TELKOMNIKA Indonesian Journal of Electrical Engineering
Vol. 15, No. 1, July 2015, pp. 128 ~ 141
DOI: 10.11591/telkomnika.v15i1.8072

Energy Efficient Intrusion Detection Scheme with Clustering for Wireless Sensor Networks

Mohammed Ali Hussain
Dept. of Electronics and Computer Engineering, KLEF University, Guntur Dist., A.P., India
E-mail: alihussain.phd@gmail.com

Abstract

Wireless sensor network (WSN) consists of a small size sensor nodes depends on battery power. Applications of sensor networks are street lighting, home automation, industrial plant, environmental parameters, health care and military. Security is becoming a major concept in the design of wireless sensor networks. Attacks on sensor networks include attack on confidentiality, integrity and availability. Lack of confidentiality means that the secret information is revealed to attackers. Lack of integrity means that the attacker modifies the contents (data) communicated in the sensor network. Lack of availability means the resources in the network is not available to authorized users. So to avoid these problems we need better security measures. In this paper we are dealing with intrusion detection. Intrusion detection plays an important role in the design of wireless sensor networks. An intruder can perform various attacks like replay, interception, worm hole, sink hole attacks. So our aim in this paper is to find such intrusions as early as possible, when they occurred and to enhance the life tome of the sensor network. This is because sensors nodes depend only on battery power. Our intrusion detection is based on clustering of the sensor network. This makes routing process, medium control and intrusion detection simple.

Keywords: *cluster head, intrusion, residual energy, TDMA, WSN*

1. Introduction

Wireless sensor networks (Figure 1) have diversified applications in various fields includes industrial plant, environmental parameters like temperature, light, rainfall, military, street lighting, home automation [1]. Many studies related to WSNs include medium access control (MAC), data collection methods and routing mechanisms. The main aim of wireless sensor network design is to optimize power (energy) consumption. This is because sensor nodes depend on small size batteries to perform operations. So more tasks require more power. Thus we need energy efficient mechanisms for wireless sensor networks. In addition to power optimization, hardware aspects are also taken in to account while designing wireless sensor networks.

In this paper we utilize the clustering option for deploying sensor nodes in the wireless sensor network. This makes the routing process and medium control simple. Each cluster has a master called cluster head (CH). All the sensor nodes within a cluster must communicate with its cluster head only. CH performs data aggregation, compaction and fusion. Data aggregation means removing repeated data received from its members and sending non redundant data to the base station. Data compaction means changing the received information short without making changes in its meaning. Fusion means CH receives data from its members by different packets and removes repeated data and then presenting it to the base station.

Wireless sensor network clustering can be mainly divided in to: homogeneous sensor clustering and heterogeneous sensor clustering. In homogeneous sensor networks, all the sensors have the same functionalities and capabilities. In these sensor networks, each cluster is assigned a cluster head. The cluster head performs communication with other cluster heads as well as the base station for performing tasks assigned to it. Several algorithms have been proposed for enhancing the network's lifetime. One such algorithm is LEACH [2]. This algorithm performs random selection of cluster heads, in case when a cluster head in a cluster drains out of energy. This is called rotating the role of cluster head, which is a very important concept in clustered WSNs. In heterogeneous network clustering consists of two types of sensors, each having different functionalities and energy requirements. In this network, sensor nodes within a

Received March 26, 2015; Revised May 13, 2015; Accepted May 29, 2015

cluster may use single hop or multi hop communication. Single hopping means the sensor nodes within a cluster can directly communicate with the cluster head, whereas multi hopping means the sensor nodes can communicate with the cluster head through some intermediate nodes. Nodes that use single hop communication requires low power to transmit data whereas nodes that use multi hop communication require high power. Nodes that use single hop communication have some problems with the nodes that using multi hop communication, this is because the nearest nodes must forward packets to cluster head received from the farther nodes, which requires much power.

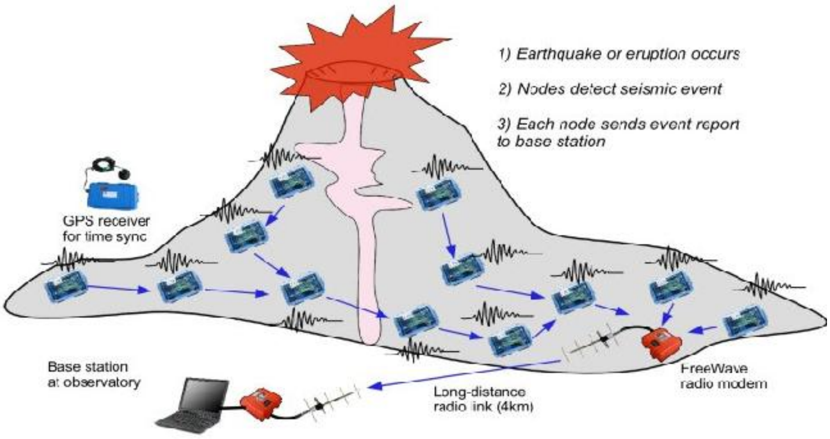
1) Earthquake or eruption occurs
2) Nodes detect seismic event
3) Each node sends event report to base station
GPS receiver for time sync
Base station at observatory
Long-distance radio link (4km)
FreeWave radio modem

Figure 1. Example Wireless Sensor Network

2. Applications of Sensor Networks

The following are the applications of wireless sensor networks:

a) Traffic Monitoring

There is need to monitor traffic at various places in a city to avoid traffic jams. This can be done with the help of wireless sensor networks. The information gathered by the sensors are sent to a central server, which then aggregated and sent to vehicle users. For example, a traffic control server sends the traffic reports to all the subscribed vehicle users about the traffic jams at various places in the city. This process can be carried out using SMS (Short Message Services) messages. Now the vehicle driver can select the roads with least traffic.

Figure 2. Traffic Monitoring

b) Military

Sensors can be used in military to monitor the enemy troop and machine movements.

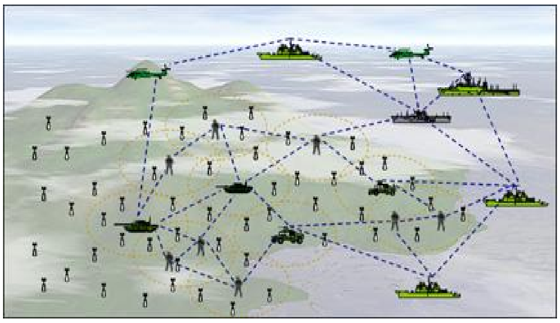

Figure 3. Military

c) Environmental Monitoring

Wireless sensor networks are used to monitor temperature, pressure, light, rainfall, etc.

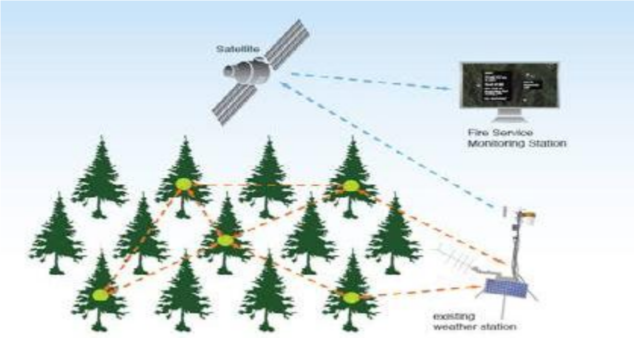

Figure 4. Environmental monitoring

d) Home Automation

Sensors are used in home appliances. For example, an air conditioner (AC) in a room can sense the room temperature and can increase or decrease the temperature. For example, during winter it increases the temperature i.e, it heats the room or during summer it cools the room by decreasing the temperature. Sensors are also used for security purpose. For example, if an unauthorized person try to steal a refrigerator from a house, then an alarm rings which informs the owner of that house.

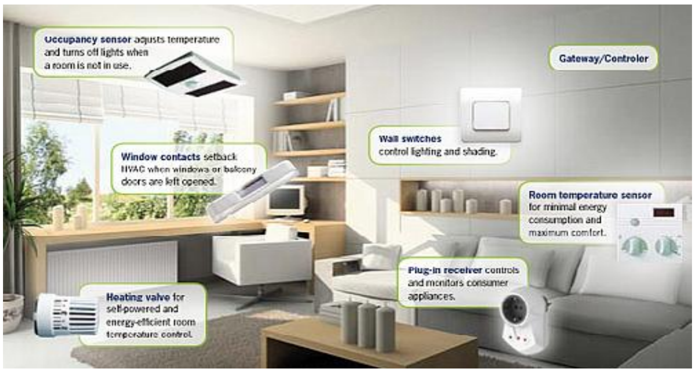
Occupancy sensor adjusts temperature and turns off lights when a room is not in use.
Gateway/Controler
Wall switches control lighting and shading.
Window contacts setback HVAC when windows or balcony doors are left opened.
Room temperature sensor for minimal energy consumption and maximum comfort.
Plug-in receiver controls and monitors consumer appliances.
Heating valve for self-powered and energy-efficient room temperature control.

Figure 5. Home appliance monitoring

e) Street Lighting

Wireless sensor networks are useful for controlling street lights. For example, during evening time, the sensor senses the light level and then switches ON all the lights in the street. During sun rise, the sensors again sense the light level and switches OFF the lights.

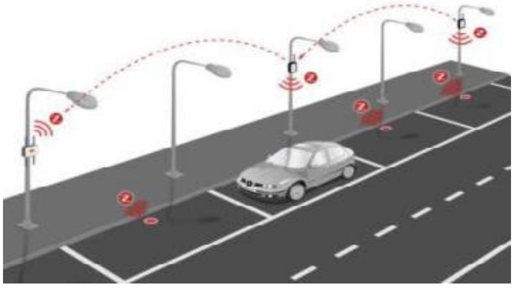

Figure 6. Street light controller

f) Medical Applications

Patients can be monitored by the sensors attached to them. For example, if the temperature level of a patient is increased then the sensors send this information to the doctor. Now the doctors take care of such patients.

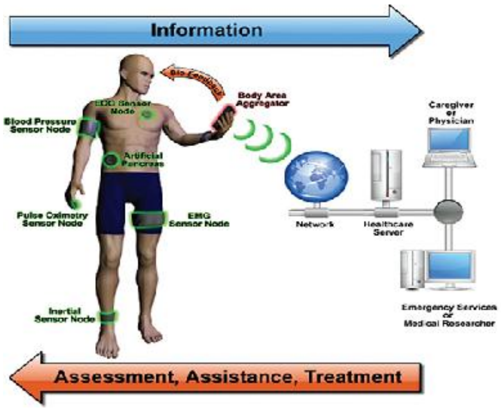

Figure 7. Patient monitoring

g) Smart Labels and RFID tags

It is used worldwide for monitoring movement of goods, movement of books in a library, electronic toll booth, etc.

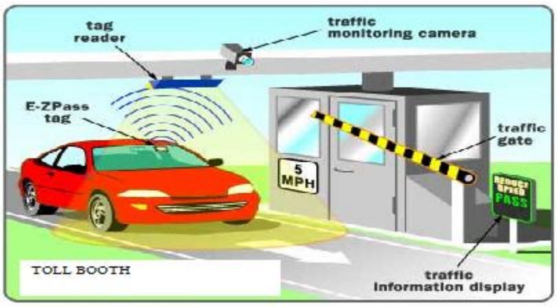

Figure 8. Electronic Toll Booth

An example using RFID technology in electronic toll booth. There are millions of drivers passing through toll booths everyday. The traditional way of collecting the toll from the vehicle owners is to stop the vehicle by the booth staff and then collect amount from them, after that the toll gate is opened for the driver to bet through the toll station. This result in huge waste of time and traffic jam created in the toll booth. So by using RFID technology, this problem can be avoided. During the registration of the new vehicle, an RFID tag is attached to it. The toll booth consists of a RFID reader. When a vehicle is passing through the toll, the RFID reader electronically debits the accounts of registered vehicle owners without requiring them to stop. In case of unregistered vehicles, while crossing the toll booth an alarm rings.

3. Attacks on WSN

3.1. Stealing Secret Data

In information security, the concept of data confidentiality means maintaining data secrecy. That is, if a sender transmits a message to a receiver, then it must be received by the corresponding receiver and not by any other user in the network. If an unauthorized person accesses that information, then it means lack of confidentiality (Figure 9). This is called interception. For example if an email is sent from a user X to user Y, then another user say Z access that email, then it is interception.

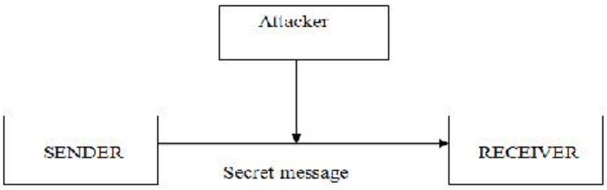

Figure 9. Lack of confidentiality

3.2. Altering Data

Altering data (Figure 10) means an unauthorized person not only obtain secret message but also modifies it. For example, user A sends a cheque for $100 to pay for the goods bought. But use C tampers modifies the message originally send by user A, which is actually destined for user B. After that user A came to know that the cheque issued is $1000. Thus it results in loss of integrity.

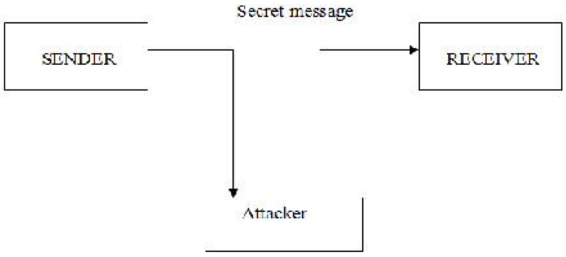

Figure 10. Lack of Integrity

The concept of data integrity is that the message received by the receiver must exactly same as the message sent by the sender and it does not modified during transmission.

3.3. Attack on Availability

Attack on availability results in interruption. The concept of interruption is the resource of a network or system is damaged, or making unavailable. For example destroying hardware components of a system or network or deleting a confidential file.

The concept of Availability states that the resources of a system or network should be available to authorized users at all times.

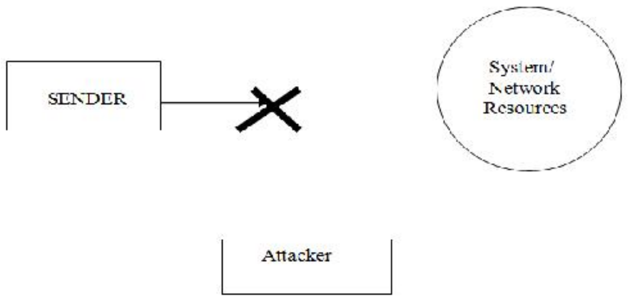

Figure 11. Lack of Availability

3.4. Fabrication

Fabrication means an unauthorized user places unwanted resources in to the network so that it can access the network easily. For example adding fake entries to a database by the attacker. Another example is an attacker can pose as an authorized user and uses the system resources.

Let an attacker C poses as user A and sends a funds transfer request (from account A's to C's account) to bank B. Upon receiving the request the bank might transfer the amount.

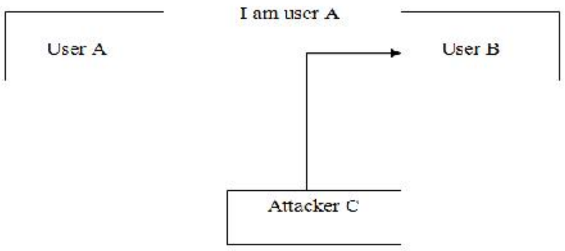

Figure 12. Fabrication

4. Clustered Organization in WSN

Clustering is a key concept for enhancing the sensor network's lifetime. Many researches have been performed on clustering of wireless sensor networks. The main aim of these researches is optimizing energy usage [3]. The idea of authors in these researches is to reduce the battery usage of each sensor node in the network and thereby enhancing the life time of the sensor network. This can be done by cutting off inter cluster communication by the way that the sensor nodes within a cluster must communicate with its cluster head only. The other way of power optimization is placing the unused nodes in sleep mode. If we combine both of these, then we can achieve more lifetime for the network.

Cluster wireless sensor networks have mainly two benefits than non clustered WSNs. They are:

a) Reducing total number of packet transmissions that floods the network. This is because; nodes within a cluster must communicate with the cluster head only.
b) Clustered WSNs used TDMA slots, thereby increasing the sleep time of the nodes. This helps in saving more power.

One might argue that, with respect to energy conservation, clustered WSNs offer two major advantages over their non-clustered counterparts: a) clustered WSNs are capable of reducing the volume of inter-node communication by localizing data transmission within the formed clusters and, more importantly, by decreasing the overall number of transmissions to the sink; b) clustered WSNs are capable of extending the nodes' sleep times by allowing cluster heads to coordinate and optimize the activities of other cluster members through some form of TDMA based scheduling.

4.1. Data Communication in Clustered WSN

The central station in a wireless sensor network called the base station performs data processing by gathering data from different clusters thereby providing processed data to end users. It is a fixed station and is situated at a greater distance from the cluster nodes. The base station acts as a sink for all the cluster heads in the sensor network. The cluster head acts as a sink for the nodes within its cluster. The main task of a cluster head is:

a) Acts as a coordinator and performs data aggregation, compaction and fusion.
b) Communication with the base station via single hop or multi hop.

There can be many intermediate nodes between the base station and the cluster heads which form a hierarchical structure, where the base station is located at the root and the sensor nodes within the clusters located at the leaves. Figure 13 shows the data communication process in the clustered wireless sensor network.

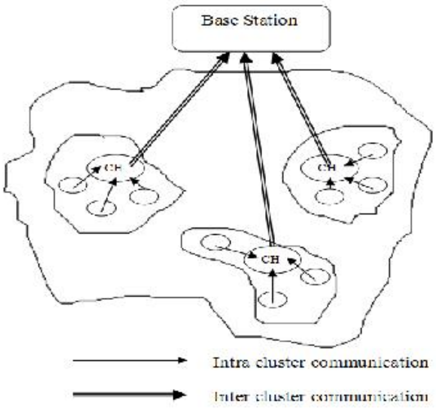

Figure 13. Data communication in WSNs

5. Related Work

It is a difficult task to setup a wireless sensor network that is attacker proof. So sensor networks are designed so that they can be self aware and can withstand any type of attack. That is they should have the ability to detect intrusion and take necessary precautions to recover from it. An intrusion is a illegal activity performed by attackers. So a wireless sensor network requires an intrusion detection system to withstand various attacks. An intrusion detection system (IDS) is a set of techniques to help discover and inform about the intrusions. Many researches have been performed on intrusion detection. An IDS must be integrated in to the sensor network during its deployment [4]. In [5] and [6], the authors proposed an intrusion detection mechanism that uses a special type of nodes called monitoring nodes. The task of these nodes is to observe its neighbour nodes. These nodes observes the packet transmission and kept them in their buffers and given as input to intrusion detection system. If any misbehaviour found, then it is consider as intrusion.

In [7], the authors focus on selfish nodes. These nodes try to enhance their resource usage. In [8] and [9], the authors proposed some intrusion detection systems which is based on the concept that routing protocols in MANETs can be used in sensor networks. In all these research work, no cooperation among nodes is considered. Collaboration between sensor nodes is very helpful in attacks like selective forwarding [10] and sinkhole attacks [11]. In [12], the authors proposed an intrusion detection system for MANETs [12]. Such networks require cooperation among sensor nodes and also require a distributed intrusion detection system. In this paper, we focus on detecting intrusions by clustering the entire sensor network. Our first task is dividing nodes in to clusters, then removing overlapping of sensor nodes within the clusters, so that the nodes can cover much area in the cluster. After this, cluster heads are elected for each cluster. Now nodes within a cluster communicate with the base station through their cluster head. A special node called master node in introduced. This will be helpful during rotation of cluster head, if cluster head is compromised and to detect intrusions outside the clusters.

6. Optimal Cluster Formation

In this section clustering of wireless sensor nodes is introduced. The clustering should be optimal, this means it should be energy efficient. To design such energy efficient clustering sensor network, some questions may arise. One question is how many sensor nodes form a cluster. Another question is what the size of the cluster is. Another one is how many such clusters should be formed. For clustering purpose, in this paper we use mountain clustering technique [13]. This technique finds the cluster centres by calculating a function called mountain function. This function is also called density function. It first selects a point in the data space of a sensor network and then selects the point with highest density as the cluster centre. This process has been performed until we get the required number of clusters. The steps in mountain clustering are as follows: First forms a grid space with the help of grid lines in the sensor network. The intersection of these lines forms the centres of each cluster. Let this set be S. Now construct a density function that is used to denote a data density measure. The height of the density function at a position s $\in$ S is given as:

$$m(s) = \sum_{i=1}^{N} \exp\left(-\frac{\| s - x_i \|^2}{2\pm^2} \right)$$

Where x_i is the ith position in the data space and ± is a constant. This equation specifies that the density of the data space is affected by all the data space positions.

The next step is selection of the centre of each cluster by destruction of the density function. Let c_1 be the centre of the first cluster with highest density measure. Now generate a new mountain function by revising the old function. This can be done by subtracting a scaled Gaussian function centered at c_1:

$$m_{new}(s) = m(s) - m(c_1)\exp(-\frac{\| s - c_1 \|^2}{2\ ^2}$$

This formula is used to eliminate the effect caused by initial cluster. Now generate a new mountain function using the centre of the second cluster formed. Continue this process until, the required number of clusters have been formed. After forming the clusters, the sensor nodes in each cluster must be redistributed so that they cover the entire cluster without overlapping. Figure 14 shows the overlapped transmission ranges of sensors within a cluster.

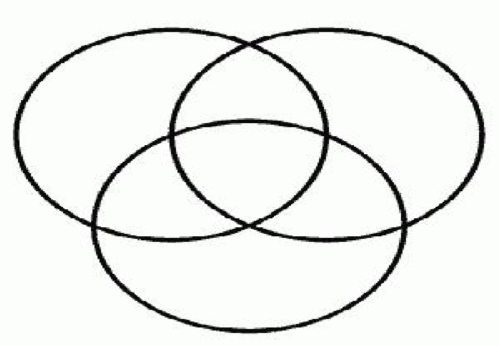

Figure 14. Sensor transmission range overlapping

Rearrange the sensors within each cluster: Let two sensors are placed on the coordinates (x1,y1) and (x2,y2) with radius r1 and r2 respectively. First determine the overlapping of the transmission ranges of the sensors by using the formula:

$$D= \sqrt{(x2-x1)^2+(y2-y1)^2}$$

Removing overlapping of the sensors by using the following formula, so that the sensors can cover more area:

$$Y2= \sqrt{((r1+r2)^2-(x2-x1)^2)+y1}$$

Repeat this process until the overlapping is sufficiently reduced. Now deploy sensors on new coordinates within the cluster. Figure 15 shows the entire clustered network.

7. Rotation of Cluster Head

The cluster head (CH) is the main node within each cluster. It performs various tasks like data gathering from sensor nodes within the cluster, aggregate the collected data and forward them to master nodes and then to base station. Since it incurs more processing than non cluster heads, they require more energy to perform those tasks. So cluster heads drown out their energy much faster than normal sensor nodes. Then there is a need to rotate the roles of cluster heads. This means assigning the task of CH to other efficient node within that cluster. The important question here is when wee need to rotate the cluster head? The solution is based on the residual power of the cluster head. Whenever the residual power of a cluster head is below some threshold value then there is a need to rotate that cluster head.

Let a cluster head CH_i finds that its residual energy level falls below some threshold T. Now it informs the master node for rotating the roles. Now the master nodes starts the rotation of the CH. The master node informs this to all other CHs in the network. Now all the CHs in the network obtain their cluster's residual powers by using TDMA slots. The maximum residual energy computer by a cluster head in its cluster is:

$$E_{res_i,\max} = \max_{j \in Ni_i^R}\{E_{res_j}\}$$

Where E_{res_i} is the residual energy of node i. This formula will be used to find nodes with high residual energy to select them as new CH. The relative residual energy level is calculated by using the formula:

$$P_i = \frac{E_{res_i}}{E_{res_i,\sup}}$$

Where,

$$E_{res_i,\sup} = \max_{j \in H \cap N_i^{2R+e}}\{E_{res_i,\max}\}$$

After calculating the residual energy then select a new CH with high residual power. After selecting a new CH, the nodes within the cluster of that CH communicates with its only. Before selecting the new CH, the nodes can communicate with the master node. The nodes can communicate with the CH or master node by using TDMA slots. Each node has its turn to send its data to the CH. Now CH aggregates this data and send to base station through master node. During these data transmissions, the nodes are not allowed to send their residual energies. They are allowed only during the rotation of the roles of cluster heads.

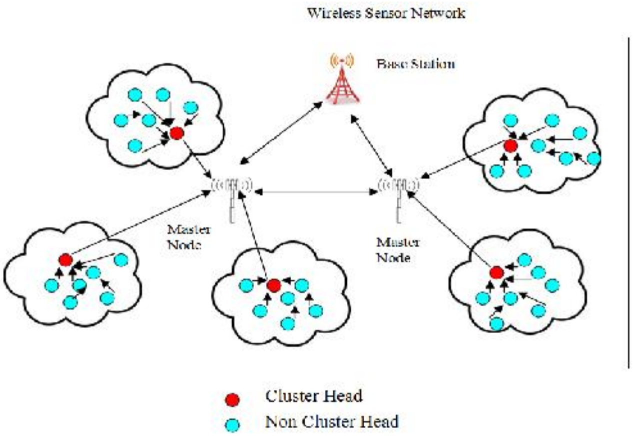

Figure 15. Clustered Wireless sensor network

8. Intrusion Detection

Intrusion detection is an important aspect in the filed of wireless networks. In our proposed work, intrusions can be detected by two ways: Detection by nodes within the cluster and detection by nodes outside the cluster.

8.1. Detection within a Cluster

When an intruder enters into a cluster, then it is the duty of the inside nodes to detect that intrusion. Figure 16 shows that an attacker node enters into the transmission range of a non CH sensor node.

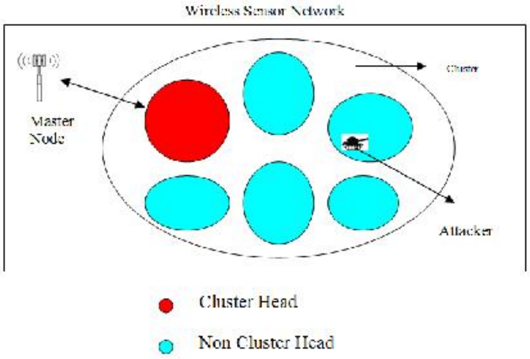

Figure 16. Attacker node inside a cluster

When a non CH node detects an intruder, then it informs its cluster head. Now cluster head sends this information to the base station through a master node. Now the base station alerts all other nodes in the network about that intrusion.

8.2. Detection Outside the Cluster

When an attacker node starts at a random point in the network, say outside of all the clusters, and then it is difficult to detect it by the nodes within each cluster, until the attacker enters into a cluster. This situation takes more time to detect the attacker. But our aim is to detect the attacker as fast as possible in order to avoid damage to the network. To do this, we introduce a new type of node called Master node, which has high battery power and longer transmission ranges. A master node can communicate with two or more cluster heads. The master nodes can be used to relay data from cluster heads to base stations. Figure 17 shows an attacker node starts at a random point in the network.

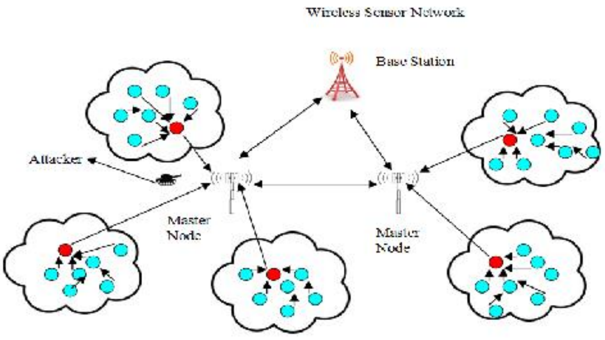

Figure 17. Attacker outside the clusters

Whenever an attacker node enters in to the transmission range of a master node, then it senses it and informs to the base station as well as all cluster heads connected to it. Now the base station informs this information to other master nodes. This process reduces the time taken to identify the attacker.

The solutions proposed above are fine but what happened if a non CH node with in a cluster was compromised. If a node within a cluster is attacked by the intruder then it must be deactivated(all the communication links from it are removed) and that node is removed from the network. This is done by CH of that cluster. This is shown in Figure 18.

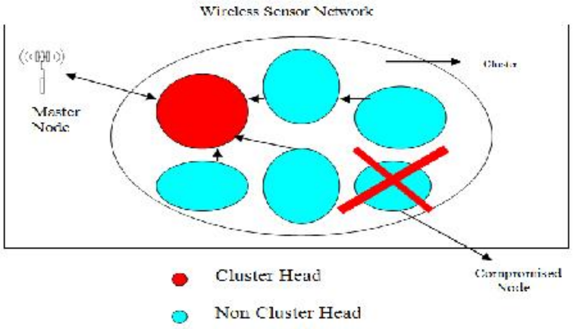

Figure 18. Compromised node deactivation and removal

If the CH node is compromised, then the master node deactivate it and now the master node acts as the CH for that cluster until a new CH is selected. Now all the nodes in that cluster can communicate with the master node. This is shown in Figure 19.

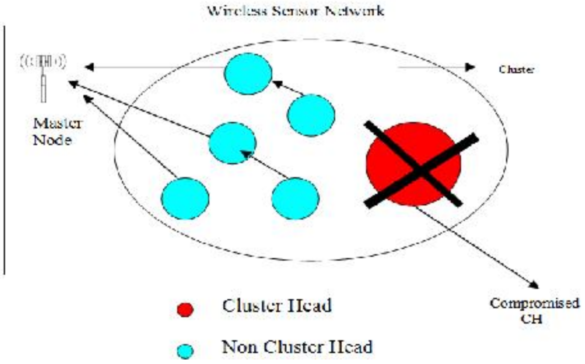

Figure 19. Compromised CH deactivation and removal

The proposed work is summarized in the following algorithm:
Algorithm

Cluster Formation:
Step 1: Deploy sensor nodes
Step 2: Form clusters by using mountain clustering:
Step 3: Form Grid G
Step 4: Construct a mountain function with height-

$$m(s) = \sum_{i=1}^{N} \exp\left(- \frac{\| s - x_i \|^2}{2\pm^{2}} \right)$$

Step 5: Select cluster center by destructing mountain function
Step 6: Obtain new mountain function is formed by subtracting a scaled Gaussian function centered at c_1 :

$$m_{new}(s) = m(s) - m(c_1)\exp(- \frac{\| s - c_1 \|^2}{2 \ {}^{2}}$$

This results in forming another cluster
Step 7: Repeat **step 6** until sufficient clusters are formed.

Overlapping Removal:
Step 1: Rearrange the sensors within each cluster: Let two sensors are placed on the coordinates (x1,y1) and (x2,y2) with radius r1 and r2 respectively. First determine the overlapping of the transmission ranges of the sensors by using the formula:

D= $\sqrt{(x2 - x1)^2 + (y2 - y1)^2}$

Step 2: Removing overlapping of the sensors by using the following formula, so that the sensors can cover more area:

Y2= $\sqrt{((r1 + r2)^2 - (x2 - x1)^2) + y1}$

Repeat this step until the overlapping is sufficiently reduced.
Step 3: Now deploy sensors on new coordinates within the cluster.

Intrusion Detection:

```
if attacker node detected
    then inform to cluster head. Now cluster head transmits
     this information to base station through master nodes.
end if
if  a sensor node within a cluster is compromised
     then CH deactives it and remove from the cluster
end if
if a CH is compromised
     then master node deactivates it and acts as CH until a
     new CH is selected.
 end if
```

Cluster Head Rotation:

```
if the energy of a CH is drown out
    then calculate residual energy and select another CH.
else if CH is compromised
    then select a most effective node as CH
end if
```

Figure 20 illustrates the flow chart of our proposed work.

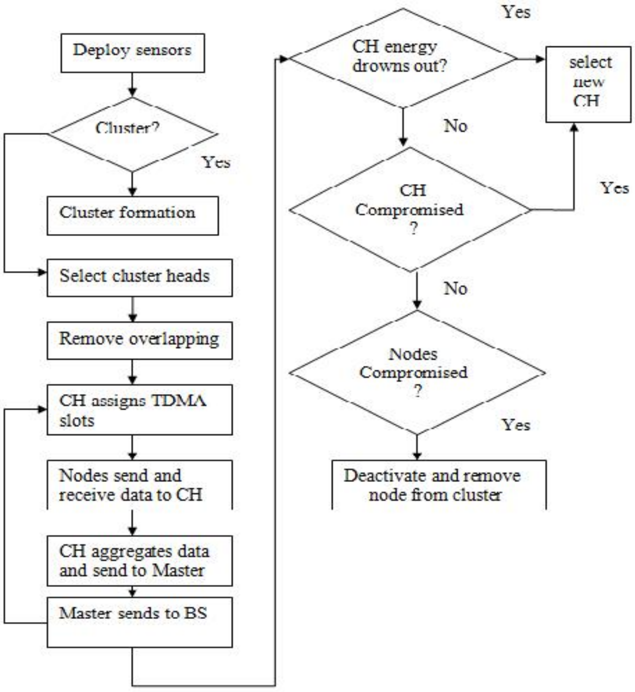

Figure 20. Flowchart of proposed work

9. Conclusion

Enhancing the lifetime of the sensor network and at the same time maintaining proper security is an important aspect in wireless sensor networks. In this paper we use the concept of clustered wireless sensor networks. Clustering is a key concept for enhancing the sensor network's lifetime. Cluster wireless sensor networks have mainly two benefits than non clustered WSNs. They are: reducing flow of packets through the network and saving energy by placing unused nodes in sleep mode. The first task in this paper is forming clusters after deploying sensors in the field. After that a cluster head is selected for each cluster. To cover most of the clustered area, overlapping between the clusters were removed. Later communication begins between the CH and its members. The members of a cluster must only be communicating with its CH only. The CH of a cluster is rotated only if CH drowns out its energy or when it is compromised. Role rotation helps in reducing the burden on CH nodes. Beyond this a new type of node called Master node was introduced. It helps to relay messages from CH to base station and plays the role of CH when CH of a cluster was compromised. Another task of the master node is to select a new CH, when there is a need to change CH of a cluster.

References

[1] IF Akyildiz, et al. Wireless Sensor Networks: A Survey. *Elsevier Comp. Networks.* 2002; 3(2): 393-422.

[2] WR Heinzelman, AP Chandrakasan, H Balakrishnan. An application-specific protocol architecture for wireless microsensor networks. *IEEE Transactions on Wireless Communications.* 2002: 660-670.

[3] Ignacio Solis, Katia Obraczka. *Isolines: Energy efficient mapping in Sensor Networks.* Proceedings of the 10th IEEE Symposium on Computers and Commnications (ISCC'05). Cartagena, Spain. 2005.

[4] M Ngadi, AH Abdullah, S Mandala. A survey on MANET intrusion detection. *International J.Computer Science and Security.* 2008; 2(1): 1-11.

[5] AP da Silva, M Martins, B Rocha, A Loureiro, L Ruiz, HC Wong. *Decentralized intrusion detection in wireless sensor networks*. In Proceedings of the 1st ACM international workshop on Quality of service & security in wireless and mobile networks (Q2SWinet '05). 2005: 16-23.

[6] I Onat, A Miri. *An intrusion detection system for wireless sensor networks*. In Proceeding of the IEEE International Conference on Wireless and Mobile Computing, Networking and Communications. 2005; 3: 253-259.

[7] F Kargl, A Klenk, M Weber, S Schlott. Sensors for detection of misbehaving nodes in MANETs. In U. Flegel, M Meier. *Editors.* Detection of Intrusions and Malware & Vulnerability Assessment, GI SIG SIDAR Workshop, DIMVA 2004. Dortmund, Germany. 2004: 83-97.

[8] CE Loo, MY Ng, C Leckie, M Palaniswami. Intrusion detection for routing attacks in sensor networks. *International Journal of Distributed Sensor Networks.* 2005.

[9] V Bhuse, A Gupta. Anomaly intrusion detection in wireless sensor networks. *Journal of High Speed Networks.* 2006; 15(1): 33-51.

[10] I Krontiris, T Dimitriou, FC Freiling. *Towards intrusion detection in wireless sensor networks*. In Proceedings of the 13th European Wireless Conference. Paris, France. 2007.

[11] I Krontiris, T Dimitriou, T Giannetsos, M Mpasoukos. *Intrusion detection of sinkhole attacks in wireless sensor networks*. In Proceedings of the 3rd International Workshop on Algorithmic Aspects of Wireless Sensor Networks (AlgoSensors 07). Wroclaw, Poland. 2007.

[12] A Mishra, K Nadkarni, A Patcha. Intrusion detection in wireless ad hoc networks. *IEEE Wireless Communications.* 2004; 11(1): 48-60.

[13] Jang JS. R Sun CT, Mizutani E. Neuro- Fuzzy and Soft Computing – A Computational Approach to Learning and Machine Intelligence. Prentice Hall.