International Research Journal of Advanced Engineering and Science
ISSN (Online): 2455-9024

Secure Efficient Clustering Routing from Different Attacks in WSN: A Survey

Ajay Kumar Mishra[1], Swatantra Tiwari[2]
[1, 2]Dept. of Electronics and Communication, Rewa Institute of Technology Rewa
Email address: {[1]ajay7872, [2]swatantratiwari84} @gmail.com

***Abstract*— *The Sensor nodes are usually scattered in a sensor field, which is an area where the sensor nodes are deployed. Since large number of sensor nodes is densely deployed, neighbour nodes may be very close to each other. Hence, multi-hop communication in sensor networks is efficiently expected. Security is an important feature for the deployment of Wireless Sensor Networks. In sensor network the attacker called flooding attack that disturb the whole activity of network and also consume link capacity and processing capability of each node in WSN. In this survey the previous protection scheme has showing the better performance that is providing by simulation results. The protection scheme has recovers the network performance in presence of attacker and provides attack free environment. The attacker information is identified by different scheme through applied security scheme and secure network from flooding attacker. The WSN overview, applications, routing techniques, types of attacks and security requirement are also mentioned in different sections. The base station is only collecting the information sending to BS. The BS is not much intelligent to take action against malicious information. The CH is identified the sink in network and after finding the sink the information of sink is send back to sender. The sink is almost exist is in next Cluster head area and sender utilizes energy by selecting the node having enough residual energy for communication. The attacker aim is to consume the resources at most of the time because of that the routing performance is affected.*

***Keywords*— *WSN Clustering, Attacker, Energy, Routing, Security*.

I. INTRODUCTION

A wireless sensor network consists of many small sensor nodes for sensing events in a particular area and sending that information to a sink node. The sensors are very small devices, with limited battery power, and often, with no source of recharge.. Sensor network lifetime depends on the number of active nodes and connectivity of the network, so energy must be used efficiently in order to maximize the network lifetime. The size of the network varies with the monitored environment [1]. For indoor environments, fewer nodes are required to form a network in a limited space whereas outdoor environments may require more nodes to cover a larger area. The no centralized authority is present in this network for supervision of proper communication, if without base station sensors are communicate with each other. In WSN mobile node can move during communicating and base stations are fixed as node goes out of the range of base station, which gets into the range of another base station [2]. The sensor networks are also considered as static and dynamic [3]. In static network Base Station (BS) collected the information from sensors. It comes under the category of infrastructure based network in dynamic also possible BS collect information and also possible to nodes are communicate with other without any presence of BS and supervision system. But wireless link has very high error proneness and fewer infrastructures. That's why attackers or malicious nodes are easily degrades the network performance Most of the energy consumption, in WSNs, is spent on three main activities: sensing, data processing and communication. All these factors are important and should be considered when developing protocols for WSNs. The communication of the sensor nodes is the major component of the energy consumption. The potential task of the proposed approach is not only to find the reliable path from a source to a destination, but also to provide the most efficient way to extend the network's lifetime.

In recent years the Mobile communications and wireless networking technology has seen a prosperous development and popularity in research area. Driven by technological advancements also as application demands varied categories of communication networks have emerged like Cellular networks, impromptu Networks, sensing element Networks and Mesh Networks. Cellular Networks are the infrastructure based or dependent networks. Ad hoc networks are the temporary network are defined because the class of wireless networks that utilize multi hop radio relaying since the nodes are dynamically and at random situated. Impromptu networks are infrastructure independent networks. Thus what's a Wireless sensor Network (WSN)? We've completely different view points for this question. According to Akylidiz WSN consists of huge number of nodes that are deployed in such the way that they'll sense the phenomena [1]. Akkaya and outline WSN as a network that consists of little nodes with sensing, computation and communication capabilities [4]. we tend to shall generalize the on top of read points and outline WSN as a special category of Wireless Network and that are also presents a wireless communication i.e. infrastructure or infrastructure less (Ad hoc network)that enables North American country to instrument, observe and answer phenomena within the natural setting and in our physical and cyber infrastructure.

A Wireless sensing element Network (WSN) contains hundreds or thousands of those sensor nodes. These sensors have the flexibility to communicate either among one {another} or on to an external base-station (BS). A larger range of sensors allows for sensing over larger geographical regions with larger accuracy. The schematic diagram of sensing element or sensor node elements is shown Figure 1. Basically, every sensor node has a capability of sensing the neighbor, processing, transmission, mobilizer, position finding system (that find current location), and functional units or

Ajay Kumar Mishra and Swatantra Tiwari, "Secure efficient clustering routing from different attacks in WSN: A survey," *International Research Journal of Advanced Engineering and Science*, Volume 3, Issue 3, pp. 171-177, 2018.

power units (some of those elements are not obligatory just like the mobilizer).

A sensing element could be a device that senses the data and passes constant on to a next neighbour or base station. Sensors are capable of playacting some process, gathering sensory data and act with different connected nodes within the network. Sensors are} wont to measure the changes to physical surroundings like pressure, humidity, sound, vibration. The figure 2 shows the communication example of WSN. Sensing nodes are sometimes scattered in an exceedingly sensor field, that is an area or section wherever the sensing element nodes are deployed.

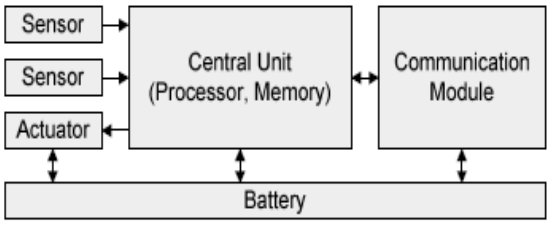

Fig. 1. Structure of sensor node.

Sensor nodes coordinate among themselves to provide high-quality data concerning the physical setting. Every sensor node bases its selections on its mission, the data it presently has, and its information of its computing, communication, and energy resources. every of those scattered sensing element nodes has the capability to gather and route data either to different neighbor sensors or back to an data collector external base station(s). The nodes in range are the neighbor nodes and each node is also moves in network with random mobility speed in meters second. Due to movement of sensor nodes the string connection establishment is also the major concern for successful data delivery [5]. The attackers or malicious nodes are easily disturbing the original routing performance [6]. The attacker node is always the intermediate node/s and this node/s are not instantly attack in network but these anodes are first analyze the routing information and exactly behaves like the normal node. If the sender is started the data sending at that instant attacker is activated and drop or corrupt all valuable information [7]. Some of the malicious nodes are also flooding unwanted information in huge amount. The attacker are also categorized in different categories and these categories are mentioned the attacker type in network. The attacker aim is only to drop the packets, consume network bandwidth or link capacity between the mobile sensor nodes and communicate with fake identity in network. In this survey the different attacks classification in WSN and types of routing protocols is detail discussed with different routing strategy in WSN.

II. Applications of Wireless Sensor Networks

The sensor nodes are gaining information from various areas like in medical, agricultural etc. The information of these sensors are accurate and also possible to used on critical areas [8]. The applications of WSN are as follows:-

1) Military or Border Surveillance Applications

WSNs are becoming an integral part of military command, control, communication and intelligence systems. Sensors can be deployed in a battle field to monitor the presence of forces and vehicles, and track their movements, enabling close surveillance of opposing forces.

2) Environmental Applications

Environmental applications Include tracking the movements and patterns of insects, birds or small animals.

3) Health Care Applications

Wireless sensor networks can be used to monitor and track elders and patients for health care purposes, which can significantly relieve the severe shortage of health care personnel and reduce the health care expenditures in the current health care systems. For example sensors can be deployed in a patient's home to monitor the behaviors of the patient. It can alert doctors when the patient falls and requires immediate medical attention.

4) Environmental Conditions Monitoring

WSN applications in this area include monitoring the environmental conditions affecting crops or livestock, monitoring temperature, humidity and lighting in office buildings, and so on. These monitoring modules could even be combined with actuator modules which can control, for example, the amount of fertilizer in the soil, or the amount of cooling or heating in a building, based on distributed sensor measurements.

5) Home Intelligence

Wireless sensor networks can be used to provide more convenient and intelligent living environments for human beings. For example, wireless sensors can be used to remotely read utility meters in a home like water, gas, electricity and then send the readings to a remote centre through wireless communication.

6) Industrial Process Control

In industry, WSNs can be used to monitor manufacturing process or the condition of manufacturing equipment. For example, chemical plants or oil refiners can use sensors to monitor the condition of their miles of pipelines. These sensors are used to alert in case of any failures occurred.

7) Agriculture

Using wireless sensor networks within the agricultural industry is increasingly common; using a wireless network frees the farmer from the maintenance of wiring in a difficult environment. Gravity feed water systems can be monitored using pressure transmitters to monitor water tank levels, pumps can be controlled using wireless I/O devices and water use can be measured and wirelessly transmitted back to a central control centre for billing. Irrigation automation enables more efficient water use and reduces waste.

8) Structural Monitoring

Wireless sensors can be used to monitor the movement within buildings and infrastructure such as bridges, flyovers, embankments, tunnels etc. enabling Engineering practices to monitor assets remotely without the need for costly sit e

Ajay Kumar Mishra and Swatantra Tiwari, "Secure efficient clustering routing from different attacks in WSN: A survey," *International Research Journal of Advanced Engineering and Science*, Volume 3, Issue 3, pp. 171-177, 2018.

visits, as well as having the advantage of daily data, whereas traditionally this data was collected weekly or monthly, using physical site visits, involving either road or rail closure in some cases. It is also far more accurate than any visual Inspection that would be carried out.

III. WSN Routing Protocol

A Network consists of several nodes. Data packets on transit normally pass through several nodes before eventually reaching the destination. Routing is the act of determining the path to be followed by a packet in order to reach its desired destination[9]. To do this, a number of factors have to be taken into account. Routing protocols takes charge of this process. The objective of routing protocol is to render the network useful and efficient. In general, routing in WSNs can be divided into three groups depending on the network structure: flat-based routing, hierarchical-based routing, and location-based routing depending. In flat-based routing, all nodes are typically assigned equal roles or functionality. In hierarchical-based routing, however, nodes will play different roles in the network. In location-based routing, sensor nodes' positions are exploited to route data in the network. A routing protocol is considered adaptive if certain system parameters can be controlled in order to adapt to the current network conditions and available energy levels. Furthermore, these same protocols can be classified [9] into multipath-based, query-based, negotiation-based, QoS-based, or coherent-based routing techniques depending on the protocol operation.

Design Issues of Routing Protocols

Initially WSNs was mainly motivated by military applications. Later on the resident application domain of wireless sensor networks have been considered, such as environmental and species monitoring, production and healthcare, smart home etc. These WSNs may consist of heterogeneous and mobile sensor nodes, the network topology may be as simple as a star topology; the scale and concentration of a network varies depending on the application. To meet this general trend towards diversification, the following vital design issues [10] of the sensor network have to be measured.

1) Fault Tolerance

Some sensor nodes may be unsuccessful or be blocked due to lack of power, have physical damage or environmental intrusion. The failure of sensor nodes should not affect the overall task of the sensor network. This is the consistency or fault compassion matter. Fault tolerance is the ability to maintain sensor network functionalities without any break due to sensor node failures.

2) Scalability

The number of sensor nodes deployed in the sensing area may be in the order of hundreds, thousands or more and routing plans must be scalable enough to take action to events.

3) Production Costs

Since the sensor networks consist of a large number of sensor nodes, the cost of a single node is very important to give reason for the overall cost of the networks and hence the cost of each sensor node has to be reserved low.

4) Operating Environment

We can set up sensor network in the interior of large machines, at the bottom of an ocean, in a geographically or chemically impure field, in a battle field beyond the enemy lines, in a home or a large building, in a large warehouse, connected to animals, connected to fast moving vehicles, in forest area for environment monitoring etc.

5) Power Consumption

Since the communication power of a wireless radio is relative to distance squared or even higher order in the company of obstruction, multi-hop routing will use less energy than direct communication. However, multi-hop routing set up momentous overhead for topology management and medium access control. Direct routing would execute well enough if all the nodes were very close to the drop [11]. Sensor nodes are prepared with restricted power source (<0.5 Ah 1.2V).Node life span is strongly reliant on its battery lifetime.

6) Data Delivery Models

Data delivery models decide when the data collected by the node has to be delivered. Depending on the function of the sensor network, the data delivery model to the drop can be Continuous, Event driven, Query-driven and Hybrid. In the nonstop delivery model, each sensor sends data occasionally. In event-driven models, the transmission of data is triggered when an event occurs. In query driven models, the transmission of data is triggered when question is generated by the drop. Some networks apply a hybrid model using a combination of nonstop, event-driven and query driven data delivery.

7) Data Aggregation/Fusion

Since sensor nodes might produce important redundant data, similar packets from multiple nodes can be aggregated so that the number of transmissions would be reduced. Data aggregation is the arrangement of data from different sources by using functions such as suppression (eliminating duplicates), min, max and average. As calculation would be less energy consuming than communication, considerable energy savings can be obtained through data aggregation. This method has been used to attain energy efficiency and traffic optimization in a number of routing protocol.

IV. Types of Attack in WSN

An Attackers or Malicious nodes are performing different types of malicious activities that have damage basic aspects of security like integrity, confidentiality, and privacy [8]. Here there are different types of attacks [9] and their mentioned in detail.The [12, 13] are classifies the routing attacks into the following categories;

Spoofed, Altered, or Replayed Routing Information

While sending the data, the information in transition may be spoofed, altered, replayed, or destroyed. Due to the short range transmission of the sensor nodes, an attacker with high

Ajay Kumar Mishra and Swatantra Tiwari, "Secure efficient clustering routing from different attacks in WSN: A survey," *International Research Journal of Advanced Engineering and Science*, Volume 3, Issue 3, pp. 171-177, 2018.

processing power and larger communication range could attack several sensors simultaneously and modify the transmitted information.

Selective Forwarding

In this kind of attack a malicious node may decline to forward every message it gets, acting

as black hole or it can forward some messages to the wrong receiver and simply drop others.

Sinkhole Attacks

In the Sinkhole attack, the goal of the attacker is to attract all the traffic. Especially, in the case of a flooding based protocol the compromised node may listen to requests for routes, and then reply to the requesting node with messages containing a bogus route with the shortest path to the requested destination.

Sybil Attacks

In Sybil attack the malicious node presents itself as multiple nodes. The attack of this type tries to degrade the usage and the efficiency of the distributed algorithms that are used. Sybil attack can be performed against distributed storage, routing, data aggregation, voting, fair resource allocation, and misbehavior detection .

Wormholes

Wormhole attack is an attack in which the malicious node tunnels messages from one part of the network over a link, that doesn't exist normally, to another part of the network. The simplest form of the wormhole attack is to convince two nodes that they are neighbors. This attack would likely be used in combination with selective forwarding or eavesdropping.

1) HELLO Flood Attacks

This attack is based on the use by many protocols of broadcasting Hello messages to announce themselves in the network. So an attacker with higher range of transmission may send many Hello messages to a large number of nodes in a big area of the network. These nodes are then convinced that the attacker is their neighbor. Consequently the network is left in a state of confusion.

2) Sleep deprivation attack

A particularly devastating attack is the sleep deprivation attack, where a malicious node forces legitimate nodes to waste their energy by resisting the sensor nodes from going into low power sleep mode. The goal of this attack is to maximize the power consumption of the target node, thereby decreasing its battery life. So, it is also known as battery exhaustion attack.

Flooding Attack

In sensor networks and networks in general is defined as any event that eliminates the network's capacity to perform its desired function. Flooding attack tries to exhaust the resources available to the victim node, by transmitting additional unwanted packets and thus prevent legitimate sensor network users from tapping work or resources to which these nodes are deployed. Flooding attack is means that not only for the adversary's attempt to subvert, disrupt, or destroy a sensor network, but also for any event that diminishes a sensor network's capability to provide a service. In network any node as normal node or week node in the radio range on attacker node agree with communication through attacker node by reply the request oof attacker, so that probing packet receive by the attack node and infect through infection, after infection this infected node launch the flooding attack.

V. SECURITY REQUIREMENTS

Sensor network have to fulfil some requirements for providing a secure communication. General security requirements of WSN are availability, confidentiality, integrity and authentication. Some other requirements known as secondary requirements are source localization, self organization and data freshness. These requirements gives protection against attacks to the information transmitted over the sensor network [13].

Data Confidentiality

In sensor network, data flows from many intermediate nodes and chance of data leak is more. To provide the data confidentiality, an encrypted data is used so that only recipient decrypts the data to its original form.

Data Integrity

Data received by the receiver should not be altered or modified is Data Integrity. Original data is changed by intruder or due to harsh environment. The intruder may change the data according to its need and sends this new data to the receiver.

Data Authentication

It is the procedure of confirmation that the communicating between nodes is the one that it claims to be. It is important for receiver node to do verification that the data is received from an authenticate node.

Data Availability

Data Availability means that the services are available all the time even in case of some attacks such as flooding attack.

Source Localization

For data transmission some applications use location information of the sink node. It is important to give security to the location information. Non-secured data can be controlled by the malicious node by sending false signal strengths or replaying signals.

Self-Organization

In WSN no fixed infrastructure exists, hence, every node is independent having properties of adaptation to the different situations and maintains self organizing and self healing properties. This is a great challenge for security in WSN.

Data Freshness

Data freshness means that each message transmitted over the channel is new and fresh. It guarantees that the old messages cannot be replayed by any node. This can be solved

Ajay Kumar Mishra and Swatantra Tiwari, "Secure efficient clustering routing from different attacks in WSN: A survey," *International Research Journal of Advanced Engineering and Science*, Volume 3, Issue 3, pp. 171-177, 2018.

by adding some time related counter to check the freshness of the data.

VI. Overview of Clustering

In clustering method of communication network nodes are organized in similar groups called clusters in which a node with higher residual energy, for example, assumes the role of a cluster head [4, 14]. The cluster head is responsible for coordinating activities within the cluster and forwarding information between clusters. Clustering has the potential to reduce energy consumption and extend the lifetime of the network. They have high delivery ratio and scalability and can balance the energy consumption. The nodes around the base station or cluster head will deplete their energy sources faster than the other nodes. Network dis-connectivity is a problem where certain sections of the network can become unreachable. If there is only one node connecting a part of the network to the rest and fails, then this section would cut off from the rest of the network. Clustering may be extended to more than just two levels having the same concepts of communication in every level. The use of routing hierarchy has a lot of advantages. It reduces the size of routing tables providing better scalability. Low-Energy Adaptive Clustering Hierarchy (LEACH) [10] is one of the most popular cluster-based routing protocols in wireless sensor networks. The operation of LEACH is broken up into rounds, where each round begins with a set-up phase, when the clusters are organized, followed by a steady-state phase, when data transfers to the base station occur. In order to minimize overhead, the steady-state phase is long compared to the set-up phase. To reduce management consumption, the steady-state phase is much longer compared to the set-up phase. The head of the cluster collects or mingle the data that's been composed by the sensor nodes and this facilitates in to sure high quantity of traffic generated within the network. With this, a large-scalable network with no traffic surplus is organized and by this additionally improved energy efficient constellation is attained as compared to the flat-topology. Single-hop routing is probable from device node to go of cluster, and by this implies able to able to accumulate the energy of the network. Property of distribute within the cluster, where it assigns the role of CH to the opposite cluster within the cluster

VII. Literature Survey

The attacker existence in network is degrades the performance of network. The previous scheme is mentioned in this section work is provides secure communication, some of them are as follows:-

In this system [15], they additionally added attack detection when any attack is done over cluster members or cluster head. This system is also able to prevent the false information sending over network aggregation node. If any attack is detected over cluster head we aggregate all information of the cluster members of information of data collection node. This novel developed system is probably gives reliable information delivery as well as secure information sending methodologies. Also they achieved solution for the problem of the data loss and enhanced the performance of network.

Energy Efficient Clustering Algorithm for data aggregation in WSN [16] is one of the examples of clustering algorithm. It includes two phases of clustering. One is the formation of cluster heads. In this phase every node broadcast their radius, residual energy and co-ordinates to the neighbour nodes. Then the nodes will calculate competition bids to select the cluster head. The other phase is data aggregation and tree construction, which includes calculation of weight values for cluster heads depending on the distance from the base station and remaining residual energy. These weight values help to select the leader node among the cluster heads. The aggregated data will be sent to base station only by leader node which leads to uniform energy dissipation and long network longevity.

Energy Efficient Clustering under the joint Routing and coverage constraint [17] addresses optimal planning of the different states of sensors, providing energy efficient scheduling of the states, energy efficient routing, clustering and data aggregation. The algorithm formulates the problem as an ILP model and implementation of TABU search algorithm to manage exponentially increasing computation times. It mentions four different states of sensor node such as Transmit, Receive, Idle and Sleep. A subset of the total number of nodes will remain active at a time to save energy and reduce redundancy. The cluster heads are chosen dynamically on the basis of residual energy and distance from the neighbours and a spanning tree connects all cluster heads which are only capable of routing and thus send data to the sink. It is stated that all nodes have same sensing range and transmission range and the cluster heads are dynamically selected from the nodes.

Another algorithm Energy Efficient Heterogeneous Clustered scheme for Wireless Sensor Network [18] has assumed that a percentage of sensor nodes are equipped with more energy and are immobile with known geographical locations. The introduction of computational heterogeneity includes more powerful microprocessor, more energy, complex data processing ability, which adds a lot of advantages to this model. The Link heterogeneity is introduced with the inclusion of high bandwidth and long distance network transceiver to prolong the lifetime of the network together with reliable data transmission. The Energy heterogeneity brought about the energy efficiency to the network, however increasing the implementation cost.

QOS supporting and optimal energy allocation for a cluster based Wireless Sensor Network [19] states that together with energy efficiency, The Quality of Service, which includes source to link delay, data pass rate, data loss rate etc. must also be taken under consideration. The algorithm states that each cluster is controlled by a cluster head having a finite capacity called SINGLE FIXED RATE. The relaying of traffic from cluster to cluster till the sink to minimize the data congestion and increase network lifetime, makes the cluster heads depend on total relaying data rate from its own cluster as well as other clusters.

Anand Balachandran, Geoffrey M. Voelker, Paramvir Bahl [20] “Wireless Hotspots Current Challenges and Future

Ajay Kumar Mishra and Swatantra Tiwari, “Secure efficient clustering routing from different attacks in WSN: A survey,” *International Research Journal of Advanced Engineering and Science*, Volume 3, Issue 3, pp. 171-177, 2018.

Directions" In this title, they observe that while the mobile computing landscape has changed both in terms of number and type of hotspot venues, there are several technological and deployment challenges remaining before hotspots can become an ubiquitous infrastructure. These challenges include authentication, security, coverage, management, location services, billing, and interoperability. They discuss existing research, the work of standards bodies, and the experience of commercial hotspot providers in these areas, and then describe compelling open research questions that remain.

Basavarajeshwari, M. Jitendranath, I Manimozhi [21] "Mitigating Hotspot Locating Attack in Wireless Sensor Network" In this title they develop a realistic adversary model which can monitor multiple parts of the network and can analyze the traffic in those areas. Next they propose a cloud based privacy preserving scheme by creating fake traffic of irregular shape which provides an efficient mechanism to protect the source node's location in addition to that they also generate the fake event at a particular time interval so that adversary cannot correlate the expected hotspot regions like pond or river with the inconsistencies in the network. Next we are introducing the concept of context aware location privacy where the sensor nodes are having the ability to perceive the presence of adversary in their vicinity in order to transmit data packets in more energy-efficient manner. Simulation and analytical results demonstrate that our scheme can provide stronger privacy protection.

S.A. Sai Sowmeyaa, S. Senthil Kumar [22] "Source Location Privacy Preservation in Wireless Sensor Network Using Computer Based Image Recognition" In this title, an algorithm called computer based image recognition is introduced to overcome such problem. Here the traffic is analysed using this method. They proposed scheme, the adversary model is considered where it is assumed that the adversary can monitor the small area or the entire network. Then they are introducing the hotspot Locating attack, considering that through the network traffic the adversaries identify the object's location. Finally for the effective source location privacy, the irregular shapes of fake packets are sent in the form of clouds. Insertion of cloud provides more privacy and it is made active only at the need of transmission.

VIII. Conclusion and Future Work

The attacker in network is not only degrades the routing performance but also the attacker is affected the performance of other layers in network. The cluster based routing is not only is reduces the cost of flooding and also effective in case of group communication in WSN. In WSN the possibility of physical security of sensor nodes is not granted as they are typically deployed in isolated and unreceptive environments. In order to optimize the conventional security algorithms for WSN, it is necessary to be aware about the constraints of sensor nodes. In this research the flooding Attack or malicious node identified by profile based security scheme. The survey of different security scheme proposed by different authors was definitely securing the network from heavy flooding of packets. The protection scheme secures the network from hunter and also blocks their communication activity in network. The sender and receiver are identified to each other through their source address and destination address. The applications of WSN having broad range, that makes work easy in different sectors of real life. The routing protocols The If the attacker is flooded large number of packets in network whenever it not the destination of given source then attacker it identified and protection scheme is provides the attack free environment in presence of attacker with recovers the performance of network and also other attackers behaviour are observe in survey. The attacker identification is necessary for better performance and effective security scheme is also reduces the unwanted overhead of communication.

References.

[1] I. Akyildiz, W. Su, Y. Sankarasubramaniam, and E. Cayirci, "Wireless sensor network : A Survey," Broadband and Wireless Networking Laboratory, School of Electrical and Computer Engineering, Georgia Institute of Technology, Atlanta, GA 30332, USA, Computer Networks 38, Elsevier, pp. 393–422, 2002.

[2] S. E. Roslin, C. Gomathy, and P. Bhuvaneshwari, "A Survey on Neighborhood Dependant Topology Control in Wireless Sensor Networks," *International Journal of Computer Science & Communication*, vol. 1, no. 1, pp. 185–188, 2010.

[3] Liping Liu, Feng Xia, Zhi Wang, Jiming Chen, Youxian Sun, "Deployment issues in wireless sensor networks", Mobile Ad-hoc and Sensor Networks, Volume 3794 of the series Lecture Notes in Computer Science pp 239-248, Springer 2005.

[4] M.Vieira, C. N. Coelho; D. C. da Silva; J. M. da Mata, "Survey on Wireless Sensor Network Devices," *In proceedings of Emerging Technologies and Factory Automation, 2003 IEEE Conference*, Volume: 1, 16-19, pp: 537-544, September 2003.

[5] Neelir Prasad and Mahbubul Alam, "Security framework for wireless sensor networks," *Wireless Personal Communications*, vol. 37, pp. 455–469, 2006.

[6] S. Batra, P. Goyal, and A. Singh, "A literature review of security attack in mobile ad-hoc networks," *International Journal of Computer Applications*, 11-15, 2010.

[7] Adrian Perrig, john Stankovic, David Wanger, "Security in wireless sensor networks," *Communications of the ACM*, pp. 53-57, 2004.

[8] S.Prasanna, Srinivasa Rao, "An over view of wireless sensor networks applications and security," *International Journal of Soft Computing and Engineering (IJSCE)* ISSN: 2231-2307, vol. 2, issue 2, May 2012.

[9] Al-Karaki, A. Kamal, "Routing techniques in wireless sensor networks: A survey," *Security and Networks*, vol. 11, issue 6, pp. 6-28, 2004.

[10] J. Pan, L. Cai, T. Hou, Y. Shi, and S. Shen, "Topology control for wireless sensor networks," *Proceedings of the Nineth ACM MobiCom*, 2003.

[11] J. Kulik, W. R. Heinzelman, and H. Balakrishnan, "Negotiation-Based protocols for disseminating information in wireless sensor networks," *Wireless Networks*, vol. 8, pp. 169–85, 2002.

[12] Shio Kumar Singh, M P Singh, and D K Singh"A survey on network security and attack defense mechanism for wireless sensor networks," *International Journal of Computer Trends and Technology (IJCTT)* pp. 1-9, May to June 2011.

[13] 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*, pp. 14-27, 2010.

[14] Xuxun Liu, "A survey on clustering routing protocols in wireless sensor networks," *Sensors*, pp. 11113-11153, 2012.

[15] Sneha Kamble, Tanuja Dhope, "Reliable routing data aggregation using efficient clustering in WSN," *International Conference on Advanced Communication Control and Computing Technologies (ICACCCT)*, pp. 246-240, 2016.

[16] Sha, C., Wang, R., Huang, H., Sun, L., "Energy efficient clustering algorithm for data aggregation in WSN," *Elsevier Journal, the Journal of China Universities of Posts and Telecommunications*, December 2010.

[17] Chamam, A., Pierre, S., "On planning of WSNs: Energy efficient clustering under the joint Routing and coverage constraint," *IEEE Transactions on Mobile Computing*, vol. 8, issue 8, August 2009.
[18] Kumar, D., Aseri, T.C., Patel, R.B., "Energy efficient heterogeneous clustered scheme for wireless sensor network," *Computer Communication*, vol. 32, issue 4, pp. 662–667, 2008.
[19] Tang, S., Li, W., "QoS supporting and optimal energy allocation for a cluster based wireless sensor network," *Computer Communication Journal*, vol. 29, issue 13-14, pp. 2569–2577, 2006.
[20] Anand Balachandran, Geoffrey M. Voelker, Paramvir Bahl, "Wireless hotspots current challenges and future directions," WMASH'03, September 19, ACM 2003, San Diego, California, USA.
[21] Basavarajeshwari, M. Jitendranath, I Manimozhi "Mitigating hotspot locating attack in wireless sensor network," *International Journal of Science and Research (IJSR)*, vol. 2, issue 6, June 2013.
[22] S.A. Sai Sowmeyaa, S. Senthil Kumar "Source location privacy preservation in wireless sensor network using computer based image recognition," *International Journal of Engineering Research and Development*, vol. 7, issue 4, pp. 75-79, May 2013.