Key Dispensation Scheme for Wireless Sensor Network

B. Sundarraj

Department of Computer Science and Engineering, Bharath University, Chennai-600073, India

Abstract: In Wireless sensor networks (WSNs), key management is one of the crucial aspects of security. We propose a probabilistic key pre-distribution scheme that guarantees a higher probability of sharing keys between nodes that are within the signal range since sensor networks suffer from the resource constraints like limited memory space, key pre distribution scheme should require less memory space as possible while supporting strong security strength i.e high resilience against node capture. If two sensor nodes closely located each other have very low probability to be in active state at the same time, unnecessary key assignment can be happened since keys shared only between them. A key pre-distribution schemes that makes use of region based deployment knowledge. Constructs a set of clustered such that each cluster contains 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 is from these cluster key spaces that nodes are assigned their keys. In this manner, we guarantee that nodes in neighboring regions share a key with given overlap probability while nodes in non-neighboring regions do not share any keys.

Key words: Wireless sensor network · Path Key Establishment · Shared Key Establishment

INTRODUCTION

A Wireless sensor network (WSN) consists of spatially distributed autonomous sensors to cooperatively monitor physical or environmental conditions, such as temperature, sound, vibration, pressure, motion or pollutants. Sensors are low battery powered devices having wireless communication capability in short distances. 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 [1-7]. 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 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.

Key Pool, Key Chain: Key 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. Kumaravel et al. [8], these key chains are called as blocks. Each sensor loaded with number of blocks.

Neighbour 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. Kumaravel et al[9], 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.

**Previous Research:**


A Key pre distribution scheme that makes 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.


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. Kumaravel et al[10], 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.


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_i 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_i and s_j are deployed closely, share more keys. Suppose that s_1 and s_2 have key set \{k_1, k_2, k_3, k_4\} and \{k_1, k_2, k_3, k_5\} respectively. During T_1, s_1 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. Kumaravel et al[11], 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 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.


An Efficient key management scheme designed for heterogeneous sensor networks. This Scheme uses a symmetric key mechanisms to distribute, revoke keys during the lifetime.


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 consist of a mix of nodes with different capabilities.
Hypothesis Testing

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 uniform distribution.
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.
Step 2: Calculate nodes for each cluster.
Step 3: Arrange nodes

Node Deployment:

Step1: Get the target area.
Step 2: Calculate number of rows for and columns
Step 3: Calculate number of cells in each row and column
Step 4: Get the coordinates of cell
Step 5: Choose deployment points randomly for each sensor node in a cluster (i,j)
Step 6: Calculate coordinates for each neighbor cell and repeat step 2 to 4

Shared Key Discovery: The shared-key discovery phase takes place during DSN initialization in the operational environment where every node discovers its neighbors in wireless communication range with which it shares keys. The simplest way for any two nodes to discover if they share a key is that each node broad- cast, in clear text, the list of identifiers of the keys on their key ring. This approach does not give an adversary any attack opportunity that he does not already have.

Path Key Establishment: 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. The design of the DSN ensures that, after the shared-key discovery phase is finished, a number of keys on a key ring are left unassigned to any link.

Scope of the Research: In this research, will be key pre distribution have been done using probabilistic approach, random number will be generated using deterministic approach.

The Results of Hypotheses Testing: In this section of paper we present analysis the results of research hypotheses. As mentioned before, for testing H2 and H4, we also use a sample of state companies. The following subsections provide analysis of results of hypotheses testing at total sample level, industrial group level and year level.

Results of Testing H1

The Results of Testing H3
The Results: The cluster key chain generated and security was achieved by key pre distribution

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. 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 omnet++ simulation tool [12-14].

REFERENCES