))^i\frac{p(i)}{P_c} \quad (7)$$

Let p(i) is the probability that two nodes share exactly i keys and that Pc is the probability that two nodes share at least one key.

Where

$$P_c=1-(1-\frac{(m+1)^2}{(m^3+m+1)})^{t^2} \quad (8)$$

$$p(i)=\binom{t^2}{i}(1-\frac{(m+1)^2}{(m^3+m+1)})^i*(1-\frac{(m+1)^2}{(m^3+m+1)})^{t^2-i} \quad (9)$$

E. Trade-KP.

The trade-based key management scheme denoted Trade-KP. Given a finite set X of v elements, a Steiner trade t − (v, k) is defined to be two disjoint sets $T_1$and T_2 respectively. The k-elements blocks of X and t elements from X occurs in precisely the same number of blocks of T_1 as those of T_2. This t elements from X is not repeated more than once in any of T_1 or T_2. The proposed scheme uses trade construction having q as prime power and k lies between ($4 \le k < q$). The constructed T_1 and T_2 blocks are represented by $t^1_{i,j}$= {(x, (xi + j) mod q) : $0 \le x < k$}, where $0\le i, j < q$, and T_2 represented by $t^2_{i,j}$= {(x, (x^2+ xi + j) mod q): $0 \le x < k$}, where $0 \le i, j < q$. Authors proved that the proposed construction results in a 2 − (qk, k) strong steiner trade. They proposed then a mapping to key pre-distribution where they associate to each element a distinct key and to each block of T_1 and T_2 a key ring. The key ring size is then equal to k and the scalability of the scheme is equal to $2q^2$.

The TRADE scheme uses the below equation for calculating the probability of resilience against the number of compromised node

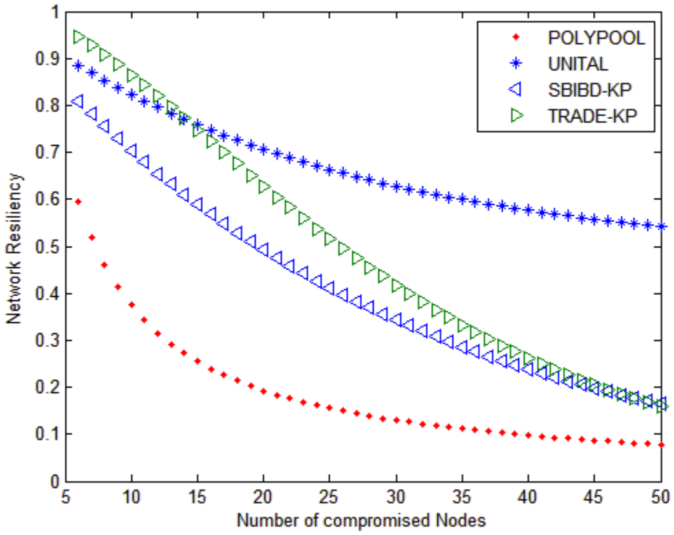

Fig. 2 Resiliency of the network of POLYPOOL, UNITAL, SBIDB, TRADE

$$R_x=\left(\frac{\binom{2q^2-4q+2}{x}+4(q-1)\binom{2q^2-4q+2}{x-1}}{\binom{2q^2}{x}}\right) \qquad (10)$$

Figure 2 explains the resiliency of the network against the number of compromised node for different key pre-distribution scheme such as POLYPOOL, UNITAL, SBIDB, TRADE scheme. Thus from this unital provides a better results while comparing to other schemes.

F. SHI-KPD Scheme (Proposed Scheme)

By using Symmetric, Hankel and Identity matrices for making the Pre-distribution scheme more secure between the sensor nodes by fasten methods we propose a fangled Pre-distribution scheme and named it as SHI-KPD scheme. Earlier the D (key space) is calculated using the product of S (private-symmetric) and I (vandermonde matrix-Public) but the proposed scheme uses square of Symmetric(private), Hankel (public) and Identity matrices on some mathematical combinations which is shown in equation (1) below inorder to make the computational more complex to improve security in generating key which is to be assigned in each sensor node for formation of secure link.

Generating matrix (D) =

$$\left(\frac{\mathrm{S} \times H)^T}{(S \times I)^T} \right) \qquad (11)$$

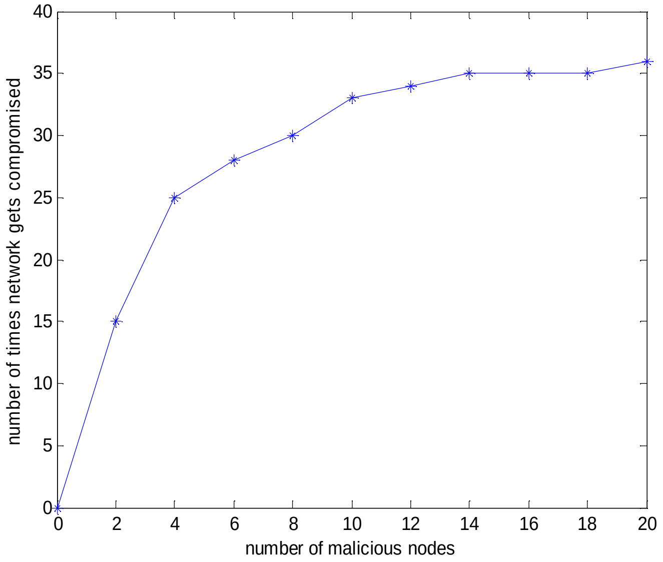

Fig. 3 Resiliency SHI-KPD Scheme

In general matrix K can be represented as shown below and we can notice that the symmetric nature gives the same key for any pair of nodes such that Kij = Kji

K= (D.H) mod 29
The keys are assigned to sensor nodes before deployment and it is changed periodically by safeguarding from attacks. Specifically it is used for military purpose.

The resiliency of the SHI-KPD scheme is shown in figure 3. It shows that number of malicious nodes is varied in x axis and the number of times the network gets compromised is performed. We infer that number of times the network gets compromised is around 36 for 20 malicious nodes.

IV. CONCLUSION

This paper presents the comparative study of Hash function, Polynomial Pool, SBIDB, UNITAL, TRADE algorithms with the proposed algorithm the new way of generating the keys using the SHI-KPD scheme. The proposed method has the advantage of increasing the resiliency and connectivity than the existing scheme. In addition, this scheme provides more complex in computation thereby increases security. The result of SHI-KPD scheme is compared with other existing schemes and it shows that SHI-KPD scheme achieves more resilience over the network.

REFERENCES

[1] Eschenauer, L., & Gligor, V. D. (2002, November). A key-management scheme for distributed sensor networks. In Proceedings of the 9th ACM conference on Computer and communications security (pp. 41-47). ACM.

[2] Chan, H., Perrig, A., & Song, D. (2003, May). Random key predistribution schemes for sensor networks. In Security and Privacy, 2003. Proceedings. 2003 Symposium on (pp. 197-213). IEEE.

[3] Blom, R. (1985, January). An optimal class of symmetric key generation systems. In Advances in cryptology (pp. 335-338). Springer Berlin Heidelberg.

[4] Ruj, S., Nayak, A., & Stojmenovic, I. (2011, April). Fully secure pairwise and triple key distribution in wireless sensor networks using combinatorial designs. In INFOCOM, 2011 Proceedings IEEE (pp. 326-330). IEEE.

[5] Du, W., Deng, J., Han, Y. S., Chen, S., & Varshney, P. K. (2004, March). A key management scheme for wireless sensor networks using deployment knowledge. In INFOCOM 2004. Twenty-third AnnualJoint Conference of the IEEE Computer and Communications Societies (Vol. 1). IEEE.

[6] Camtepe, S. A., & Yener, B. (2004). Combinatorial design of key distribution mechanisms for wireless sensor networks. In Computer Security–ESORICS 2004 (pp. 293-308). Springer Berlin Heidelberg.

[7] Shaila, K., Manjula, S. H., Thriveni, J., Venugopal, K. R., & Patnaik, L. M. (2011). Resilience Against Node Capture Attack using Asymmetric Matrices in Key Predistribution Scheme in Wireless Sensor Networks. International Journal on Computer Science & Engineering, 3(10).

[8] Subash, T. D., & Divya, C. (2011, December). Double hash function scheme in wireless sensor networks. In Information and Communication Technologies (WICT), 2011 World Congress on (pp. 88-92). IEEE.

[9] Subash, T. D., & Divya, C. (2011, March). Novel key pre-distribution scheme in wireless sensor network. In Emerging Trends in Electrical and Computer Technology (ICETECT), 2011 International Conference on (pp. 959-963). IEEE.

BIOGRAPHY

C. Divya Received M.E degree in Communication System in the year 2010 from SSN college of Engineering, Anna University, Chennai. She is currently working as an Assistant Professor in Centre for Information Technology and Engineering, Manonmaniam Sundaranar University, Tirunelveli, India. Awaiting for Ph.D Thesis Evaluation report on “Security Mechanisms on Wireless Sensor Networks” in Manonmaniam Sundaranar University. Her research interest is on Wireless sensor networks, QWFET and Remote Sensing. She is a member in various professional bodies like Association of Engineers.

J. Jagannathan was born in Kanchipuram, India in 1991. He received his Bachelors of Technology degree in Information and Communication Technology from Manonmaniam Sundaranar University, Tirunelveli, India in 2012. And he is currently pursuing the Masters of Technology degree in Information and Communication Technology from Manonmaniam Sundaranar University, Tirunelveli, India. His Research interests include Image Processing, Wireless Sensor Network, and QWFET transistors.

C. Sathish Kumar was born in Kanyakumari, India in 1990. He received his Bachelors of Technology degree in Information and Communication Technology from Manonmaniam Sundaranar University, Tirunelveli, India in 2012. And he is currently pursuing the Masters of Technology degree in Information and Communication Technology from Manonmaniam Sundaranar University, Tirunelveli, India. His Research interests include Image Processing, Wireless Sensor Network and Transistors.