*ISSN: 2278 – 1323*
*International Journal of Advanced Research in Computer Engineering & Technology*
*Volume 1, Issue 4, June 2012*

# Intrusion Detection Based Security Solution for Cluster Based WSN

Shilpa S.Patil
M.Tech (CSE),
Department of PG Studies, VTU, Belgaum.
Email- s123shilpa@gmail.com

P.S.Khanagoudar
Professor,
Department of CSE,
GIT, Belgaum
Email-khanagoudar@yahoo.com

## ABSTRACT

Wireless sensor network (WSN) can provide low cost solution to variety of real-world problems. Sensors are low cost tiny devices with limited storage, computational capability and power. they can be deployed in large scale for performing both military and civilian tasks. Security will be one of the main concerned when they will be deployed in large scale

In wireless network however one cannot make assumption that wireless users are trusted. Malicious individuals could easily disrupt the network & is critical to protect a sensor network from such malicious attacks, which presents a demand for providing security mechanisms in the network. In this project, we propose a new approach of Security Solution for Cluster-Based Wireless Sensor Networks. In the proposed methodology, an efficient MAC address based intruder tracking system has been developed for early intruder detection and its prevention.

**Keywords**: Wireless Sensor Networks (WSNs), Cluster Head (CH), Base Station (BS), Intrusion Detection System (IDS)

## 1Introduction

Security is becoming a major concern for protocol designers of WSN because of the broad security-critical applications of wireless sensor networks (WSNs). To protect a network, there are usually several security requirements, which should be considered in the design of a security protocol, including confidentiality, integrity, and authenticity. An effective security protocol should provide services to meet these requirements. In many cases, no matter how carefully we design a security infrastructure for a network, attackers may still find a way to break into it and launch attacks from the inside of the network. If they just keep quiet to eavesdrop on traffic flows, they can stay safe without being detected. If they behave more actively to disrupt the network communications, there

will be some anomalies, indicating the existence of malicious intrusion or attacks. An intrusion can be defined as a set of actions that can lead to an unauthorized access or alteration of the wireless network system. Intrusion detection mechanisms can detect malicious intruders based on those anomalies. Intrusion detection system (IDS) attempts to monitor computer networks and systems, detecting possible intrusions in the network, and alerting users after intrusions had been detected, reconfiguring the network if this is possible [1], [2]. Usually, the neighbors of a malicious node are the first entities learning those abnormal behaviors. Therefore, it is convenient to let each node monitor its neighbors such that intrusion detection mechanisms can be triggered as soon as possible.

In case of cluster-based hierarchical routing wireless sensor network, network topology depend on communication range of the nodes, location information, distance between the nodes and remaining battery power [2],[3],[7]. An intruder can manipulate these parameters to mount spoofed, altered, or replayed routing information attack and attract the network towards it to create a sinkhole. This sink hole may turn into black hole if it absorbs the data completely. These protocols transmit data in multi-hop so intermediate nodes take the responsibility of data aggregation/fusion and forward data to upper level. An adversary who joins the network in setup phase can selectively forward data to upper level and change the data to lead data integrity attack. Attacker can mount adversary nodes with same id in different place of the network and actively join the network. These nodes generate the false data and disrupt the data communication. Also, in multi-hop hierarchical routing, whenever a node sends data to another node, it expects an acknowledgement from the receiving node. Adversary nodes may take the benefit of this and send false acknowledgement for weak and dead nodes to convince the network as alive. In this paper, we propose Intrusion Detection Based Security Solution for Cluster-Based Wireless Sensor Networks. The paper is organized as follows. Section 2 summarizes the related previous works. Section 3 describes the proposed security system. Conclusion is given in Section 4.

## 2.RelatedPrevious Work/Literature Survey

**[1.] Kamal Kant, Nitin Gupta , "Application based Study on Wireless Sensor Network" International Journal of Computer Applications (0975 – 8887).**

In this paper we discuss overview of the wireless sensor network, types of sensor networks, how it works, how differ from the tradition network, and challenges, features, protocol stack of the sensor network, Applications of wireless sensor network. But wireless sensor networking has a bright future in the field of computer networking because we can solve the monitoring problems at an advanced level in the future with the help of such technology of networking. From this paper it was helpful to find the basic concepts on wireless sensor networks.

**[2.] P. Mohanty, S. A. Panigrahi, N. Sarma, and S. S. Satapathy, "Security Issues in Wireless Sensor Network Data Gathering Protocols: A Survey" Journal of Theoretical and Applied Information Technology, 2010, pp. 14-27.**

This paper outlined different security issues in wireless sensor network in general and made an extensive study of different threats associated with existing data gathering protocols. As these protocols are not designed taking security issues into account, most of them are prone to different types of attacks. Even some of the protocols are seems to be vulnerable to most of the attacks. Similarly some attacks like HELLO flood, Acknowledgement spoofing and sniffing can be used by the adversaries to affect most of the protocols. From this paper it was helpful to find the different types of attacks that exist in wireless networks.

**[3.] C.C. Su, K.M. Chang, Y.H. Kue, and M.F. Horng, "The new intrusion prevention and detection approaches for clustering-based sensor networks", in Proceedings of 2005 IEEE Wireless Communications and Networking Conference (WCNC'05), vol. 4, New Orleans, L.A., Mar. 2005, pp. 1927-1932.**

The two approaches to improve the security of clustering-based sensor networks: authentication based intrusion prevention and energy-saving intrusion detection. In the first approach, different authentication mechanisms are adopted for two common packet categories in generic sensor networks to save the energy of each node. In the second approach, different monitoring mechanisms are also needed to monitor cluster-heads and member nodes according to the importance of them. When monitoring

cluster-heads, member nodes of a cluster-head take turns to monitor this cluster-head. This mechanism reduces the monitor time, and therefore saves the energy of the member nodes. When monitoring member nodes, cluster-heads have the authority to detect and revoke the malicious member nodes. This also saves the node energy because of using cluster-heads to monitor member nodes instead of using all the member nodes to monitor each other. However, a disadvantage of the proposed key management mechanism is that sensor nodes cannot move and new sensor nodes cannot be added after the pairwise keys are established. This paper was helpful in finding the different detection approaches for cluster based network.

**[4.] C.C. Su, K.M. Chang, Y.H. Kue, and M.F. Horng, "The new intrusion prevention and detection approaches for clustering-based sensor networks", in Proceedings of 2005 IEEE Wireless Communications and Networking Conference (WCNC'05), vol. 4, New Orleans, L.A., Mar. 2005, pp. 1927-1932**.

Continuous monitoring may be energy consuming, which is not desirable in WSNs. Therefore, a cluster-based detection approach is developed for WSNs. In this approach, a network is divided into clusters. Each cluster head monitors its cluster members. All the members in a cluster are further divided into groups and the groups take turns to monitor the cluster head. Not all the sensor nodes keep monitoring, thus reducing the overall network energy cost.

**[5.] I. Khalil, S. Bagchi, and C. Nita-Rotaru, "DICAS: Detection, diagnosis, and isolation of control attacks in sensor networks", in Proceedings of the 1st IEEE International Conference on security and Privacy for Emerging Areas in Communications Networks (SecureComm'05), Athens, Greece, Sept. 2005, pp. 89-100**.

The security protocol proposed in this paper uses local monitoring, in which a neighbor of both a sender and a receiver can oversee the communication behaviors of the receiver. If the receiver has any abnormal behavior on the received packets, it may be detected. If the number of abnormal behaviors is larger than a threshold, the neighbors of the detected malicious node refuse to receive packets from and send packets to it so that the malicious node is isolated from the network.

**[6.] S. Ganeriwal and M. Srivastava, "Reputation-based framework for high integrity sensor networks", in Proceedings of the 2nd ACM Workshop**

**on Security of Ad Hoc and Sensor Networks (SASN'04), Washington,**
**DC, Oct. 2004, pp. 66-77.**

In this paper a reputation-based framework is established, in which each node holds reputations for other nodes. Based on the observations of whether other nodes are cooperative or not, those reputations are updated through an iterative procedure and are used as criteria to decide whether a node is malicious or not

## 3. Proposed System:

Intrusion detection in WSNs by characterizing intrusion detection with respect to the network parameters. Two detection models are: Single-sensing detection and Multiple-sensing detection models .These are two detection models. We are detecting the intruder both single sensor and multiple sensor heterogeneous wireless sensor network.

**Disadvantage:**

1 .The sensed information provided by a single sensor might be inadequate for recognizing the intruder.

2. So that there is no guarantee for our information has been sent securely.

**Advantage:**

1. Through sensing the network we able to find possible node in the wireless Sensor network.

2. By finding the intruders we can send our information in a secured manner.

### 3.1 Layout of WSN

A wireless sensor network (WSN) is homogeneous and highly distributed network of tiny, low cost, low wireless devices (called sensor node or motes) deployed in large numbers.

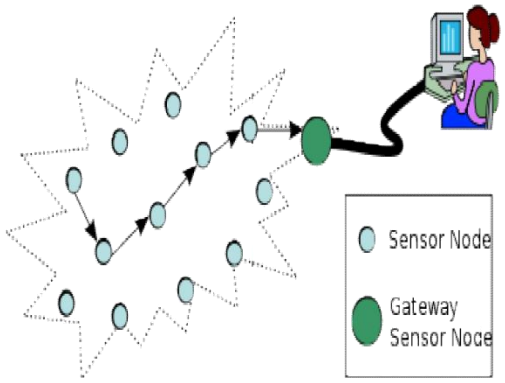


**Fig 1:WSN Architecture**

### 3.2 Clustering in WSN:

Clustering are formed in WSN to facilitate many network operations such as aggregation & for efficient & scalable in network processing. E.g: Data Aggregation, Routing, DataQuery, & broadcast. Clustering is introduced because of its

network scalability ,energy saving attributes & network topology stability. Clustering scheme reduces the communication overheads, there by decreasing the energy consumptions & interferences among sensor nodes Advantages of clustering scheme are: low/less overhead, easy maintenance.

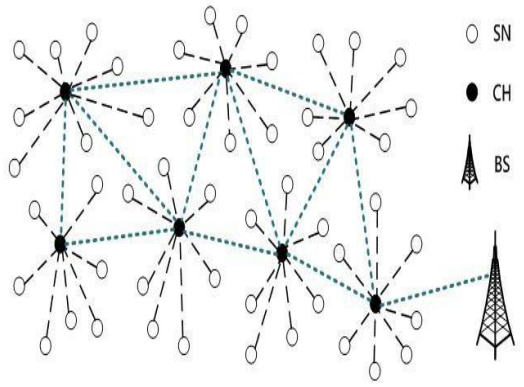


**Fig2 : Clustering in WSN**

## 3.3 Communication

Communication among the nodes and CH in a WSN is through HELLO messages, sending the requests (ACK) and receiving the responses. Mainly the concept of routing table is maintained where in it keeps track of the nodes information, their neighbor nodes, destination nodes and source nodes, etc. Hence, the nodes in the network can communicate and identify their neighbor nodes in the network which are the first entities to know about the intruder in the network .

### 3.4 Routing

Routing in wireless sensor networks differs from conventional routing in fixed networks in various ways: There is no infrastructure, wireless links are unreliable, sensor nodes may fail, and routing protocols have to meet strict energy saving requirements. Routing protocol used in the present context primary and alternate route. Here, it uses broadcast and limits to multicast technique. Here, we refer the multipath technique in the sensor networks.

### 3.5 Technology Used

In order to detect the intruder/malicious node in the WSN network, the concept of port numbers, IP address, MAC address are used. We setup the network initially considering the multisensor and single sensor networks. In the first network multiple nodes are considered whereas in second network single nodes are considered, hence named as single and multiple sensor nodes as shown in figure 3

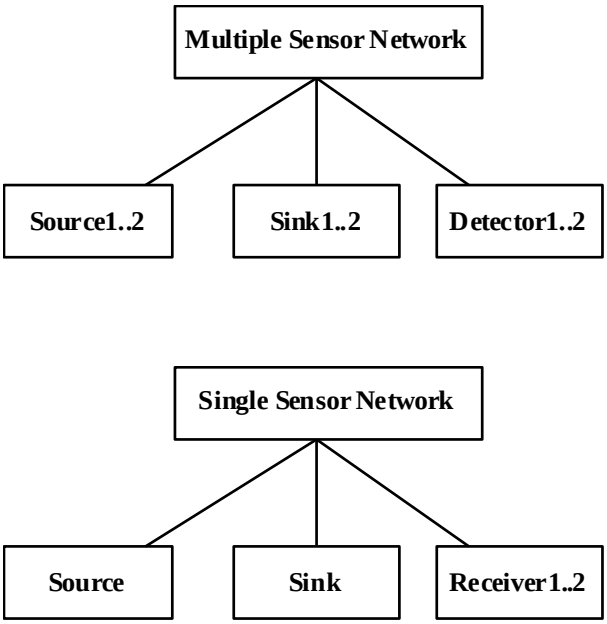


**Fig 3: Architectural Diagram**

**3.5 Possible intrusions in the network:**

In the present technology traffic in the network is increasing leading to various effects on the network operations like data transmition time, throughput, bandwidth consumption, unwanted messages, data loss, link breakage all these and other effects leads to energy consumption which forms the major and an serious issue to the WSN as they are battery constrained and are irreplaceable one by any other sources[1]. The main cause of the traffic in network are the intruders in the network. Where in they can harm the network in fallowing ways:

1. By creating the duplicate node
2. By creating duplicate CH

Once an intruder enters the network they initially search for the nearest node , on finding nearest node they try to create the duplicate node of the real node. And acts like the actual real node and takes part in the transmition of the information and harms the network. Hence we need to detect such malicious node existing in the network. The concept we use to identify such nodes are using Port number, IP address, MAC address. Using the port number concept we authenticate the nodes. If the nodes are not assigned the actual port number than the detector node using the concept of IDS detects the intruder and gives the alarm message that intruder is detected[3].

Nodes considered in this system are: source, sink, detector, receiver. **Source node operations**: To gather the message, To select the port number (Authentication),Packetization, Displays the status information about the nodes. As a basic concept of the networking systems the message which is to be transmitted over the network needs to be divided into packets. Further the packet length depends on the type of wireless network used. Here, in WSN the length is 48 octets.

**Sink node Operation:** 1.Only one task is to synchronize the information. Detector node operations: Using the developed system i.e.

IDS and using the concept of HIDS it detects the intruder, Gives the alarm message about detection to user.

**Receiver node operations:** This node receives the information from the detector node, It gives the information about the packet number, information received.

**Note**: packet length is calculated at each and every time.

**Function of the Base Station:**

1. All nodes are able to send data to BS via Cluster Head.
2. Base station has all the information regarding each Cluster (number and MAC address)
3. The removal or addition of any node in a Cluster is monitored by the Base Station.
4. Poll status of each node is received with MAC address.
5. Base station runs task of MAC address tracking, MAC address history and management of database.
6. The Base Station has the capability to seize the operation of any node in the network .

Flow chart in Fig. 4 illustrates the logic of the proposed intrusion detection based security solutions for cluster-based wireless sensor networks.

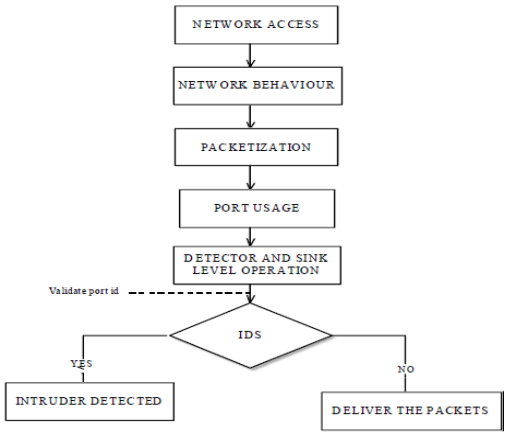


**Fig:4 IDS Flow Diagram**

## Effect on Energy Efficiency of the Wireless Network:

1.Same energy is used for sending any message to one or many receivers. Hence, if an intruder is reading the data (in listen node) sent by any node, no additional energy is used by that node.

2.When an intruder tries to replace a node or CH, number of send/receive messages are executed. In such case, the send and receive messages are limited as the BS takes immediate action to block the intruder.

3. Minimal energy is spent to revive the effected part of wireless network

## Steps for preventing future attacks:

1 Ensure that the security algorithm / firewall in the Base Station is updated

2. An automatic system could be designed which changes the working frequency and

channel of the wireless network when an intruder attacks the network.

3. A more rugged encryption and user authentication system to be deployed

## 4.Conclusion

In this paper we have illustrated MAC address, IP address, Port Number based intruder tracking system for cluster based wireless sensor networks. This proposed system is very energy-efficient for early detection and prevention of security threats and attacks. Early detection and prevention of the intruder by efficient security system can prevent many problems like slowing down of the network, sending of fake data, etc. By designing a security system in which the Base Station (BS) keeps track of the security of the Wireless network, high security can be ensured without any significant energy overheads on individual nodes and cluster heads.

## REFERENCES

[1]. Kamal Kant, Nitin Gupta, "Application based Study on Wireless Sensor Network**",** International Journal of Computer Applications (0975 – 8887) Volume 21– No.8, May 2011.

[2]. Al-Sakib Khan Pathan,Hyung-Woo Lee,Choong Seon Hong, "Security in Wireless Sensor Networks: Issues and Challenges".

[3].Zoran S. Bojkovic, Bojan M. Bakmaz, and Miodrag R. Bakmaz "Security Issues in Wireless Sensor Networks", International Journal of Communications Issue 1, Volume 2, 2008.

[4]. Dr. Joshua Lackey, Andrew Roths, Jim Goddard, CISSP**, "** Wireless Intrusion Detection", IBM Global Services,April 2003.

[5]. Dazhi Chen and Pramod K. Varshney, " QoS Support in Wireless Sensor Networks: A Survey". [6]. Gurdas Singh, Janpreet Singh, Sukhjit Singh, Sehra Mohanjeet Singh, Inderjit Singh, "Secure Communication Schemes in Wireless Sensor Network".

[7]. C.C. Su, K.M. Chang, Y.H. Kue, and M.F. Horng, "The new intrusion prevention and detection approaches for clustering based sensor networks", in Proceedings of 2005 IEEE Wireless Communications and Networking Conference (WCNC'05), vol. 4, New Orleans, L.A., Mar. 2005, pp. 1927-1932.

[8]. S. Ganeriwal and M. Srivastava, "Reputation-based framework for high integrity sensor networks", in Proceedings

of the 2nd ACM Workshop on Security of Ad Hoc and Sensor Networks (SASN'04), Washington,DC, Oct. 2004, pp. 66-77

[9]. c.C. Su, K.M. Chang, Y.H. Kue, and M.F. Horng, "The new intrusion prevention and detection approaches for clustering-based sensor networks", in Proceedings of 2005 IEEE Wireless Communications and Networking Conference (WCNC'05), vol. 4, New Orleans, L.A., Mar. 2005, pp. 1927-1932.