International Journal of Application or Innovation in Engineering & Management (IJAIEM)
Web Site: www.ijaiem.org Email: editor@ijaiem.org
Volume 4, Issue 5, May 2015 **ISSN 2319 - 4847**

Key PreDistribution Model for Wireless Sensor Network

Miss. Snehal A. Zade[1] ,Dr. D. G. Harkut[2]

[1]M.E. (CSE) II Year,
Prof. Ram Meghe College of Engineering & Management, Amravati, India

[2]Department of Computer Science & Engineering,
Prof. Ram Meghe College of Engineering & Management, Amravati, India

ABSTRACT

The collection of spatially disseminated autonomous sensors with restricted resources that work together and supervise the physical or environmental conditions is a Wireless Sensor Network (WSN). These networks are prone to various kinds of attacks because of their operating nature. The establishment of secure links between nodes is a problem in WSNs. Key management is one solution but it has become a challenging issue in the design and deployment of secure WSNs. Because of resource limitations, symmetric key establishment is one of the most suitable paradigms for securing exchanges in WSNs. Symmetric schemes were mainly categorized into two categories such as probabilistic and deterministic schemes. As WSNs are highly resource constrained, they suffer from reduced storage capacity. So, it is essential to design smart technique to build blocks of keys that will embed on nodes to secure network links. But in most existing solution, the design of key rings is related to network size. This solution either suffers from low scalability or degrades other performance metrics including secure connection, storage overhead. This motivates the use of unital design theory that allows a smart building of blocks with unique feature that allow coping with scalability and connection issues. In contrast to these solutions, the goal is to enhance the scalability of WSN key management scheme without degrading the other network performances. To achieve this goal, a new scalable key management scheme for WSN which provides good secure connectivity coverage is proposed which make use of the unital design theory. Also the basic mapping from unitals to key predistribution allows achieving high network scalability. But this naive mapping does not guaranteed a high key sharing probability. So, an enhanced unital-based key distribution scheme providing high network scalability and good key sharing probability is proposed.

Keywords: Wireless Sensor Network, Key PreDistribution, Key Management, Unital Design Theory

1. INTRODUCTION

Typical sensor networks usually consist of a large number of ultra-small autonomous devices called as sensor nodes. Each sensor node is typically of low cost; battery powered, equipped with data processing, having storage capability and can communicate over a short range wireless network interface [1]. A Wireless Sensor Network (WSN) consists of spatially disseminated autonomous sensor to check physical on environmental environments like temperature, sound vibration, pressure, motion and humidity and to transmit their information through the network to the main location cooperatively [2][3]. WSN devices have severe resource constraints in terms of energy, computation and memory. These networks are prone to various kinds of attacks because of their operating nature. The establishment of secure links between nodes is a problem in WSNs. Key management is one solution over this problem. But it has become a challenging issue in the design and deployment of secure WSNs. The energy, computational and related communication limitations of sensor nodes make it impractical to use typical asymmetric cryptography to secure communication. Thus, symmetric key establishment is one of the most suitable paradigms for securing exchanges in WSNs [4].

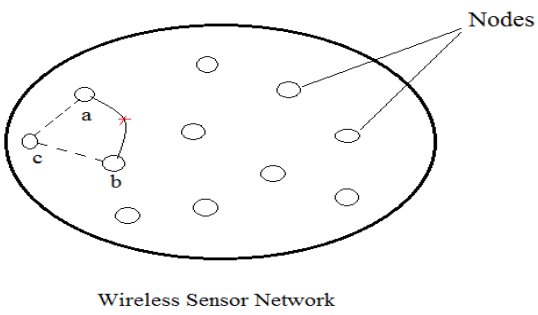

Figure 1 A typical Wireless Sensor Network

2. LITERATURE REVIEW

The key predistribution phase refers to task of distributing secret keys between communicating parties to provide secrecy and authentication. Random key predistribution schemes [28, 27, 23] are suggested using node deployment knowledge [22] for multi-phase WSNs [17] to address bootstrapping problem [25].
For reducing the storage overhead symmetric key predistribution systems are generated [32, 14, 8]. To enhance the security in WSN, pairwise key establishment is done [24, 15, 34, 33, 26]. Some of the techniques were based on the location of the nodes in a grid pattern [20, 19, 12, 21]. Further combinatorial method is used to generate the key in the network [18, 7, 6]. Many key predistribution techniques were depends on the groups form by the sensor nodes during deployment [11, 16, 13].

Table 1 Summary of Literature

Reference No., Author Name, Year	**Concept / methodology**	**Performance Evaluation**	**Claims by Author**	**Our Findings**
[5] Walid Bechkit, Yacine Challal, Abdelmadjid Bouabdallah, and Vahid Tarokh, 2013	Key predistribution using unital design theory	Good secure connectivity coverage, enhance network scalability, reduced storage overhead	Unital design helps to improve the security while reducing the storage overhead	Maintains other performance parameters as well
[6] Wangke Yu and Shuhua Wang, 2013	Key predistribution using combinatorial designs	High secure Connectivity, strong node capture resiliency, minimal memory consumption	Combinatorial designs as a tool for building key pre-distribution schemes is suitable for WSN environments	More computational cost
[11] Sushmita Ruj, Jennifer Seberry and Bimal Roy, 2009	Key Predistribution Schemes Using Block Designs	Large network coverage, more secure, better resiliency, low cost	Use of block design for KPD improves security	More computation overhead
[12] Simon R. Blackburn, Tuvi Etzion, Keith M. Martin, and Maura B. Paterson, 2008	Key Predistribution for Grid-Based WSN	No communication overhead	Grid based deployment provides better security	lower probability of establishing direct keys
[13] Donggang Liu, Peng Ning and Wenliang Du, 2008	Group-Based KPS Hash key-based scheme Polynomial-based scheme	Improved security	Achieve much better performance when the sensor nodes are deployed in groups.	Communication overhead
[17] C. Castelluccia and A. Spognardi, 2007	RoK Pre-distribution protocol for Multi-phase WSN	Improved security	Temporarily attacked network is able to automatically self-heal after an attack	More computation overhead
[22] W. Du, J. Deng, Y. Han, S. Chen, and P. Varshney, 2004	RKP using Node Deployment	improved network connectivity and resilience against node capture, reduced amount of memory required	Exploits deployment knowledge and avoids unnecessary key assignments	Less global connectivity and local resiliency, communication overhead
[26] Donggang Liu and Peng Ning, 2003	Establishing Pairwise Keys in Distributed Sensor Networks	High probability, tolerance of node captures, low storage, computation and communication	Presents an optimization technique for polynomial evaluation, which is used to compute	Less secured

		overhead	pairwise keys	

3. PROPOSED APPROACH

3.1 Block Schematic

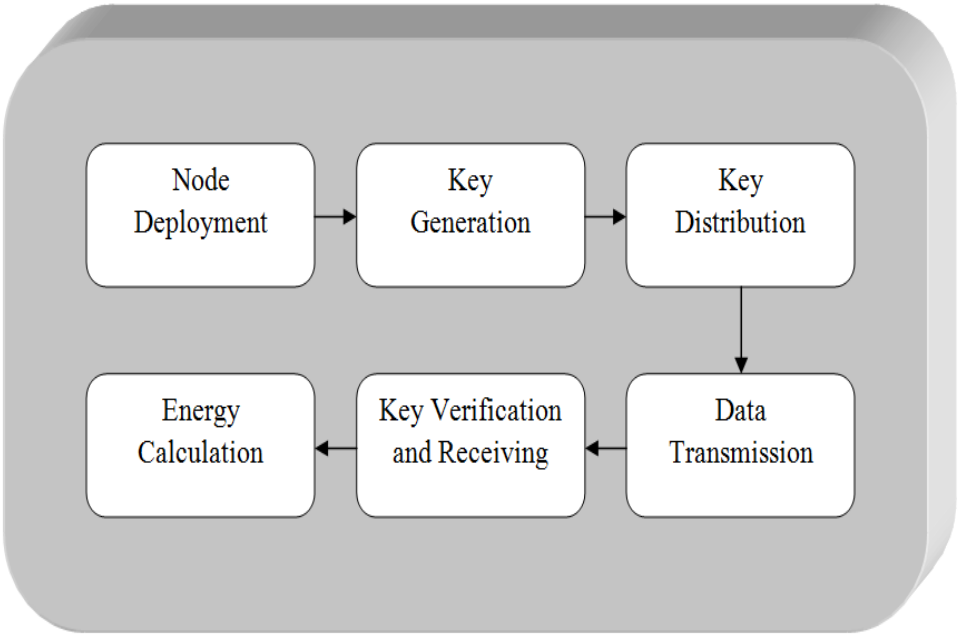

Figure 3 Block Diagram for proposed model

Node Deployment
The first module is Node deployment, where the node can be deployed by specifying the number of nodes in the network. After specifying the number of nodes in the network, the nodes are deployed. The nodes are deployed with unique ID (Identity) number so that each can be differentiated. And also nodes are deployed with their energy levels.

Key Generation
After the Node deployment module, the key generation module is developed where the number of nodes and number of blocks should be specified, so that the key will be generated. The key is symmetric key and the key is displayed in the text area given in the node.

Key Distribution
In this module, we generate blocks of m order initial design, where each block corresponds to a key set. We pre-load then each node with t completely disjoint blocks where t is a protocol parameter. In the basic approach each node is pre-loaded with only one unital block and we proved that each two nodes share at most one key. Contrary to this, pre-loading each two nodes with t disjoint unital blocks means that each two nodes share between zero and keys since each two unitals blocks share at most one element. After the deployment step, each two neighbors exchange the identifiers of their keys in order to determine the common keys. This approach enhances the network resiliency since the attackers have to compromise more overlap keys to break a secure link. Otherwise, when neighbors do not share any key, they should find a secure path composed of successive secure links.

Secure Transmission with Energy
In this module, the node distance is configured and then the nodes with their neighbor information are displayed. So the nodes which is near by the node, is selected and the energy level is first calculated to verify the secure transmission. After that the data is uploaded and sent to the destination node. Where in the destination node, the key is verified and then the data is received.

4.IMPLEMENTATION

4.1Flow of System

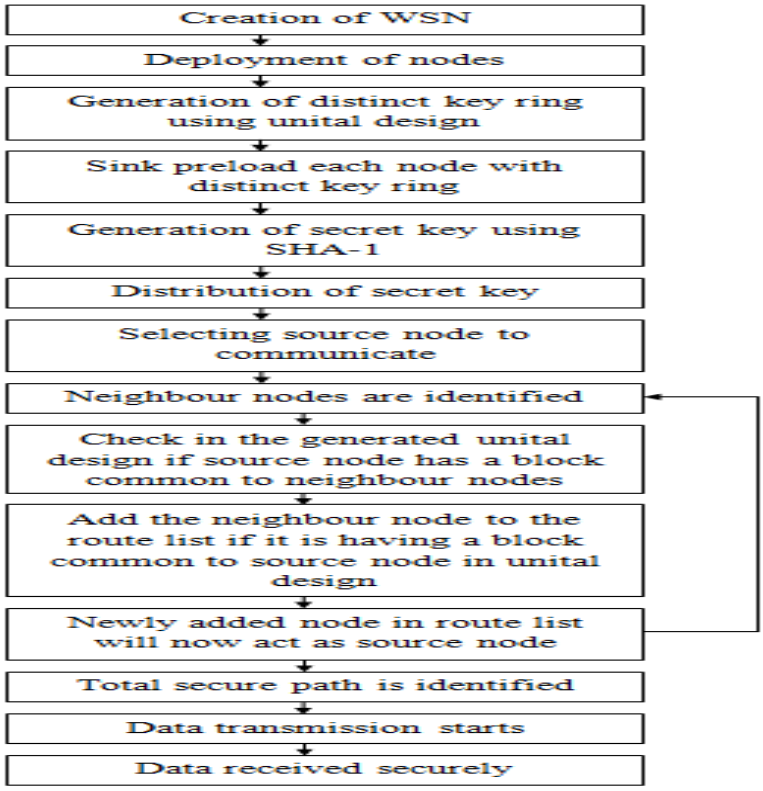

Figure 4.1 Working of proposed model

We implemented a new enhanced unital-based key pre-distribution scheme for WSN. At first, there is a creation of WSN environment by setting up the simulation parameters. Then creation of nodes and their configuration is done. There is an implementation of an algorithm for generating pairwise secure hash key named SHA-1 algorithm. In order to enhance the key sharing probability while maintaining high network scalability, we propose to build blocks using hermitian unital design and to pre-load each node with a number of blocks picked in a selective way. At the deployment step, we propose to generate blocks of m order unital design each block matches a key set. Now for communication, source node identifies its neighbouring node and shares its key identifier with them. If they share a common block then the neighbour node gets added to the route list. Like this a secure path is identified until we reach the sink and is used for data transmission. The aim of our construction is to enhance the key sharing probability between neighboring nodes and then decrease the average secure path length.

4.2Unital Design

A Unital design is a Steiner 2-design which consists of b = m2(m3+1)/(m+1) = m2(m2−m+1) blocks, of a set of v = m3 +1 points. Each block contains m+1 points and each point is contained in r = m2 blocks. Each pair of points is contained in exactly one block together. This Unital is denoted by 2−design(m3+1,m2(m2−m+1),m2,m+1, 1) or by (m3 + 1,m+ 1, 1) design for simplicity sake.

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:

$$M_{ij} = 1 \text{ if } P_i \in B_j$$
$$0 \text{ otherwise}$$

We have used 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.

We propose in algorithm 1 a random block distribution allowing to pre-load t disjoint blocks in each sensor node.

Generate B =< Bq >, key sets corresponding to blocks of a unital design of order m
For each Nodei do
KRi = {}
while ($|KRi| \leq t(m + 1)$) do
pick Bq from B
if ($(KRi \cap Bq) = \emptyset$) then
$KRi = KRi \cup Bq$

B = B − Bq
end
end
end
Algorithm 1: A random approach of unital block pre-distribution in the enhanced unital-based scheme

4.3SHA-1 Algorithm

SHA-1 algorithm consists of 6 tasks:
Task 1. Appending Padding Bits.
The original message is "padded" (extended) so that its length (in bits) is congruent to 448, modulo 512.
The padding rules are:

- The original message is always padded with one bit "1" first.
- Then zero or more bits "0" are padded to bring the length of the message up to 64 bits less than a multiple of 512.

Task 2. Appending Length.
64 bits are appended to the end of the padded message to indicate the length of the original message in bytes.
The rules of appending length are:

- The length of the original message in bytes is converted to its binary format of 64 bits. If overflow happens, only the low-order 64 bits are used.
- Break the 64-bit length into 2 words (32 bits each).
- The low order word is appended first and followed by the high-order word.

Task 3. Preparing Processing Functions.
SHA-1 requires 80 processing functions defined as:

f(t;B,C,D) = (B AND C) OR ((NOT B) AND D)	(0 <= t <= 19)
f(t;B,C,D) = B XOR C XOR D	(20 <= t <= 39)
f(t;B,C,D) = (B AND C) OR (B AND D) OR (C AND D)	(40 <= t <= 59)
f(t;B,C,D) = B XOR C XOR D	(60 <= t <= 79)

Task 4. Preparing Processing Constants.
SHA1 requires 80 processing constant words defined as:

K(t)= 0x5A827999	(0 <= t <= 19)
K(t) = 0x6ED9EBA1	(20 <= t <= 39)
K(t) = 0x8F1BBCDC	(40 <= t <= 59)
K(t) = 0xCA62C1D6	(60 <= t <= 79)

Task 5. Initializing Buffers.
SHA-1 algorithm requires 5 word buffers with the following initial values:
H0 = 0x67452301
H1 = 0xEFCDAB89
H2 = 0x98BADCFE
H3 = 0x10325476
H4 = 0xC3D2E1F0
Task 6. Processing Message in 512-bit Blocks.
This is the main task of SHA1 algorithm, which loops through the padded and appended message in blocks of 512 bits each. For each input block, a number of operations are performed. This task can be described in the following pseudo code:
Input and predefined functions:
M[1, 2, ..., N]: Blocks of the padded and appended message
f(0;B,C,D), f(1,B,C,D), ..., f(79,B,C,D): Defined as above
K(0), K(1), ..., K(79): Defined as above
H0, H1, H2, H3, H4, H5: Word buffers with initial value
Algorithm
For loop on k = 1 to N
(W(0),W(1),...,W(15)) = M[k] /* Divide M[k] into 16 words */
For t = 16 to 79 do:
W(t) = (W(t-3) XOR W(t-8) XOR W(t-14) XOR W(t-16)) <<< 1
A = H0, B = H1, C = H2, D = H3, E = H4

For t = 0 to 79 do:
TEMP = A<<<5 + f(t;B,C,D) + E + W(t) + K(t)
E= D, D = C, C = B<<<30, B = A, A = TEMP
End of for loop
H0= H0 + A, H1 = H1 + B, H2 = H2 + C, H3 = H3 + D, H4 = H4 + E
End of for loop
End of for loop

Output:
H0, H1, H2, H3, H4, H5: Word buffers with final message digest

4.4Protocol Used

Destination sequenced distance vector routing (DSDV) is a modification of the conventional Bellman-Ford routing algorithm. It is adapted from the conventional Routing Information Protocol (RIP) to sensor networks routing. It adds a new attribute, sequence number, to each route table entry of the conventional RIP. Using the newly added sequence number, the mobile nodes can distinguish stale route information from the new and thus prevent the formation of routing loops. It addresses the drawbacks related to the poor looping properties of RIP in the face of broken links. The modification adapted in DSDV makes it a more suitable routing protocol for sensor networks.

4.5Network Simulator (NS)

Network simulator 2 is used as the simulation tool in this project. NS was chosen as the simulator partly because of the range of features it provides and partly because it has an open source code that can be modified and extended.

5.EXPERIMENTAL RESULTS AND DISCUSSION

5.1Results

In this section, we compare the implemented unital-based scheme to existing schemes regarding different criteria. We have generated some graphs for different evaluation parameters and found out that as compared to existing system, communication cost, energy consumption and delay in network for our implemented system is less.

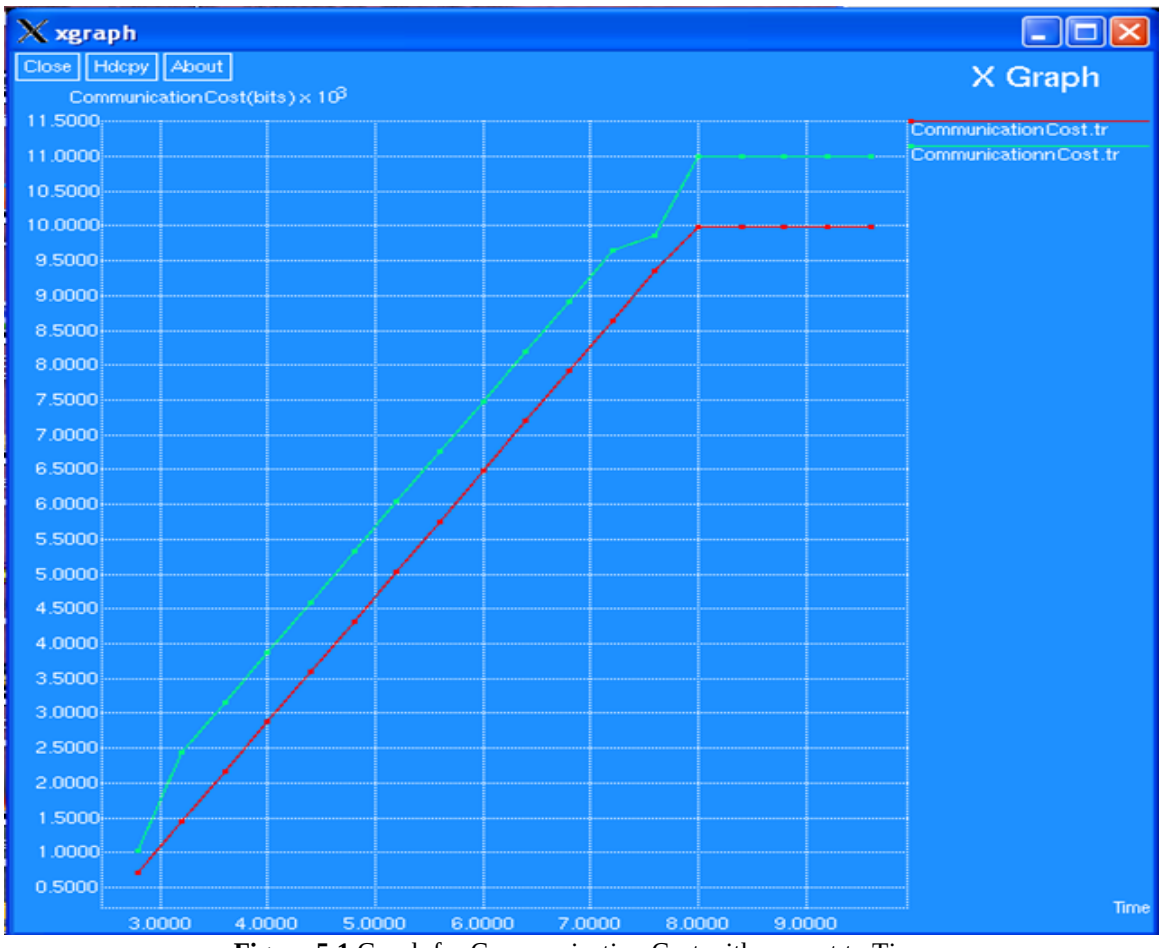

Figure 5.1 Graph for Communication Cost with respect to Time

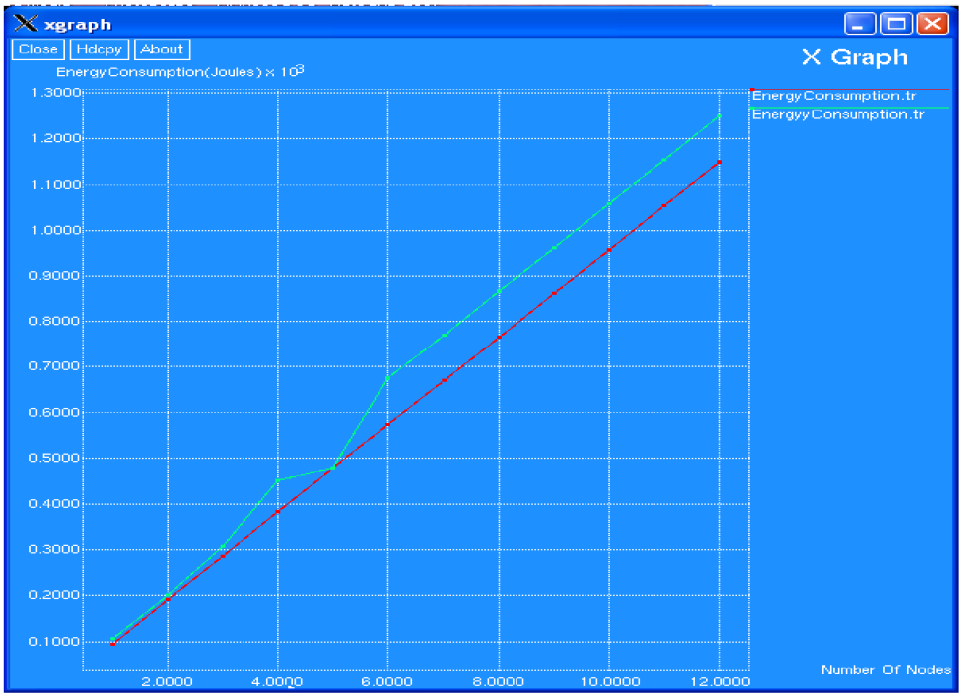

Figure 5.2 Graph for Energy Consumption with respect to Number of Nodes

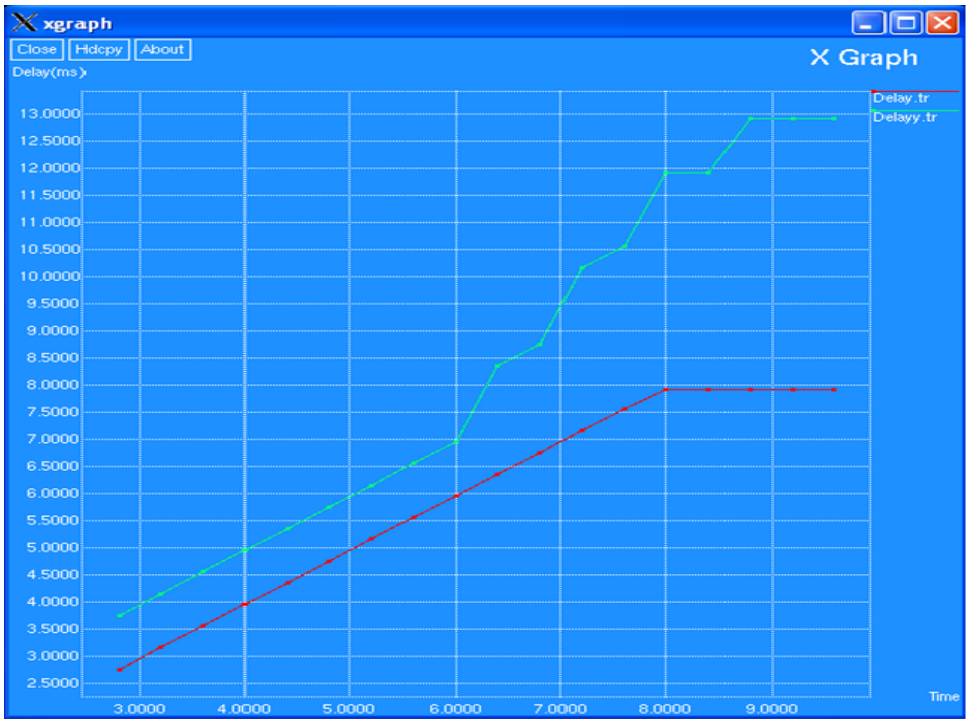

Figure 5.3 Graph for Delay with respect to Time

5.2Evaluation Parameters

Table 5.1 Evaluation parameter comparison

Parameters	**Proposed Approach**	**Q-composite Random Key PreDistribution Scheme**	**Random Perturbation-Based Scheme for Pairwise Key Establishment**
Key ring size	Due to the use of unital design, key ring size get independent of the network size	Key ring size depends on the network size	----
Key storage overhead	Overhead of storing	----	Low storage

	keys for all nodes get reduced		requirement
Secure connectivity coverage	Provides more secure network connectivity	Achieves significantly improved security under small scale attack	Maintains security even if some nodes get compromised
Network resiliency	Provides high network resiliency	Possesses perfect resilience against node capture attacks	Network resiliency is on average
Computational overhead	Low computational overhead	High computational overhead	Low computational overhead

6.CONCLUSION AND FUTURE SCOPE

6.1Conclusion

We have implemented an efficient key management scheme which ensures a good secure coverage of WSN with a low key storage overhead. We make use of the unital design theory for this purpose. We showed that a basic mapping from unitals to key pre-distribution allows to achieve high network scalability while giving low direct connectivity coverage. We proposed then an efficient unital-based key predistribution scheme providing high network scalability and good secure connectivity coverage. We then compare our solution with some of the existing methods and found out that our system provides high secure network coverage with low storage overhead and reduced computation cost. Our system provides secured communication in WSN without degrading other performance parameters.

6.2Future Scope

Our system is implemented for static WSN. In future we can extend it to the dynamic WSN. For implementation purpose we are restricting the number of nodes to 13 while in future we can implement it for large number of nodes.

References

[1] Wenliang Du, Jing Deng, Yunghsiang S. Han, Shigang Chen, and Pramod K. Varshney, "A Key PreDistribution Scheme for Sensor Networks Using Deployment Knowledge", IEEE Transactions on Dependable and Secure Computing, Vol. 3, No. 1, January-March 2006.

[2] Irfanullah Khan, Faheem Khan, Lala Rukh, Zaidullah and Yasir Ali, "A Survey about Security of the Wireless Sensor Network", International Journal of Computer Science and Telecommunications, Volume 3, Issue 7, July 2012.

[3] Clare, Loren P., Gregory J. Pottie, and Jonathan Agre, "Self-Organizing Distributed Sensor Networks", Proc. SPIE Aero-sense 99, 1991.

[4] Walid Bechkit, Yacine Challal, Abdelmadjid Bouabdallah, "A new scalable key predistribution scheme for WSN", IEEE ICCCN, pp. 1–7, in Proc. 2012.

[5] Walid Bechkit, Yacine Challal, Abdelmadjid Bouabdallah, and Vahid Tarokh, "A Highly Scalable Key PreDistribution Scheme for Wireless Sensor Networks", IEEE Transactions on Wireless Communications, Vol. 12, No. 2, February 2013.

[6] Wangke YU and Shuhua WANG, "Key pre-distribution using combinatorial designs for wireless sensor networks", E-ISSN: 2224-2880, Volume 12, Issue 1, January 2013.

[7] Maura B. Paterson and Douglas R. Stinson, "A Unified Approach to Combinatorial Key PreDistribution Schemes for Sensor Networks", January 7, 2012.

[8] Adrian Herrera and Wen Hu, "A Key Distribution Protocol for Wireless Sensor Networks", LCN Proceedings of IEEE 37th Conference on Local Computer Networks, Pages 140-143, 2012.

[9] Taehwan Choi, H. B. Acharya, and Mohamed G. Gouda, "The best keying protocol for sensor networks", IEEE WOWMOM, pp. 1–6, in Proc. 2011.

[10] A. Jemai, A. Mastouri and H. Eleuch, "Study of key predistribution schemes in wireless sensor networks: case of BROSK (use of WSNet)", Applied Mathematics & Information Sciences–An International Journal 5(3), 655-667, 2011.

[11] Sushmita Ruj, Jennifer Seberry and Bimal Roy, "Key PreDistribution Schemes Using Block Designs in Wireless Sensor Networks", International Conference on Computational Science and Engineering, 2009.

[12] Simon R. Blackburn, Tuvi Etzion, Keith M. Martin, and Maura B. Paterson, "Efficient Key PreDistribution for Grid-Based Wireless Sensor Networks", Information Theoretic Security Lecture Notes in Computer Science, Volume 5155, pp 54-69, 2008.

[13] Donggang Liu, Peng Ning and Wenliang Du, "Group-Based Key PreDistribution for Wireless Sensor Networks", ACM Transactions on Sensor Networks, Vol. 4, No. 2, Article II, March 2008.

[14] Yun Zhou and Yuguang Fang, "A Two-Layer Key Establishment Scheme for Wireless Sensor Networks", IEEE Transactions on Mobile Computing, Vol. 6, No. 9, September 2007.
[15] Wensheng Zhang, Minh Tran, Sencun Zhu and Guohong Cao, "A Random Perturbation-Based Scheme for Pairwise Key Establishment in Sensor Networks", MobiHoc Proceedings of the 8th ACM international symposium on Mobile ad hoc networking and computing, Pages 90-99, 2007.
[16] Sushmita Ruj and Bimal Roy, "Key PreDistribution Using Partially Balanced Designs in Wireless Sensor Networks", ISPA, LNCS 4742, pp. 431–445, 2007.
[17] C. Castelluccia and A. Spognardi, "A robust key predistribution protocol for multi-phase wireless sensor networks", IEEE Securecom, pp. 351–360, in Proc. 2007.
[18] Seyit A. Camtepe, Bulent Yener, "Combinatorial design of key distribution mechanisms for wireless sensor networks", IEEE/ACM Trans. Netw., Vol. 15, pp. 346–358, 2007.
[19] R. Kalindi, R. Kannan, S. S. Iyengar and A. Durresi, "Sub-Grid based Key Vector Assignment: A Key PreDistribution Scheme for Distributed Sensor Networks", Journal of Pervasive Computing and Communications, Vol. 2, No. 1, March 2006.
[20] Haowen Chan and Adrian Perrig, "PIKE: Peer Intermediaries for Key Establishment in Sensor Networks", INFOCOM, 24th Annual Joint Conference of the IEEE Computer and Communications Societies. Proceedings IEEE Vol. 1, Pages 524 – 535, 2005.
[21] Yun Zhou, Yanchao Zhang, and Yuguang Fang, "Key Establishment in Sensor Networks based on Triangle Grid Deployment Model", Military Communications Conference (MILCOM), IEEE, Vol. 3, Pages1450 – 1455, 2005.
[22] W. Du, J. Deng, Y. Han, S. Chen, and P. Varshney, "A key management scheme for wireless sensor networks using deployment knowledge", IEEE INFOCOM, pp. 586–597, in Proc. 2004.
[23] Joengmin Hwang and Yongdae Kim, "Revisiting Random Key PreDistribution Schemes for Wireless Sensor Networks", SASN, Proceedings of the 2nd ACM workshop on Security of ad hoc and sensor networks, Pages 43 – 52, 2004.
[24] Wenliang Du, Jing Deng, Yunghsiang S. Han and Pramod K. Varshney, "A Pairwise Key PreDistribution Scheme for Wireless Sensor Networks", CCS, Washington, DC, USA, October 27–30, 2003.
[25] Haowen Chan, Adrian Perrig and Dawn Song, "Random key predistribution schemes for sensor networks", in IEEE SP, pp. 197–213, 2003.
[26] Donggang Liu and Peng Ning, "Establishing pairwise keys in distributed sensor networks", ACM CCS, pp. 52–61, in Proc. 2003.
[27] Sencun Zhu, Sanjeev Setia and Sushil Jajodia, "Leap: efficient security mechanisms for large-scale distributed sensor networks", ACM CCS, pp. 62–72, in Proc. 2003.
[28] Laurent Eschenauer and Virgil D. Gligor, "A key-management scheme for distributed sensor networks", ACM CCS, pp. 41–47, in Proc. 2002.
[29] Adrian Perrig, Robert Szewczyk, Victor Wen, David Culler, J. D. Tygar, "Spins: security protocols for sensor networks", ACM MOBICOM, pp. 189–199, in Proc. 2001.
[30] Antoine Joux, "A One Round Protocol for Tripartite Diffie-Hellman", ANTS-IV, LNCS 1838, pp. 385-393, 2000.
[31] Carlo Blundo, "Perfectly Secure Key Distribution for Dynamic Conferences", Advances in cryptology—CRYPTO'92, 471-486, 1993.
[32] Rolf Blom, "An optimal class of symmetric key generation systems", Eurocrypt Workshop Advances Cryptology: Theory Appl. Cryptographic Techniques, pp. 335–338, in Proc. 1985.
[33] Donggang Liu and Peng Ning, "Improving Key PreDistribution with Deployment Knowledge in Static Sensor Networks", ACM Journal Name, Vol. No. 20, Pages 1–32.
[34] Donggang Liu, Peng Ning and Rongfang Li, "Establishing Pairwise Keys in Distributed Sensor Networks", ACM Journal Name, Vol., No., 20.

AUTHOR

Snehal A. Zade received B.E. (Computer Science & Engineering) from SGB Amravati University in 2013 and pursuing M.E. (Computer Science & Engineering) from SGB Amravati University.

Dinesh G Harkut received B.E. (Computer Science & Engineering) & M.E. (Computer Science & Engineering) from SGB Amravati University in 1991 and 1998 respectively. He completed his masters in Business Management and obtained his Ph.D. from SGB Amravati University in Business Management in 2013 while serving as a full-time faculty in the Dept. of Computer Science & Engineering at Prof Ram Meghe College of Engineering & Management, Badnera – Amravati. His research interests are Embedded Systems and RTOS.