IJCAES
ISSN: 2231-4946
Volume III, Special Issue, August 2013

International Journal of Computer Applications in Engineering Sciences
Special Issue on National Conference on Information and Communication (NCIC'13)
www.caesjournals.org

Key Distribution Scheme for Hierarchical Cluster Wireless Sensor Network

S. Jenifer Ruby[1], T.Kavitha[2]

M.E Student [1] , Senior Assistant Professor[2]
Computer Science And Engineering,Information Technology
Jerusalem College of Engineering
Chennai, India

s.jeniferruby@yahoo.com,haikavi18@yahoo.co.in

***Abstract*— In wireless sensor networks (WSNs), key management is one of the vital aspects of security. Since sensor networks suffer from the resource constraints like inadequate memory space, connectivity, resiliency, communication overhead, key pre distribution scheme be supposed to need a smaller amount memory space as likely as supporting strong security power, *i.e.*, high resilience against node capture. a random-key pre distribution scheme has professional explanation for distribution keys between sensor nodes. In this paper propose new key distribution which is based on stated based, signal range and clustering heterogeneous sensor nodes. Uses deployment knowledge to divide deployment regions into overlap clusters, every of which has its own distinct key space. The signal ranges of the sensor nodes might considerably develop the performance of the key-sharing method, if two sensor nodes directly located within communication range and also to be in active-state at the similar time. Key pre distribution scheme that guarantees a higher probability of sharing keys between nodes that are within the signal range. As an outcome, the planned approach provides enough security and is expected to minimize the key ring, decrease the communication overhead, and provide high connectivity. Through careful assembly of these clusters, network resilience is enhanced, without compromise connectivity or communications overhead.**

***Keywords* — Key Pre Distribution, Cluster Head, Path Key Establishment, Shared Key Discovery.**

I. INTRODUCTION

A Wireless Sensor Network (WSN) typically consists of a large number of small sensors with inadequate computation capability, memory space and low-cost, battery-powered devices; each sensor node is prepared with integrated sensors, inadequate data processing capabilities, and a limited radio range. Typically, WSNs are deployed at elevated density in regions requiring observation and monitoring. In military applications, sensors may be deployed in unattended or hostile environments such as battlefields. WSNs are, therefore, vulnerable to various kinds of malicious attacks like eavesdropping, concealed, traffic-analysis, etc. Hence, it is important to protect communications among sensors to maintain message confidentiality and integrity. Availability of the transmitted data .Providing secure communication among sensor nodes deployed in hostile environment is an important and challenging problem. A common approach to solve this problem is to use a key pre distribution scheme in which each sensor node is assigned a subset of keys selected from some key pool prior to deployment. Keys are selected at random from a large key pool and placed in sensors. Two nodes share one or more keys with certain probability. Establish the pair wise key which increases the key connectivity among the sensor nodes. It is subset of elements of elements of key pool which occur in the key chain of a sensor node. The sensor nodes are usually scattered in a sensor filed. Each of the scattered sensor nodes has the capabilities to collect data and route data back to the sink and end users.

A .Key Pool, Key Chain

K*e*y Pool contains list of all keys or keying materials which are used in the WSN. Key chain is a list of keys or keying materials which are stored on sensor nodes that are randomly selected from key pool. These key chains are called as blocks. Each sensor loaded with number of blocks.

B .Neighbor Discovery and Shared Key Discovery

After deployment, all sensor nodes find their neighbor nodes using communication signal range because all sensor nodes have its own communication range. The rationale is that not all nodes may be within communication range of each other. Thus it is necessary to find the neighbor nodes that are reachable from that node. After the neighbor discovery process, the sensors need to find if they share common key (Shared Key Discovery) with their neighbor nodes. If there are no keys in common, the path key establishment in which intermediate nodes serve as relays otherwise direct communication link will be establishment between the sensors.

C .Clustering

In cluster-based networks, nodes are typically organized into clusters, with cluster heads (CHs) relaying messages from sensor nodes in the cluster head to the base stations (BSs).

II. RELATED RESEARCH

L. Eschenauer and V. D. Gligor[8], The key pre-distribution phase of our scheme consists of five off-line steps, namely generation of a large pool of *P* keys (e.g., 217 - 220 keys) and of their key identifiers; random drawing of *k* keys out of *P* without replacement to establish the key ring of a sensor; loading of the key ring into the memory of each sensor; saving of the key identifiers of a key ring and associated sensor identifier on a trusted controller node; and for each node, loading the *i*-th controller node with the key shared with that node. A link exists between two sensor nodes only if they share a key; and if a link exists between two nodes, all communication on that link is secured. The path-key establishment phase assigns a path-key to selected pairs of sensor nodes in wireless communication range that do not share a key but are connected by two or more links at the end of the shared-key discovery phase.

Huyen Thi, Mohsen Guizani, Minho Jo[10],A Key sharing in probabilistic key pre distribution schemes that takes the signal range into consideration while deciding on the keys to be deployed on each node. The scheme guarantees that nodes in the signal range will share keys with much higher probability. Probabilistic key pre distribution scheme that guarantee a higher probability of sharing keys between nodes that are within signal range.

Jaemin Park, Zeen Kim, KwangjoKim [11]In this paper consider two major operational states: active and sleep. In the sleep state, the lowest value of the node power is consumed, while being asleep a sensor cannot interact with other. State of sensor is considered which avoid unnecessary key assignments and the number of required keys. Let s_i and k_j denote the sensor nodes and its pre distributed symmetric keys, respectively. Let T_i denote the time interval when sensor s_i is supposed to be in active state with high probability. Two Sensors s_1 ands_2 are deployed closely, share more keys. Suppose that s1 and s2 have key set {k_1, K2, k3, k4} and {k_1, k3, k5, k6} respectively. During T1, s1 are s2 are in active state and sleep state, respectively. Then as time goes by s_1 and $s_{2\ transit}$ their states to sleep and active .Pair wise key scheme in which, each node stores K<N-1 keys. The rationale is that not all nodes may be within communication range of each other and it is enough to establish links with nodes which are in close proximity. Each node stores all the pair wise keys, and also all the node identifiers, with which it shares pair wise keys. The results in large storage cost (O (K log N)).This scheme was proposed for a static network, but can be extended to a mobile network. All pair wise keys have to be stores all the time, even if the nodes sharing pair wise keys are not within communication range.

Née raj Mittal, Ramon Novales[16] The Key pre-distribution scheme that make use of region-based deployment knowledge. This Scheme construct a set of clusters such that each cluster contain number a small number of deployment regions, all of which are neighbors of each other. Every pair of neighboring deployment regions belongs to at least one cluster. Each cluster has its own distinct key space, and it's from these cluster key spaces that nodes are assigned their keys. Neighbor regions are combined into clusters and each cluster has an associated key space which maximizes the overall key pool size and its resilience. In region based deployment knowledge, the deployment regions, and the individual sensor nodes is partitioned into a set of groups such that sensor nodes belonging to same group are deployed together.

Patrick Traynor, Raju Kumar, Heesook [17], Heterogeneity to provide more robust key management and established protocols for sensor network. Communication between adjacent nodes is limited by key matching. Due

to the random nature of the deployment, the potential for node mobility and addition of nodes at a later time. Instead of homogeneous composition of nodes, the network now consists of a mix of nodes with different capabilities. In homogeneously composed sensor networks assume one of two scenarios: either a network with access to a key distribution centre via base station or remotely located, stand alone system without access any infrastructure. If nodes are equipped with symmetric keys through an priori distribution scheme, Neighbors will be able to exchange encrypted transmission.

II. PROPOSED WORK

Before that, we introduce the symbols and notations that will be used throughout this paper as follows:
Signal range: Area that the radio signal of a node can cover.
Sharing keys: Common keys that are used between two nodes.

A. Network Model

We assume that a large number of resource-limited sensor nodes are randomly scattered around an adversarial area. Examples of such networks can be military or environmental applications in which a large number of sensors are dropped from an airplane to an adversarial or hazardous environment. There is no trusted infrastructure in the deployment area, and sensor nodes have identical processing, storage, battery life, and communication resources. Once deployed, each sensor node receives/transmits messages from/to another sensor node if the former is located within the signal range of the latter node. The signal coverage area (signal range) for each sensor is assumed to be a circle that is centered at its deployment location with radius *r*. Two sensor nodes are "neighbors" if they are physically located within each other's signal range. It may be possible for a sensor to have a long transmission. Sensor nodes communicate with each other to exchange application data at the data layer and routing information at the control layer. In random key pre-distribution schemes, any of the two nodes in the sensor network has the same probability of shared keys. However, if two nodes cannot communicate with each other, it is unnecessary to store common keys.

1) The key pre distribution and node deployment phases are the two major phases in the proposed scheme and are presented in following Sections respectively.

2) Shared-key discovery phase: After deployment, each node needs to discover if it shares any keys with its neighbors that are in the wireless communication range. Among the many ways to do this, that proposed is given as follows: First, the sending node broadcasts a message that contains its identifier. The receiving node uses a function to derive the key identifiers and then compares them with its key ring for the common keys. The common keys will be used to find both the authentication and encryption keys. The neighboring node uses these keys to secure the communication channel between itself and the broadcasting node.

3) Path-key establishment phase: Two nodes in the signal range of each other may not find any common keys between them. In that case, they need to find a secure way to agree upon a common key. Therefore, the intermediary nodes are used to forward the message between the two terminal nodes. A grid of the target field is used to predetermine the possible deployment positions of nodes or groups of nodes. There are various kinds of grids, such as square, hexagonal, and polygonal grids. In this scheme, we use a square grid; others can be handled in a similar manner. The setup server partitions the target field into *C* columns and *R* rows. Each cell of the grid is denoted by coordinate (*iC, iR*) and may be assigned some virtual nodes. The virtual nodes are representatives of the nodes in the key distribution process at the setup server. The key network on the virtual nodes makes a key map that can be used for adding a new node afterward.

Key Set Up

Step 1: Get number of cluster, key pool size, number of nodes.
Step 2: Divide key pool size based on cluster.
Step 3: Generate Random number using Random function.
Step 4: Get number of time neighbor.
Step 5: Calculate random number for each cluster head, each node in time neighbor.

Node Arrangement

Step 1: Get the total number of nodes.
Step2: Calculate number of nodes for each cluster.
Step 3: Arrange the nodes based on node id for time group in every cluster.

Node Deployment

Step1: Get the length and width of target area.
Step 2: Calculate number of rows for h hexagonal or number of columns for v hexagonal.
Step 3: Calculate number of cells in each row for h hexagon or column for v hexagon.
Step 4: Obtain the coordinates of first cell of H (V) hexagon. Generate set of possible points, check whether the point lying inside the hexagon.
Step 5: Pick deployment points randomly for each sensor node in a cluster (i, j)
Step 6: Choose centre of hexagon (i, j) as deployment for each cluster head in corresponding cluster (i, j)
Step 7: compute coordinates for each neighbor hexagon of hexagon (i, j) repeat step 2 to 4.

B. Network Bootstrapping

Once the nodes are deployed, the cluster heads begin the registration process with the base station, and the clustering process is done; this is explained as follows.

C. Clustering

Cluster head registration with BS After deployment, each cluster head establishes a connection with the base station. The cluster head forwards, an initialization packet having its identifier C H_i, and the identifier of the unit it belongs to $U_{r,c}$, to the base station in a single hop or through multi hops, which is encrypted by a key, $K_{CiB.}$

After receiving the initialization packets from all the cluster heads, the base station checks with its database for authentication, and gives a reply saying that the registration was done successfully.

D .System Architecture

The key setup and key management activities are shown in figure 1. During initialization step, the key chain is generated by assigning the keys from the key pool. After that key chain is loaded into the sensor node. After deployment, the sensor node need to find if they share common key (Shared-key discovery).If there are no keys in common, then path key is established in which intermediate nodes serve as relays. A link exists between two sensor nodes only if they share a key and if a link exists between two nodes, all communication on that link is secured .The path-key establishment phase assigns a path-key to selected pairs of sensor nodes in wireless communication range that do not share a key but are connected by two or more links at the end of the shared-key discovery phase. Path keys need not be generated by sensor nodes.

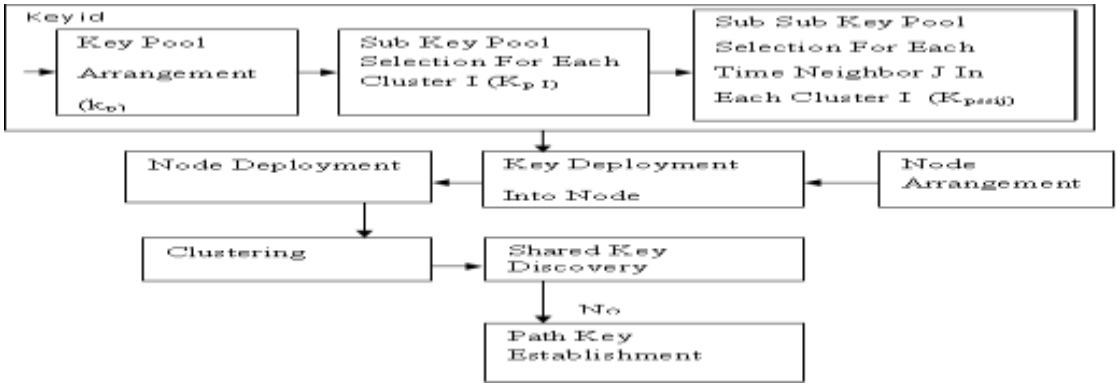

Figure 1 System Architecture

III. RESULT AND DISCUSSION

The Proposed Key Distribution Scheme is implemented using C++ ,Java. The Figure 2 , 3 shows that Number Of State Group Allocated to Nodes.

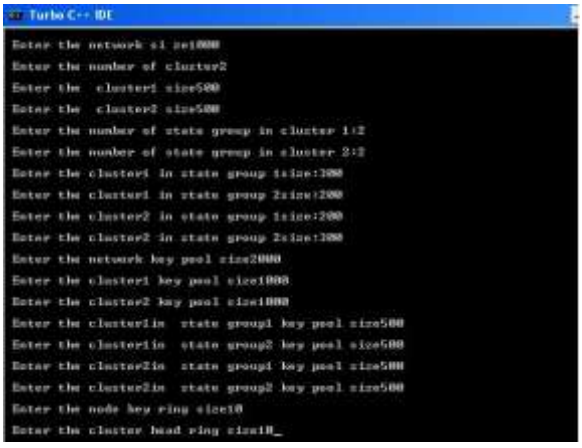

Figure 2 Key Set Up

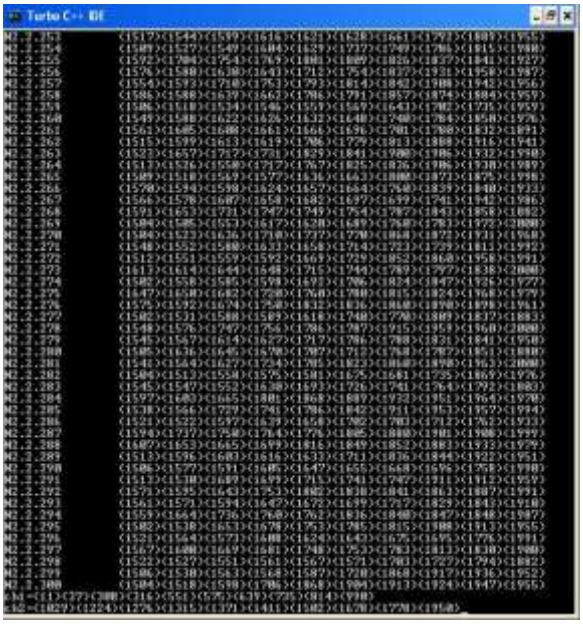

Figure 3 Key Deployment Into Node

The Figure 4,and Figure 5 shows that check whether the points lying within the range,if the coordinate lying within the range,then sensor nodes had deployed at corresponding location .

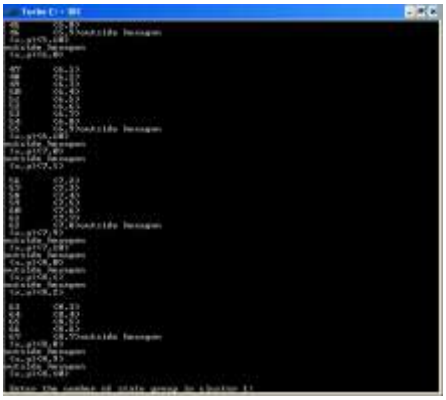

Figure 4 Node Deployment

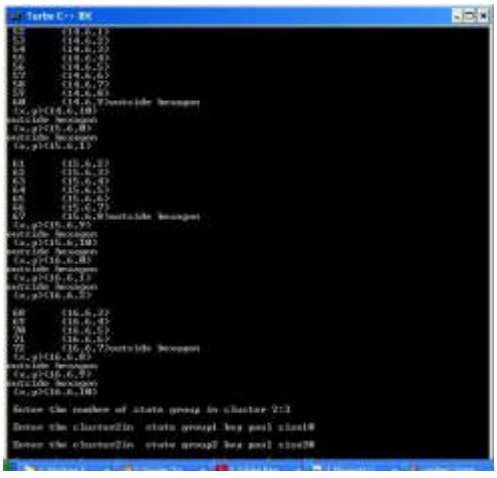

Figure 5 Node Deployment

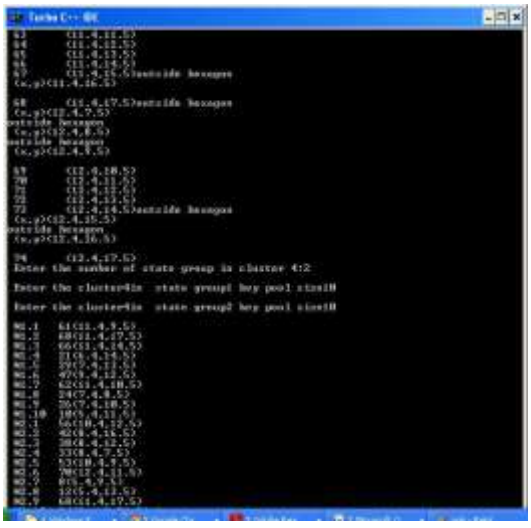

Figure 6 Key Deployment Into Node

IV. CONCLUSION

In wireless sensor network, the pair wise key pre-distribution is used to provide secure communication among sensor nodes deployed in hostile environment. The probabilistic key distribution achieves good key connectivity between the sensor nodes. Thus the signal ranges of the sensor nodes might significantly improved the performance of the key-sharing mechanism and Clustering scheme has designed to maximize the overall key pool size.

The key distribution algorithm should satisfy efficiency factors in order to achieve the good connectivity with low storage and high resilience. These factors should be evaluated during key distribution. The future direction of this work is to analyze the efficiency factors considered during key distribution using C++ ,Java.

REFERENCES

[1] F. Akyildiz, W. Su, Y. Sankara subramaniam, and E. Cayirci,"*A survey on sensor networks*," IEEE Communications Magazine, vol. 40, no. 8, pp. 102–114,(2002).

[2] S. A. Camtepe and B. Yener, "*Key distribution mechanisms for wireless sensor networks: A survey,"* Comput. Sci. Dept., Rensselaer Polytech. Inst., Troy, NY, Tech. Rep,(2005).

[3] H. Chan, A. Perrig, and D. Song, "*Random key predistribution schemes for sensor networks,"* in IEEE Symposium on Security and Privacy, Berkeley, California(2003).

[4] W. Du, J. Deng, Y. S. Han, S. Chen, and P. K. Varshney, "*A key management scheme for wireless sensor networks using deployment knowledge*," in Proc. 23rd IEEE Annu. Joint Conf. IEEE Comput. Commun. Societies(2004).

[5] W. Du, J. Deng, Y. S. Han, and P. K. Varshney, "*A pairwise key predistribution scheme for wireless sensor networks,"* in Proceedings of the 10th ACM Conference on Computer and Communications Security (CCS), Washington, DC, USA, pp. 42–51(2003).

[6] W. Du, J. Deng, Y. S. Han, P. K. Varshney, J. Katz, and A. Khalili, "*A pairwise key pre-distribution scheme for wireless sensor networks,"* ACM Trans. Inf. Syst. Secur., vol. 8, no. 2, pp. 228–258{2005).

[7] W. Du, J. Deng, Y. S. Han, and P. K. Varshney, "A key predistribution scheme for sensor networks using deployment knowledge," IEEE Trans.

[8] L.Eschenauer and V.D.Gligor," *A Key Management Scheme for distributed sensor networks,"* in proc, 9th ACM conf.commun.Security, pp41-47(2002).

[9] A. M. Hegland, E. Winjum, S. F. Mjolsnes, C. Rong, O. Kure, and P. Spilling, *"A survey of key management in ad hoc networks,"* Commun. Surveys Tuts., vol. 8, no. 3, pp. 48–66(2006).

[10] Huyen Thi, Mohsen Guizani, Minho Jo," An Efficient Signal Range Based Probabilistic Key Pre distribution Scheme in a Wireless Sensor Network," IEEE Transactions on Vehicular Networks. Vol.58, No.5(2009).

[11] Jaemin Park, Zeen Kim, Kwangjo Kim," *State Based Key Management Scheme for Wireless Sensor*".in Proc .IEEE Int.Conf.Mobile Adhoc Sensor syst,Nov,2005,pp,pp,1-10,(2009).

[12] T.Kavitha, D.Sridharan,"*Security Vulnerabilities in Wireless Sensor Network: ASurvey*,"Journal of Information Assurance and Security.

[13] J. C. Lee, K. H. Wong, J. Cao, H. C. B. Chan, and V. C. M. Leung, "*Key management issues in wireless sensor networks: Current proposals and future developments*," IEEE Wireless Commun., vol. 14, no. 5, pp. 76–84,(2007).

[14] D. Liu and P. Nimg,"*Establishing Pair wise Keys in Distributed Sensor Network",* to appear in the 10th ACM Conference on Computer and Communication Security (CCS03), Washington D.C,(2003) .

[15] G. Li, J. He, and Y. Fu , "*A hexagon-based key predistribution scheme in sensor networks*," in Proc. Int. Conf. Workshops Parallel Process., Aug. 2006, pp. 175–180. Dependable Secure Comput., vol. 3, no. 1, pp. 62–77,(2006).

[16] Née raj Mittal, Ramon Novales ,"*Clustering Based pre-distrution Using Knowledge*," IEEE Transaction on Dependable and Secure Computing, vol7, No3,(2010).

[17] Patrick Traynor,Raju Kumar,Heesook choi,Guohong Cao,Sencun,Thomas La Porta,","*Efficient Hybrid Security Mechanism For Heterogeneous Sensor Networks*,IEEE Transaction On Mobile Computing,Vol 6,No 6,(2007).

[18] J. P. Walters, Z. Liang, W. Shi, and V. Chaudhary, "*Wireless sensor network security: A survey,"* in Security in Distributed, Grid, and Pervasive Computing, Y. Xiao, Ed. Boca Raton, FL: CRC,(2007).

[19] Y.Wang, G. Attebury, and B. Ramamurthy,"*A survey of security issues in wireless sensor networks,"* Commun. Surveys Tuts., vol. 8, no. 2, pp. 2–23,(2006).

[20] Wenliang Du, Jing Deng, Yunghsiang S. Han, and Pramod Varshney, *"A Pairwise Key Predistribution Scheme for Wireless Sensor Network"*, In Proceedings of the 10th ACM Conference on Computer and Communications Security (CCS), Washington D.C,(2003).