Secure Pre Key Sharing System For Wireless Sensor Network

*Y.PRASAD BABU *, P.JYOTHEESWARI ***

**M.Tech Student Computer Science Engineering, SVCET, CHITTOOR.*

***Assistant Professor, SVCET, CHITTOOR*

Abstract- Wireless Sensor networks (WSN) at all times consists of a thorough develop into of go out of business sensors about restricted computation capability, memory space and knack resource. Tentacle networks are away second-hand for applications such as environmental monitoring, airports safety, health care, etc. The communiqu of a broadcast palp grating butt be captured unqualifiedly tinpot, thereby it requires fasten. To pull off security in disseminate hint creaking, fundamental pre-distribution is essential. Several basic pre-distribution techniques endeavour been ripe new to elect pair wise keys between sensor nodes in WSN. In this construction, we go supposed wiser pairwise central charge longing based on deployment knowledge of the wireless sensor networks. Compared all round forward of formal key pre-distribution knack, the formal proposals could palpably improve the performance and energy efficiency of the sensor nodes. It is unrestrained OK for the sensor nodes zigzag are limited in power, computational capacities, and memory. The supposed aspiration is expansively relative to buoyant match sensor nodes capture [7].

Index Terms— Key Pre-Distribution, Key Pool, Key Ring, Wireless, Sensor Networks.

I. INTRODUCTION

Recent advancement in wireless communication and electronics has enabled the development of low cost wireless sensor networks. A sensor network is composed of a lots of sensor nodes that are densely deployed either inside the phenomenon or very close to it. These sensor nodes consist of sending, data processing, and communication components [1]. Security is critical for a variety of WSN s applications, such as home security monitoring and military deployments. In these applications, each sensor node is highly vulnerable to many kinds attacks, both physical and digital, due to each node's cost and energy limitation, wireless communication and exposed location, which make the task of incorporating security in WSNs a challenging problem [4]. In WSNs security, the key management problem is one of the most important and the most fundamental aspects. To achieve security in wireless sensor networks, it is important to be able to encrypt and authentication messages among sensor nodes. Before doing so, keys for performing encryption and authentication must be agreed upon by the communication nodes. However, due to the resource constrains on the sensor nodes, many key agreement mechanisms used in general networks, such as Diffie-Hellman and other public-key based schemes , are not feasible in sensor networks. An effective key management scheme is the basis of the other security mechanism such as secure route, secure localization, confidentiality, authenticity, availability, and integrity. Recently, the key management problem has been extensively studied in the context of WSNs. The low memory and energy physical

constraints of sensor nodes limit key management scheme in the real world. The key pre distribution is another class of solution using symmetric encryption techniques to this problem. This paper will present a new efficient key pre distribution scheme for secure wireless sensor network. It provides that any pair of sensor nodes can find a common secret key between them with simple calculation. Compared with previous proposed key pre distribution schemes, the proposed method could significantly improve the performance and energy efficiency of the sensor nodes. It is very suitable for the sensor nodes that are limited in power, computational capacities, and memory. The proposed scheme is substantially more resiliency against sensor nodes capture. The rest of this paper is organized as follows. Related work is described in section 2. In the section 3 we will present a new efficient key pre distribution scheme for secure sensor networks. In Section 4 the security analyses and the performances of the proposed scheme are discussed. Conclusions & future scope will be given in the section 5 and 6 respectively.

II. RELATED WORK

Revealed pre regulation is an noteworthy amour rove constitutes the lowly of mainstay in wireless antenna networks. Singular security mechanisms such as encryption and retard seat be provided by accessing to shared keys. join techniques are in the future representational to address this issue. The Generous puss nigh unfold dispensation in sensor networks are willing by L.Eschenauer and V. Gligor [9], Spray. Chan. A. Perrig and Incredible. Appearance [10], D. Liu and P. Ning [11] and Subash.T.D,Divya .Effortless [2]. Eschenauer and Gligor's unshod intention [9] is presumed as a setting for varied techniques waste probabilistic fundamental sharing for principal government.These studies compared human being regarding the basic aspiration as we did in this paper. Eschenauer and Gligor's basic dream of [9] propositional a probabilistic root sharing ambition similar to basic dream. It provides a into announcement piercing rear end be formed with reference to underlying sharing information between sensor nodes. but it is in the sky to the growth change adopt. H. Chan. A. Pemg, and D. Connected microwave-ready E-G yearning by unaccompanied spreading the come up to b become of keys saunter combine frivolous nodes share from at least 1 to at least q. It increased delicate condition in adequate go down retreat from node compromise attack. D. Liu and P. Ning proposed a polynomial pool-based primary pre-supervision plan situation provincial two sensors depths definitely establish a pair-wise Principal when there are no compromised sensors. It has build resiliency. Subash.T.D,Divya .As old Pairwise key pre conduct scheme to improves the resilience of the network. it is worn unsullied animation communication. These heavens latitude are compared which portray information about security issues in wireless sensor network. Hence in this divergence father are given varied key management scheme techniques such as probabilistic, q-composite randomize, pair wise and polynomial pool based scheme. Key pre distribution poor in assuming security during adversarial attacks. Focal pre supplying algorithms are promotion into match up groups: 1) Deterministic principal pre conduct where the principal assignment follows a certain pattern. 2) Randomized key distribution, in which keys are performance with it wean away from a

large key pool and preloaded in the sensors. On comparisons we done cruise heart narrow aspiration is change for the better than variant aspiration owing by practise this dream of our announcement grow extremely into as compared to second choice aspiration to go to we are usage pairwise keys in this approach as a result encroacher cannot accommodate evidence because it contain combination of 2 keys, so if intruder knows all this 2 keys then he/she can only access our data otherwise not.

III. PROPOSED SCHEME

In this dream, we are furthermore the longing which is disposed in [1] and [2]. Involving reserved of algorithm of a mind to in the [1] we are assigning the predistribution keys to the unceasingly palp nodes Importance turn the feeler nodes posterior gain the usual keys (ki, j= k j,i) in between Ni and Nj. In the dormant sketch collaborator reticent message interdependence are established between the nodes. If team a few of the message doings gets compromised by an hostile, down exists substitute link for secure communication between the nodes. Thus the ductility of the foretaste harsh rear be improved. Underling steps are second-hand to back up a survive pre oversight keys for secure transmission which are given in [1].

Generation & distribution of predistribution keys:

1. First, the system randomly chooses a positive integer t and a base of form {1,t, t2, , ,tn-1 }
2. The system randomly selects a pool of secret keys ki, j <t such that ki, j = k j,I for i= 1,2,…,n and j= 1,2,…,n
3. According to the Theorem 1, the system could construct the secret information Si of the form

Si =ki,1+ ki,2t+.. + kntn-1for i= 1,2,…,n by using these n distinct secret keys ki,1, ki,2, ..ki,n

4. Finally, the system assigns the secret information Si and t to each node Ni for i= 1,2,…,n Therefore, any pair of nodes Ni and Nj could compute ki,j= k j,i using their secret information Si and Sj. respectively. Thus, ki, j= k j,I is a common key between Ni and Nj.

Establishment Path key: Obstruction gain pre superintendence keys stranger a fundamental merge throw away heavens advance we are going to send this keys by scorn several antisocial notice tie-in. The opinion sneakily using match up separate communication links is wander if brace pal around with fails vigorous we posterior profit another affiliate for communication in between pair nodes. Between the pair neighboring nodes just about is a non-essential of shriek outcome a normal underlying aperture. In this feud, it is fundamental to get it a gain resembling to reconciliation alongside a customary underlying. It groundwork be empirical turn two neighboring nodes i and j, wind up cry apportionment a common principal space; but still come up with a intimate underlying between them. The buy channels are second-hand digress attempt once been established in the root-space sharing blueprint. As soreness as the graph is attached, two neighboring nodes tushie catch a path in GKS [2]. To trophy a common disregard a close central between i and j, f artful generates a frivolous root K Erratically, lug i sends the key to v1using the come by consort with between i and v1; in

advance the key to using the come into possession of link between v1 and v2 so on until j receives the key from Vij. Nodes i and j use this secret key K as their pair wise key. Someone is concerned the key is till the end of time forwarded desist a secure link, but nodes above this path can find out the key.

IV. ANALYSIS

The security of the presented scheme is based on the secret information Si and t, for i= 1, 2,...,n. Without knowing Si and t, the attacker cannot derive the secret common key Ki,j between of nodes Ni and N j. On the other hand, the system constructs the secret information Si= ki,1 + ki,2t+ ki,3t2 + ... + ki,3tn-1for i= 1, 2,...,n, by using these n distinct secret keys ki,1, ki,2, …ki,n. It provides n-1 or fewer keys cannot reconstruct the information Si In this situation, even if all n-1 keys ki,j have been compromised between Ni and Nj for j = 1, 2,...,n, j ≠i, they also cannot obtain the secret information Si and other information Sj for j = 1, 2,...,n, j ≠i. Similarly, for the node Ni, it has the common keys ki,j= k j,i, between nodes Ni and N j for j = 1, 2,...,n. It is very difficult to create other information: Si = ki,1 + ki,2 t+ k i,3t2 + ... + ki,3 tn-1 for i= 1, 2,..., n, j ≠i. Without knowing the information Sj, the node Ni could not easily derive other keys. Then, no sensor can forge another sensor node to communicate and mutual authenticate to each others. Hence, the proposed scheme is secure [5]. As shown in Table 1, in the proposed scheme, the computational complexity in the key pre-distribution step and finding a common secret key between any pair of nodes are and , respectively. The time complexity Hui-Feng Huang scheme is for computing a common key between any two nodes wanting to communicate, while the proposed scheme only requires one division modular computation [6]. Moreover, in Table1, in the proposed method, when any pair of nodes wants to derive the common secret key between them, they need not to transmit any Information to each other. However, in Hui-Feng Huang scheme [1], they have to exchange some messages for computing a common key. Compared with Hui-Feng Huang scheme, it is obvious that the proposed method can reduce large amounts of computation & communications for both in the key pre-distribution step and computing a common secret key for any pair of nodes. Thus, our method is more efficient and uses fewer communications than those of existing key pre distribution schemes for secure wireless sensor networks. It significantly improves the performance and energy efficiency of the sensor nodes [6].

Table I: Comparisons of Hui-Feng Huang scheme and the proposed scheme

	Hui-Feng Huang scheme	**proposed scheme**
Key pre-distribution step	n^2T_m	n^2T_d
Compute a common key for any pair of nodes	T_d	T_d
Total number of transmissions for finding all pair of common keys	0	0

V. CONCLUSION

In this balance we venture worked a contrary principal supplying ambition for ghetto-blaster sensor networks ramble provides security. In all directions we strive minuscule wide intelligent jugs acute central provision hankering based on deployment knowledge of the wireless sensor networks. The puppet intention is lavishly more conformability

against sensor nodes capture. Our intention has a sum total of loved properties. Sly, our hankering is scalable and flexible. For a squawking that uses 64-bit private keys, our goal allows at hand to N = 264 sensor nodes. These nodes cut scream ring to be deployed at the alike life-span; they duff be extra in due course, and sedate be gifted to establish secret keys with actual nodes. Encourage, compared to existing central pre-distribution stratagems, our plot desire is substantially more resilient against attack. Our aspiration provides skilful agreement of a purchase cherished acute hesitation plan without relying on the random model.

VI. FUTURE SCOPE

We backbone focus on probabilistic hankering in lot. We resolve go to hoard Native connectivity between nodes by supplement XOR operation in efficient key management scheme. In the future, this prevalent zone of fascination areas courage remorseful tester networks an integral part of our lives. How in the world, feat of tester networks needs to respond the compact introduced by actually such as rail against sanction, scalability, cost, hardware, topology change, environment and power consumption. On the side of these chains are standing burdensome and antitoxin for hint networks, new wireless ad hoc networking techniques are required.

REFERENCES

[1] Hui-Feng Huang,"A New Design of Efficient Key Pre-distribution Scheme for Secure Wireless Sensor Networks", Proceedings of the Third International Conference on International Information Hiding and Multimedia Signal Processing (IIH-MSP 2007) -Volume 01, 2007.

[2] Subash.T.D, Divya .C ,"Novel Key Pre-distribution Scheme in Wireless Sensor Network", 978-1-4244-7926-9/11/$26.00 ©2011 IEEE.

[3] T.Kavitha, S. JenifaSubhaPriya, Dr. D.Sridharan, "Design of Deterministic key pre distribution using number theory", 978-1-4244-8679-3/11/$26.00 ©2011 IEEE.

[4] Shuai Yang, Jie Liu, Chunxiao Fan, Xiaoying Zhang , JunweiZou , "A new design of security wireless sensor network using efficient key management scheme".

[5] Murat Ergun and Albert Levi, "Combined Keying Materials for Key Distribution", Sabaci,Istanbul,Turkey.

[6] Tzu-Hsuan Shan and Chuan-Ming Liu ,"Enhancing the Key Pre-distribution Scheme on Wireless Sensor Networks".

[7] I.F. Akyildiz, W. Su*, Y. Sankara subramaniam, E. Cayirci, "Wireless sensor networks: a survey".

[8] Marcos A.M. Vieira1, Ariano B. da Cunha2, and Di´ogenes C. da Silva Jr.2, "Designing Wireless Sensor Nodes".

[9] L. Eschenauer and V. D. Gligor. "A key-management scheme for distributed sensor networks", In Proc. of the 9th ACM CCS conference, pp. 41 – 47, 2002.

[10] 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.

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

[12] 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.
[13] Donggang Liu, PengNing, Wenliang Du, “Group Based Key Pre Distribution in Wireless Sensor Networks”.

BIOGRAPHY

Author Details: ***Y.PRASAD BABU*** *Student of M.Tech CSE, Sri Venkateswara College of Engineering & Technology, Chittoor. Email: babu496@gmail.com*

Guide Details: P.JYOTHEESWARI *M.Tech, Associate Professor, Sri Venkateswara College of Engineering & Technology, Chittoor Email:jyosvcetcse@gmail.com*