CHAPTER-5

KURCS: KEY UPDATION FOR REMOVAL & REPLACEMENT OF COMPROMISED SENSOR NODES

An energy efficient key management scheme is an important aspect to ensure secure services in the resource constrained Wireless Sensor Networks (WSNs). This chapter presents an energy efficient key revocation scheme for removing compromised sensor nodes from the network. Unlike most of the key removal schemes focused on removing the compromised node from the network by redistributing the keys or keying material to each and every node in the network, our presented scheme, known as Key Updation for Removing & replacement of Compromised Sensor nodes from Wireless Sensor Networks (KURCS), uses key updation techniques to update the keys of uncompromised sensors to remove compromised sensors from the network. Proposed scheme is validated through simulation and results proven that it is better than existing schemes without any increase in communication overheads.

Rest of the chapter is organized as follows:

Section 5.1 presents introduction to key revocation scheme and types of compromised node detection and key revocation schemes used in WSNs. Clustering scheme is explained in Section 5.2 followed by key sharing scheme in Section 5.3. Section 5.4 describes system model for key updation. Performance analysis of the proposed system is given in Section 5.5 to show the comparative study with existing schemes. Finally, chapter has been summarized in Section 5.6.

5.1. KEY REVOCATION SCHEME

Key distribution and key revocation are the two components of key management scheme. Key distribution is the task to manage the key in such a way that if two or more sensors want to communicate with each other for the purpose of sharing the

data or control messages, the key is to be made available to them only. The scheme should be energy efficient, as the sensor nodes in the network are resource constrained. However, Key revocation is the task of removing the compromised sensors from the network to restrict such nodes to participate in further communications to avoid any kind of interference or disturbance in communication process.

5.1.1. Types of Compromised Node Detection and Key Revocation Schemes

Compromised node detection scheme refers to preparing a list of ID's for those sensors that are performing malicious activity in the network and key revocation refers to the task of key updation in such a way that the updated key is unavailable to the compromised sensor. There are two types of Compromised Node Detection and Key Revocation Schemes (CNDAKRS):

a. Base Station Initiated Scheme
b. Group Based Scheme

5.1.1.1. Base Station Initiated Scheme

In Base station initiated Compromised Node Detection and Key Revocation Scheme, a centralized authority (Base Station) is responsible for the detection of compromised sensor node in the network and the same authority updates the key in such a way that the updated key is not available to the compromised sensors in the network. In this scheme, base station monitors the activities of each node in the network using following method:

- ***Continuously Monitoring:*** In this scheme, every node monitors the activities of its neighbors and sent this activity in the form monitoring report to the base station. If all the nodes in the network have at least j neighbors then at least j monitoring reports are transmitted by every node to the base station to detect the compromised node. Therefore this scheme is not scalable.
- ***Periodic Monitoring:*** In this scheme, instead of transmitting the monitoring reports to the base station in every round, every node records the activities of each of its neighbor in every round. If some node A in the network is

misbehaving to other node B then node B declares node A as a malicious node. In this way, every node monitors the activities of all of its neighbors. A node records the behavior of its neighbors directly by the experience or by the suggestions received from the common neighbors indirectly. On the basis of this direct experience and indirect suggestions, every node in the network gives a positive or negative rank to each of its neighbor. If the behavior and suggestions are good, then rank increases otherwise the rank is decreases. If the rank of any sensor is below a threshold value, the node is declared as a malicious node and its intimation in the form of a report is given to the base station at the same time.

Now using any one technique (continuous or periodic monitoring) the base station collects all the lists containing the ID's of malicious nodes from every sensor in the network. On the basis of these reports, base station declares the nodes as a compromised node based on some criteria applied to all the reports. Finally the base station prepares a list containing the ID's of compromised nodes and broadcast this list in the entire network to aware all nodes about the ID's of uncompromised nodes. The key used by these compromised sensors is also updated and a new key is provided to all uncompromised sensors in the network. In this way, role of all compromised sensors is ignored in the network and are treated as they have been removed from the network.

If cryptography is used in the network then the list is also broadcasted in the encrypted form. If a single key is shared and used in the entire network, then the updated key is encrypted with this key and broadcasted in the network. Since the key used in the encryption process is already known to the compromised node, this compromised key is never used in the network to encrypt any confidential message. Network with single shared key is not preferred as if key is compromised; entire network becomes unreliable and unsecure.

On the other hand, if each sensor is using a different key known to a particular sensor and the base station only, for example in a network of 'n' sensors the base

station stores ‘n’ unique keys in its memory. Now if ‘p’ number of sensors is compromised, the base station prepares (n-p) individual lists containing the ID of compromised sensors. Now the base station encrypts first list with the key of first uncompromised sensor and sent this list to that sensor. Similarly second list is encrypted with the key of second uncompromised sensor and sent this list to second uncompromised sensor & so on. Now all the sensors get the encrypted list containing the ID’s of compromised sensors in the network. Every sensor decrypts the list with its own key and knows the IDs of compromised sensors in the network.

In this scheme, total n-p messages unicasted by the base station for list updation. The drawback of this individual key sharing is communication with base station only by all sensors; no communication among the sensor nodes. WSNs with this scheme seem to be efficient in applications based on clustering. For example clustering is used to achieve network performance but in clustering local decisions have to be made in order to cluster formation and cluster head selection where it is necessary that sensors from the local area should communicate with each other, without any interference from the base station.

5.1.1.2. Group Based Scheme

In this scheme, the decision of compromised node is made by several sensors in a fixed group locally without any dependency to the base station. But in this type of schemes, it is necessary for every sensor node to have two keys stored in its memory. One key is used to make a communication with the base station and other key is to communicate with the group members. It is also necessary that the key of one group is different from the key of other groups in the network. But the drawback of this scheme is that if some sensor in a group is compromised, the key of entire group is also compromised. If the system provides a new key to this group then this key is again available to the compromised sensor. On the other hand if we are encrypting the new key with the group key, it’s useless as the group key is already known to compromised sensor node in the group. One of the solutions to this problem is create a new key for encryption by the base station with the individual

keys of each sensor and transfers this encrypted key to every member in the group separately.

The advantage of this scheme is that the traffic that flow from sensor to base station decreases as there is no need to handover the monitoring report to the base station. In previous schemes every member of the network is transmitting his own report about each of its neighbor to the base station but in a group based scheme, only one report is given to the base station in a group of sensors. If there are 100 sensors in the network and each group contains ten percent of total sensors then ten such groups' needs to formed. Each group contains ten members. In this scheme instead of transmitting one hundred monitoring reports (one by every sensor) or 100*j (one report by every sensor about its each neighbor) to the base station, only one report per group is given to the base station. Therefore total ten reports needs to be transmitted in the network and given to the base station.

The drawback of this scheme is that network traffic from base station to sensor nodes is not decreasing because unicasting is the only solution to update the group key. Similarly this scheme performs better if compromised nodes are belonging to a particular area in the same group in the network, as unicasting is done only in that group to update the key. Rest of the traffic flow in the network (from base station to the unaffected area) is unaffected because there is no need to update the key in the uncompromised groups. If minimum one node is compromised in each group then base station needs to update the key of every group. Base station sent the updated key to every sensor in every group using unicasting method by encrypting the new updated key encrypted with the key of individual sensor to every sensor in every group in the entire network. In this scenario, this scheme is working in a similar way as a network with the single shared scheme.

The chances of key hacking are greater in this scheme because the same group key is to be used for long time unless any group member is compromised.

In net shell, there is a need of a scheme to detect the compromised nodes and update the key for uncompromised nodes without affecting the performance of the network.

5.1.2. Requirements of Key Revocation Scheme

Following are the requirements for any kind of key revocation scheme:

- ***Local Decision:*** The decision of compromised node detection is made locally by the group members instead by the base station.
- ***Minimum interference from Base Station:*** The key updation process should update group key locally with minimum communication from the base station.
- ***Secure key distribution:*** An updated group key is distributed in such a way that it is unavailable to the compromised sensor in the group.
- ***Periodically key updation:*** The group key is updated periodically irrespective compromised or compromised status of any node.
- ***Minimum congestion:*** The updated group key is communicated to the base station so that traffic of unicasting to update the group key in the network is reduced.
- ***Key chain secrecy:*** The principle of backward and forward secrecy needs to be maintained in the network.

5.2. CLUSTERING SCHEME

Clustering is the task of grouping wireless sensor nodes in a cluster. All the nodes in this group communicate with each other to send their sensed data to the cluster heads (CH). CH aggregate this collected data for onward transmission to the base station. Clustering is used for effective data communication. Clustering minimizes the energy consumption in the network by reducing long distance transmission with reduced number of nodes participating in long distance transmission.

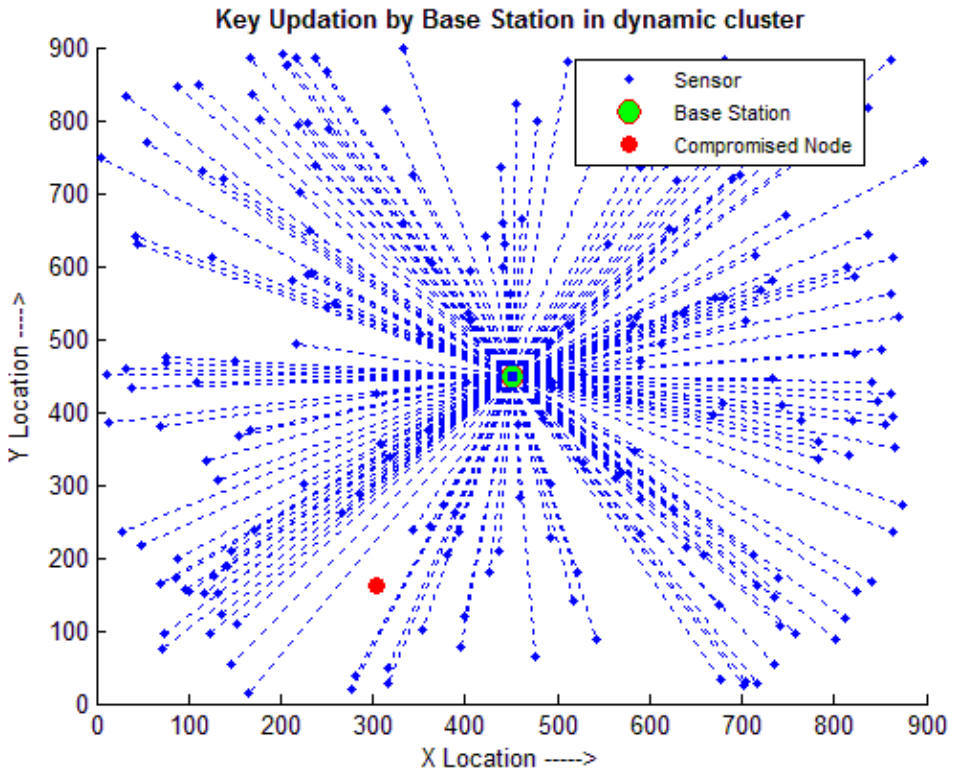

Figure 5.1: Key Updation by Base Station in Dynamic Clustering

There are two types of clustering scheme used in wireless sensor networks, i.e. static and dynamic. In static clustering scheme, clusters are fixed and there is no updation into the size and members of the cluster after cluster formation. But in dynamic clustering scheme, the members of every cluster are decided during cluster formation phase before every round. Thus, the size and members of every cluster are different and depends on the location of the cluster heads elected for the current round. Presented model uses the concept of static clustering, once the cluster is decided for any sensor, it is fixed and permanent in every round throughout the network lifetime. In presented model, the cluster for any sensor is decided with its physical location in the network.

The drawback of using dynamic clustering is that if one sensor is compromised in the network then cluster key of entire network should be updated as shown in Figure 5.1 because it is not known in advance that which sensor should join

which cluster under which cluster head. There are several advantages of using static clustering. Some of them are given below:

a. ***Advance knowledge of network:*** Cluster members are fixed and known in advance. Advance knowledge lets us know in advance about the affected area in case of any compromised node.
b. ***Reduce compromise node spoiling area:*** In static clustering, the members of any cluster are fixed and any node communicates only with the cluster members. If any node within a cluster is compromised, only the members of that cluster are affected not the entire network area.

c. ***Reduce key updation area:*** If static clustering is used and once a node is compromised then the key need to be updated for that cluster rather updating for entire network as in case of dynamic clustering because victims are not predicted in advance.

d. ***Fast key updation:*** If one sensor is compromised then key revocation scheme is applied only to the member of one cluster to which the compromised sensor belongs.

e. ***Reduce Network Traffic:*** As less number of keys are updated to implement key revocation scheme in the network so less number of communications are required in the network.

As shown in Figure 5.2, if some sensor is compromised, there is no need to update the key of entire network. The BS should update the key of all the sensors as belonging to the cluster. In our model, the concept of cluster guard is introduces to reduce the long distance transmission between base station and uncompromised sensors.

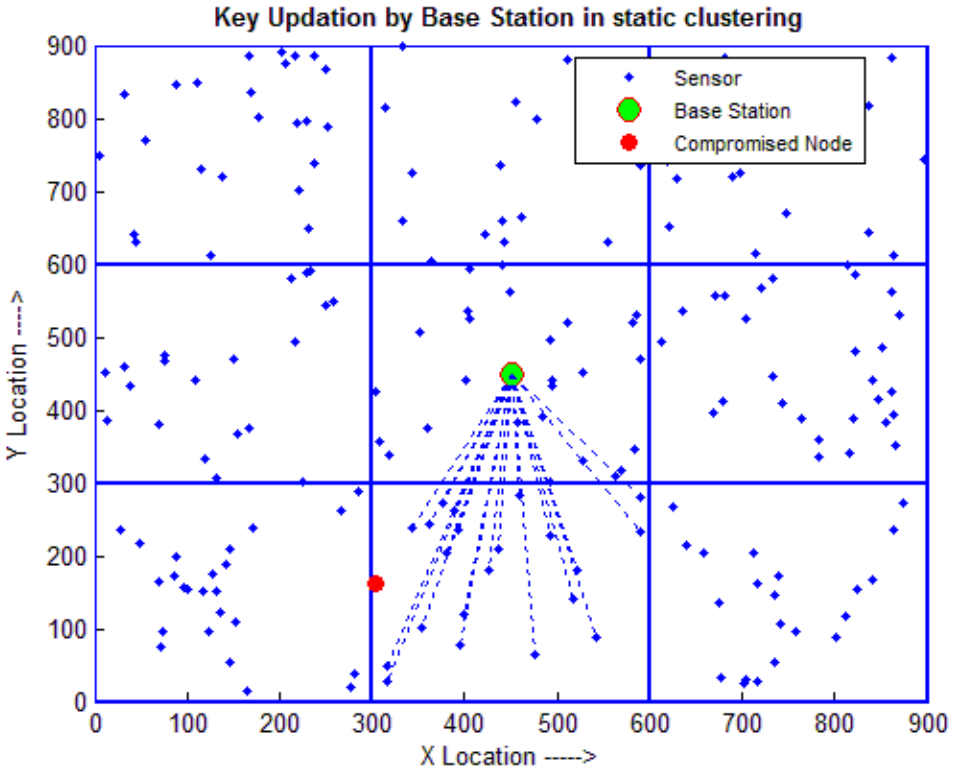

Figure 5.2: Key Updation by Base Station in Static Clustering

5.3. KEY SHARING SCHEMES

A sensor node either forwards the aggregated data to the base station (Data Forwarding) by collecting it from all cluster members if it is a cluster head or injects its own data to the cluster head (Data Injecting) if it is not a cluster head. In first key management scheme, a single key is shared and used in the entire network. All sensors use this key for data injection and cluster head uses the same key for Data forwarding process. The drawback of using a single shared key in the entire network is that if the key is compromised by any sensor in the network, entire network is compromised.

In second scheme, a different key is used by all sensors in the network. This key is known to a particular sensor and the base station only. In this scheme, compromising a single sensor does not affect the functioning of entire network. Data Injecting in this scheme is completely impossible thus data aggregation scheme fails which is the key factor to achieve network performance. This scheme is useful in

the networks where all sensors communicate with the base station only. There is no secure link or communication between the sensors in the network.

In third scheme, a different key is used for different clusters in the network. All members of the same cluster use this shared cluster key for Data Collection and Data Injecting process. The drawback of using this scheme is that if any sensor in a cluster is compromised, entire cluster is also compromised.

In fourth scheme of key management, two different keys are provided to all the clusters and keys of one cluster are different from the keys of other cluster in the network. From these two keys, first key (sensor key) is shared between an individual cluster member and the base station only and the second key (cluster key) is shared between all the cluster members and the base station only. The sensor key is used in the Data Injecting process and cluster key is used in the Data Forwarding Process (DFP). The advantage of this scheme is that if sensor key of any sensor within a cluster is compromised, it may not affect the sensor keys of other sensors in the same cluster. But the drawback of this scheme is that if cluster key of any sensor in a cluster is compromised, the cluster key of entire cluster is also compromised as this key is shared between all the members of the same cluster.

So there is requirement of a key management scheme to decide a key to be used in encryption or decryption process which is updated after a fixed interval of time. In these schemes, a key is provided but not generated, i.e. the secret is distributed, which is not safe for the secrecy. If key is distributed, the chances of key compromise are more in these types of scheme. Moreover, these schemes increase the communication overhead due to keys redistribution to each and every node after a fixed amount of time. So, there is a need of a good key management scheme which should never distribute a key in unsecure wireless medium, instead the key is to be generated with the help of a keying material which is distributed in the wireless channel. Compromising a keying material does not give any clue about the key since the seed value stored in the memory of each sensor node is also used in key generation process along with the keying material.

5.4. SYSTEM MODEL FOR KEY UPDATION

Following assumptions about sensor network have been considered in the presented general framework for removal and replacement of compromised sensor nodes from wireless sensor networks.

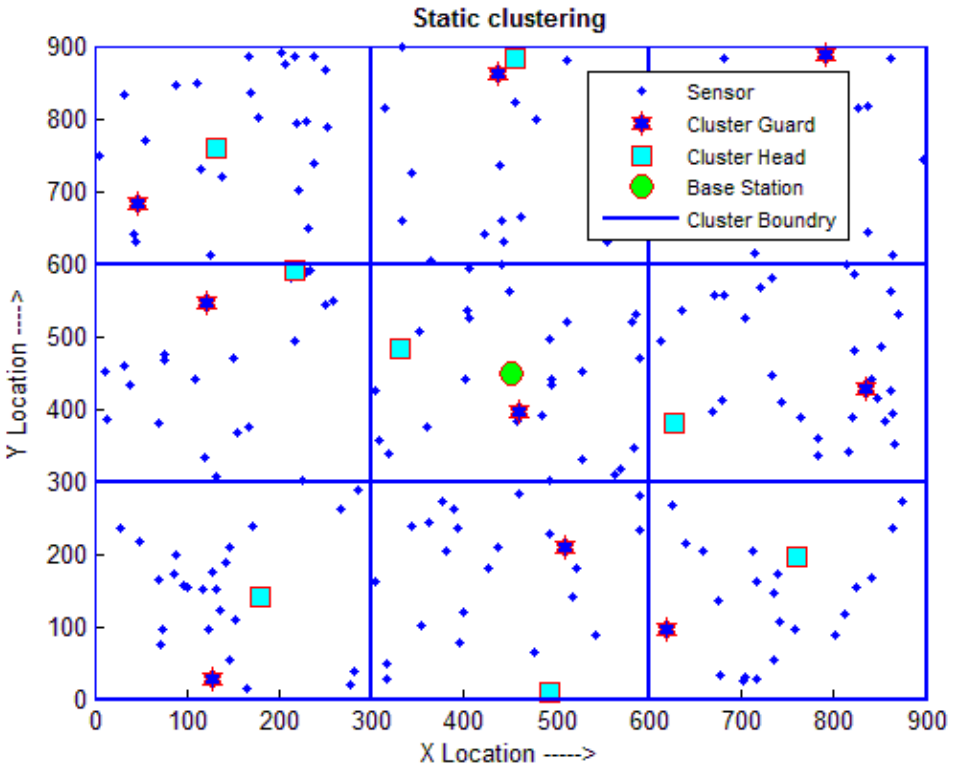

Figure 5.3: Static Clustering with Guard Nodes

First, assumption is that any scheme of clustering is applied to detect a compromised sensor node from the network because the detection of compromised sensor node is out of the scope of this chapter. Once the scheme detects a compromised sensor node from wireless sensor networks, the presented system provides a new key to all the uncompromised sensors in such a way that the updated key is unavailable to the compromised sensors.

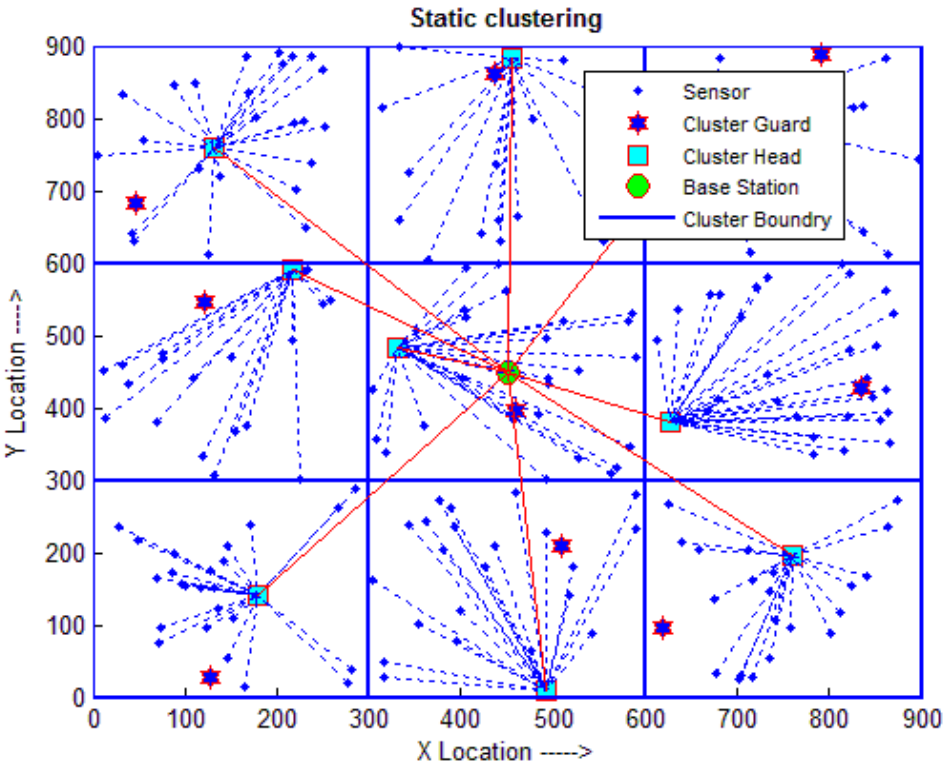

Figure 5.4: Sensor to Cluster Head to Base Station Communications

In the presented scheme, the network is divided into static clusters. Any scheme is chosen for clustering but once the members for a cluster are decided, the members are freeze and become permanent throughout the network lifetime. One cluster guard sensor is provided to every cluster as shown in Figure 5.3. In every round, one cluster head is selected among all the cluster members on rotation basis to balance the energy consumption among all the cluster members. Any scheme is chosen for cluster head selection. All the members in a cluster sense the environment in the form of an event and sent this event in the form of digital information to the cluster head in the encrypted form using cluster key. This cluster key is dynamic in nature, i.e. the key is updated in every round. Now the cluster head compress the data by applying aggregation function after decrypting the data collected from the cluster members. Now cluster head transfers this compressed data to the base station as shown in Figure 5.4 in the encrypted form with the help of a sensor key shared between cluster head and the base station.

Each sensor in the network shares a secrete key with base station known as sensor to base station key. Once a sensor is compromised, cluster guard generates new cluster key generation parameters (seed values) and unicast these seed values to every cluster members except the compromised sensor using cluster guard key shared between cluster guard and the individual cluster member as shown in Figure 5.5.

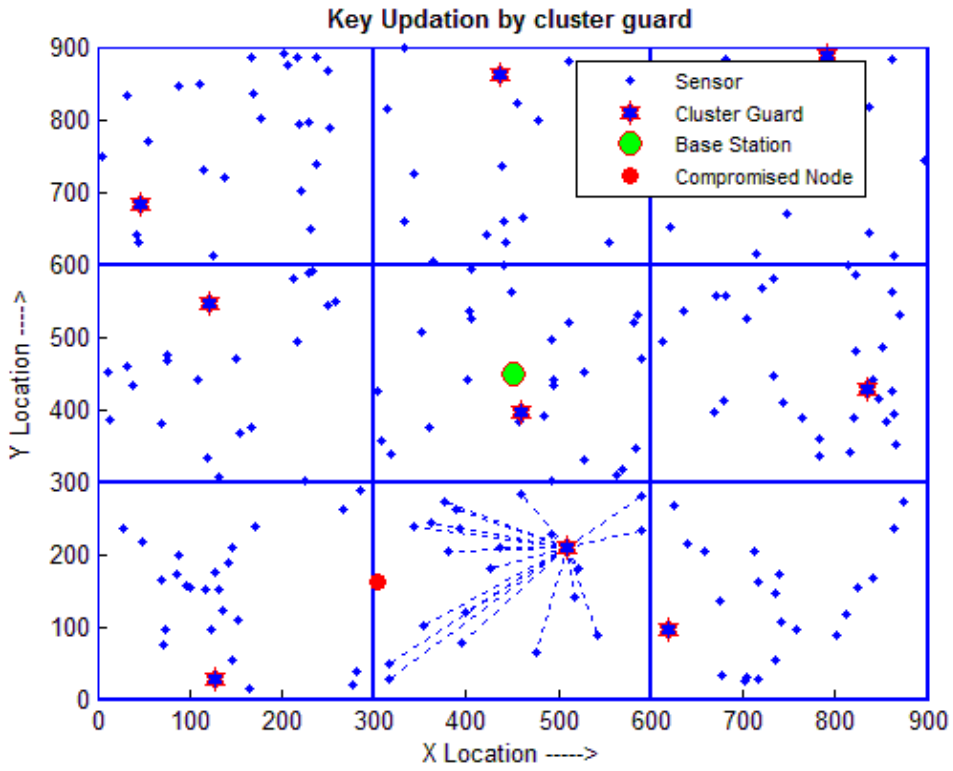

Figure 5.5: Key Updation by Guard Node in Static Clustering

5.4.1. Types of Keys Used in the Presented Model

For proper functioning of the network, several types of keys are used in the network. There are three types of scenario in which sensor communicate in the system. In first scenario, the sensor is communicating with the base station, in second scenario the sensor is communicating with the cluster guard and in last scenario, the sensor is communicating to a cluster head which is different in each round. So a different key is used in different scenario. The keys included are as:

a. ***Sensor BS key:*** This key is shared between a particular sensor and the base station. Base station uses this key to make a communication with a particular sensor in the network. Base station have the knowledge about the key of every sensor in the entire network but an individual sensor knows only a single key shared with itself and base station. All the sensors use this key to make a communication with the base station.

b. ***Cluster key:*** This key is used and shared within cluster members of the same cluster. This key is dynamic in nature and is updated after every round in each cluster. The updation of this key is managed in a way to minimize the communication required to updates the cluster key. If some malicious sensor has come to know the key in current round then the key that is used in next round is hidden from this malicious sensor to minimize the data generation in compromised network.

c. ***Sensor guard key:*** This key is shared and known to a particular sensor within a cluster and a guard node only. Cluster guard uses this key to have a communication with a particular cluster member. Guard node knows the key of every sensor in its cluster but a cluster member knows a single key shared with the guard node. Cluster member uses this key to have a communication with the cluster guard of respective cluster.

5.4.2. Key Generation

There are three types of keys that are used in the system. The keys include sensor-BS key, cluster key and sensor-guard key. From these three keys, two keys (sensor-BS key and cluster key) are frequently in the system whereas the sensor-guard key is only used by all the sensors of a particular cluster whenever any sensor in that cluster is compromised. So both sensor-BS key and cluster key are generated in the network whereas the sensor-guard key is fixed. The process to generate sensor-BS key and cluster key is done using VLKM scheme given in chapter 4.

5.4.3. Key Updation

To detect a compromised sensor, any scheme is used. Detection of compromised sensor node is out of the scope of this chapter. Communication concept of a sensor node to cluster head and cluster head to base station (S-CH-BS) is used in the network, i.e. all the members of a cluster sense data from the environment and forward this data to the cluster head using cluster key known to all the members. Now the cluster head forward this data collected from all the members to the base station using its sensor key known to the sensor node and the base station. The concept of one key-one time (OKOT) is applied on cluster and sensor keys. According to the principle of OKOT, once a key is used in the system, the key is discarded and is never used again in the system in any subsequent round. Any time a key is used, the key is updated for further use as all the cluster members elect a different cluster head in each round on rotation basis to balance the energy consumption. Now this newly elected cluster head collects data from all the members with the cluster key. A sensor node uses this key to transmit the cluster data after aggregation in encrypted form to the base station to achieve aggregation secrecy and hence the cluster key is updated in every round whereas the sensor key is updated by a particular sensor whenever it uses its sensor key.

Sensor key is used by a particular sensor. If this key is compromised, there is no loss as sensor node is using a different key in the next time when this sensor node is elected as a cluster head. Since every time sensor uses its sensor key, the sensor node updates its current virtual location by moving virtually with a virtual angle and virtual speed of movement within virtual sensor boundary to update its current virtual location and a new key is generated by applying a one way hash function to update the sensor key. The old key which was compromised is discarded automatically thereafter.

If the cluster key is compromised, there is no effect on the functioning of the network as this key is automatically updated in every round to achieve the principle of OKOT. On the other hand, if a cluster member is compromised then its sensor

key and cluster key both are also compromised as sensor key is used only by a particular sensor node only, therefore it does not affect the rest of the system components. The only attack that is possible in this case is to inject false data within the system. All the uncompromised sensors stop communications with the compromised sensor node and maintain a list of IDs of compromised sensors in the cluster.

But since the cluster key used by this sensor is also compromised which is to be used by all the other uncompromised cluster members, the cluster key updation procedure does not help, as the key generation parameters and the key generation procedure is already known to the compromised sensor node. Therefore, there is need to update the key in such a way that this updated key is unavailable to any of the compromised sensor in the cluster. The solution of this problem is to have an updated cluster key after updating any one or all of the cluster key generation seed parameters. To update the cluster key, the cluster guard of the respective cluster unicasts a new cluster key generation seed values to all the uncompromised cluster members in encrypted form with the individual sensor guard key. All the uncompromised sensors update their cluster key by using VLKM scheme except the compromised sensors. Now the new cluster key made available to all the uncompromised sensors. Cluster guard sends a list containing the IDs of compromised sensors in the cluster to all the uncompromised cluster members to avoid the false data injection attack in the network. The format of the message given by the cluster guard sensor to the cluster members is given in the following message:

$$CG_i \rightarrow S_{i,j}:E_{SGK_j}(CVL,CVB,CVM,CVA,R,TS_t) \quad \cdots \quad (6.1)$$

Where CG_i is the cluster guard of ith cluster, S_{ij} is the j^{th} cluster member within i^{th} cluster, E_{SGK} is the encryption function with the help of a sensor node to guard key of j^{th} sensor within the cluster i, CVL is the Cluster Virtual Location, CVB is the Cluster Virtual Boundary, CVM is the Cluster Virtual Movement, CVA is the Cluster Virtual Angle of movement, R is the list that contains the ID of compromised cluster members and TS_t is the time stamp when cluster initial virtual location is

updated. Now all the cluster members generate a new current virtual location and updates cluster key that is available to all the uncompromised sensors only.

5.5. PERFORMANCE ANALYSIS

To evaluate the performance of any scheme, some performance measurements are necessary. For evaluating the performance of KURCS scheme, following measurements are considered:

5.5.1. Key Updation cost

Key updation cost is measured in terms of energy, i.e. the amount of energy that is consumed in updating the compromised key in the network. Two types of environments are considered in the network as given under:

a. Compromised Nodes Spreading from Particular Area Sequentially in the Network:

In this case, a compromised node is assumed to be detected in the first cluster. The second node, third, fourth and so on all nodes is compromised one by one from the first cluster. When all the nodes of first cluster are compromised, the second cluster is chosen as a victim, i.e. one by one all nodes of second cluster are compromised. In this way compromised nodes are spreading from part of the network to the entire network.

Simulation result in Figure 5.6 proves that if dynamic clustering is used then it is not known in advance that which node is elected as a cluster head and which nodes joins this cluster. That's why key updation process updates key for all those sensors that are uncompromised in the entire network. The scheme is represented as DBS (Dynamic cluster and key updation by Base Station). But on the other hand if static clustering is used, then there is no need to update the key in entire network because a sensor node is bounded to communicate with other sensor nodes of the same cluster. Therefore, instead of key updation in the entire network, the key in particular cluster is updated to which the sensor is compromised. SBS (Static cluster and key updation by Base Station) represents a scheme where key is updated by the

base station and SCG (Static cluster and key updation by Cluster Guard) represents presented KURCS scheme where the key is updated by the cluster guard rather the base station. Simulation results show that whenever entire cluster is compromised, then no energy is consumed in both SBS and SCG schemes as there is no need to update the key of any sensor node in that cluster. Simulation results prove that presented SCG scheme is efficient in terms of energy from SBS and DBS schemes.

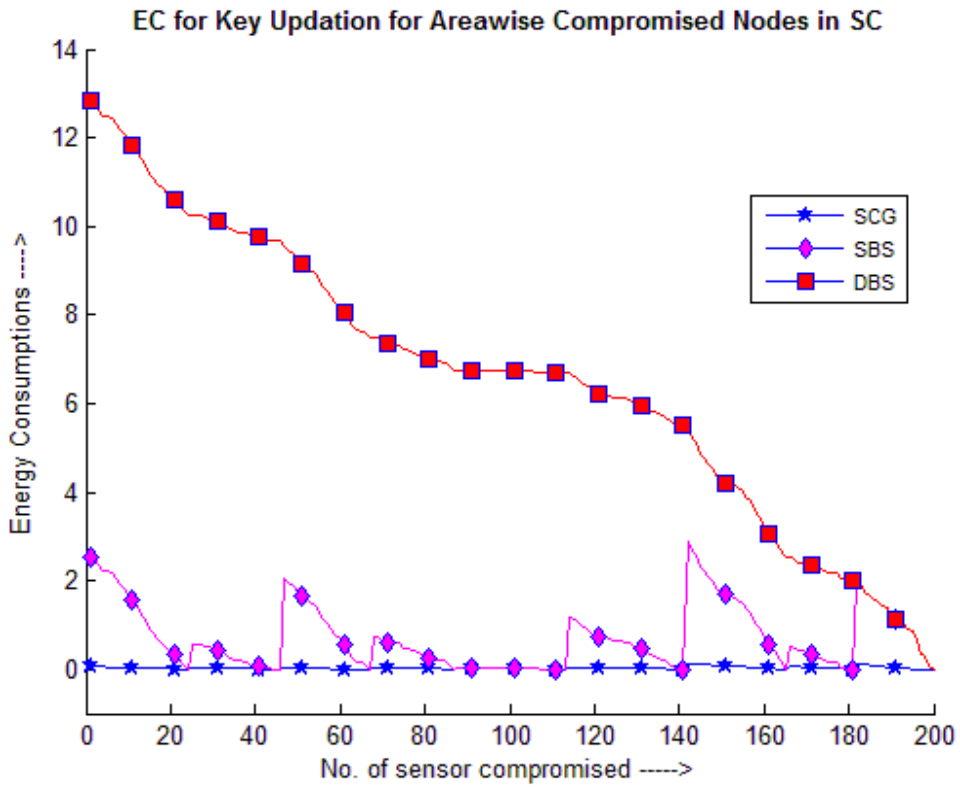

Figure 5.6: Energy Consumption in Static Clustering with Compromised Node from Area Wise Spreading in the Entire Network

b. Compromised Nodes Spreading Randomly in the Network

In this case, a compromised node is assumed to be detected at any part of the network. All nodes in the network are compromised one by one till the network gets compromised. In this way compromised nodes are spreading randomly one by one in the entire network.

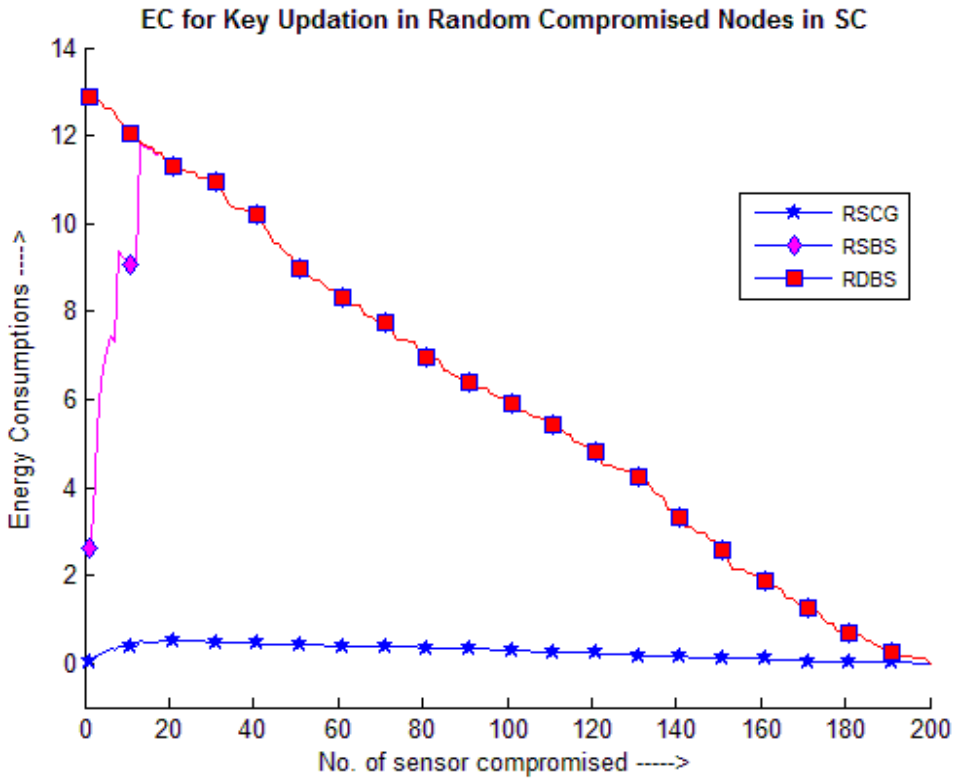

Figure 5.7: Energy Consumption in Static Clustering with Random Compromised Node from Entire Network

In Figure 5.7, RDBS (Dynamic clustering and key updation by Base Station) scheme is shown where sensor nodes are compromising randomly in the network. On the other hand, when static clustering is used and the key is updated by base station only in the cluster with at least one compromised sensor node is represented with RSBS. Similarly, when the key is updated by cluster guard in that cluster in which at least one sensor is compromised is represented with RSCG presented KURCS scheme. Simulation results prove that RSBS scheme perform in same way as RDBS scheme when at least one sensor is compromised in all the clusters in RSBS scheme. But overall the performance of RSCG scheme is better in terms of energy consumption.

5.5.2. Communication Overheads

Communication overhead is measured in terms of the number of control messages transferred in the network to update the compromised key after detecting the compromised sensor nodes in the network. The performance of the KURCS scheme depends mainly on cluster key updation process. The cluster key is updated when a sensor node is compromised and is updated by unicasting, i.e. cluster guard of the cluster from which the node is compromised unicast key generation parameters to all the cluster members which are not compromised.

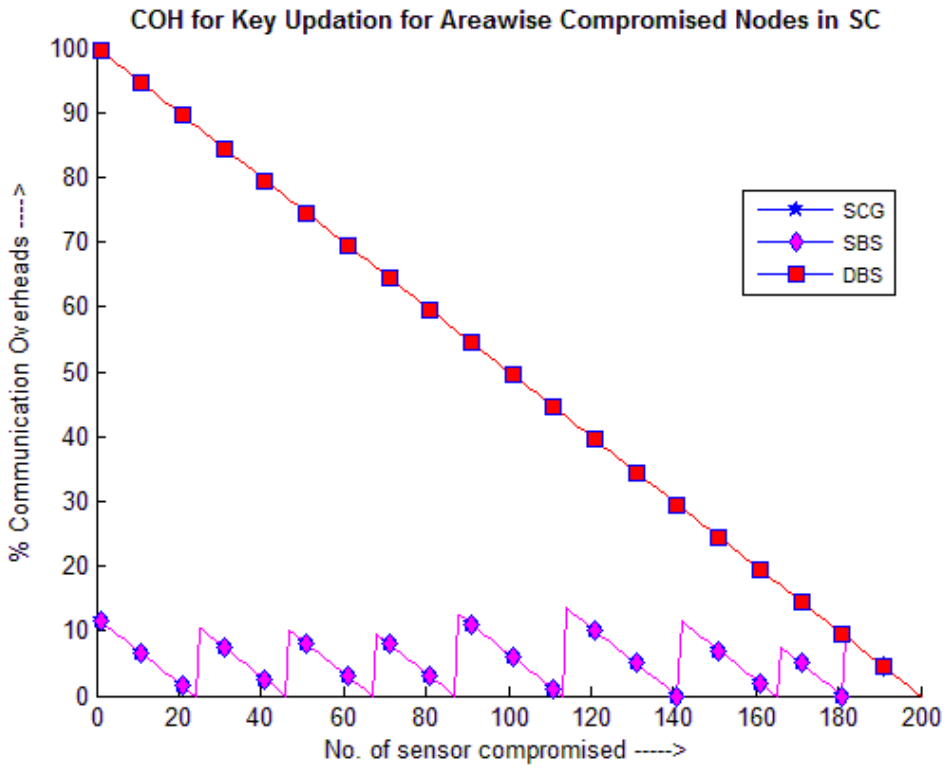

Figure 5.8: Communication Overheads in Static Clustering with Compromised Node from Area Wise Spreading in the Entire Network

Simulation results in Figure 5.8 shows DBS (Dynamic clustering and key updation by Base Station) scheme. In this scheme, key updation process updates keys for all those sensor nodes which are uncompromised in the entire network. If static clustering is used and the key is updated by the base station in particular cluster to which

the sensor is compromised is represented as SBS. Similarly SCG represent the presented KURCS scheme where key is updated by the cluster guard in particular cluster to which the sensor is compromised. Simulation results show that both SCG and SBS perform in same way in terms of communication overheads. Communication overheads are 0% when the entire cluster is compromised in both SCG and SBS schemes, but in DBS scheme, communication overheads reach to 0% whenever the network is dead, i.e. all nodes in the entire network are compromised. Simulation results prove that both SCG and SBS schemes perform better than DBS scheme in terms of communication overheads.

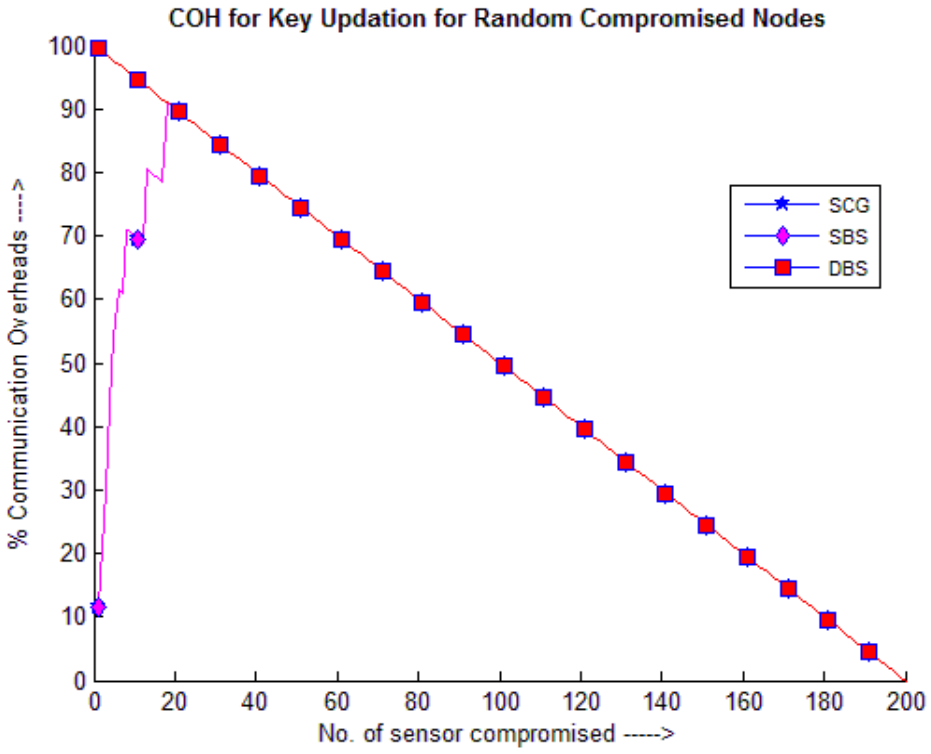

Figure 5.9: Communication Overheads with Random Compromised Node from Entire Network

In Figure 5.9, dynamic clustering is represented as DBS when key is updated by base station in the entire network whenever a ransom sensor is compromised in the network. On the other hand when static clustering is used and the key is updated by base station only in the cluster in which at least one sensor is compromised is repre-

sented with RSBS. Similarly, when the key is updated by cluster guard in that cluster in which at least one sensor is compromised is represented with RSCG which is the presented KURCS scheme. Simulation results show that both SCG and SBS schemes perform in same way in terms of communication overheads. All of the schemes perform in same way when at least one sensor is compromised in all the clusters. The performance of SCG and SBS schemes are better than DBS scheme in terms of communication overhead.

5.6. SUMMARY

This chapter presents a key updation scheme for removal and replacement of compromised sensor (KURCS) node from Wireless Sensor Networks. This scheme significantly reduces the number of transmissions needed for removing a compromised sensor node from the network. The scheme also updates the keys of all those sensors which are not compromised by using the key which is stored in the memory of compromised sensor in such a way that the updated key is unavailable to the compromised sensor nodes. This scheme is much suitable for removing and replacement of compromised sensor nodes in WSNs. Simulation results prove that this scheme performs better in terms of energy efficiency without increasing the communication overhead. In chapter-6, Dynamic Encryption Function (DEF) has been presented in detail.