ISSN: 2278 – 1323
*International Journal of Advanced Research in Computer Engineering & Technology (IJARCET)*
*Volume 2, Issue 2, February 2013*

# Selfishness of Discriminate Node in Caching Based Wireless Sensor Network

**Poonam Bisht**
**Lovely professional University, India**

**Arvind kumar**
**Lovely professional University, India**

*Abstract:***The size of wireless sensor node is small and the battery power of these sensor nodes is also limited. The wireless sensor nodes consume battery power in transmitting, processing the data. Generally, Wireless sensor nodes consume more energy in transmitting the data than processing of the data. The wireless Sensor nodes are deployed in the far places like forests, it is vary difficult to recharge or replace the battery of these sensor nodes. Main focus of this research is to reduce the energy consumption of the wireless sensor nodes during data transmission. With the use of caching the energy consumption is reduced and data can be collected faster and traffic on the network will also reduce. The Inter discriminate nodes is responsible for storing of the data in its cache, when sink generates an query message, sink will directly access data from Inter-discriminate nodes. The source nodes collect the data and pass it to the Inter-discriminate node through the discriminate node. One possibility is that if the discriminate node is selfish and responsible of dropping of the data packets, then Inter-discriminate node will not able to get the collected data.**

**Keywords: Discriminate Node, Inter-Discriminate Node, Selfishness, Dropping.**

## I. INTRODUCTION

Wireless Network can be defined as the decentralized and self configuring type of Network and used to monitor the environment conditions like temperature, pressure, fire etc. The wireless sensor nodes collect the environment data and pass the collected data to the sink (base station), sink broadcast the collected data. The simple sensor network is shown in the figure1:

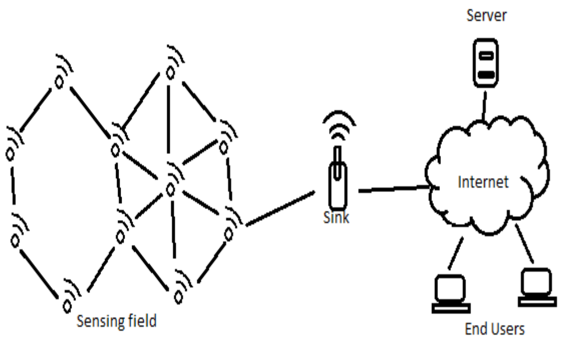

**Fig1**: Sensor Network

The size of the wireless sensor nodes is small and battery power of the sensor nodes is also limited. In the far places, like forests etc it is very difficult to recharge or replace the battery of sensor node. The maximum battery power of sensor node is consumed in the transmitting the collected data [9]. The base station or sink broadcast the query message to various sensor nodes and sensor nodes reply back with the collected data. The traffic in the sensor network depends on the query message generated by the sink per mean time. The sensor node having the result of the injected query will reply to the sink node through some routing protocol. The Inter-discriminate node is selected from the existing wireless sensor network and Inter-discriminate node is responsible for maintaining cache .When sink generates the query message, Inter-discriminate reply back with the collected data to the sink. The Inter-discriminate node collects the data from the source node through discriminate node and stores the data in cache. With the use of this approach, the traffic on the network is reduced and helps in saving response time and energy consumption [8]. The battery life of the sensor nodes can be extended if we manage to reduce the amount of communication, caching is the approach through which we can reduce the communication and extend the battery life of the sensor node. In the large network with thousands of sensor nodes, much number Inter-discriminate nodes excites. When the Inter-discriminate node and source node are not in the range of each other, nodes between the Inter-discriminate node and source node are responsible for data forwarding; these nodes are called discriminate nodes as shown in the figure 2:

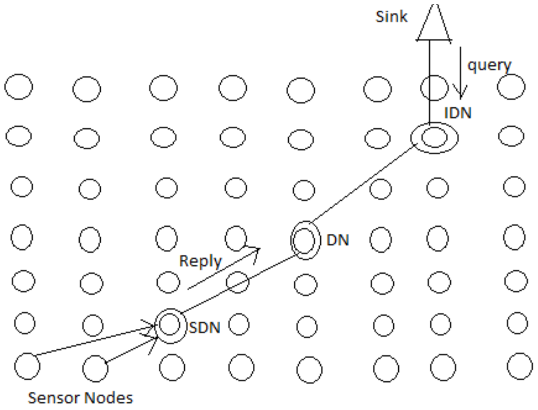

**Fig2**: Sensor Network with Inter-discriminate node and discriminate node

## II. PREVIOUS WORK

Z. Vincze et. all proposed a novel iterative algorithm for multiple sink deployment in WSNs in which sink are deployed on the basis of location information of neighboring nodes while the location of the distant nodes is being approximated. The stimulation results show that the proposed approach will solve the generated query in less time and in more efficient way [1].

Narottam Chand had proposed the cooperative caching which ensures sharing of data among various nodes reduces the number of communications over the wireless channels and thus enhances the overall lifetime of a wireless sensor network, cooperative caching scheme called ZCS (Zone Cooperation at Sensors) for wireless sensor networks [2].

Amir Shiri , Shahram Babaie had proposed a method for recovering lost packets by caching data in some of network nodes which is a combination of Extended NACK and Active Caching (AC) methods and called as New Active Caching (NAC) [3].

Long Cheng, Yimin Chen and Canfeng Chen and Jian Ma had proposed the Query-Based Data Collection Scheme . In order to minimize the energy consumption and packet delivery latency, QBDCS chooses the optimal time to send the Query packet and tailors the routing mechanism for partial sensor nodes forwarding packets [4].

Ms Manisha Rana , Senior Lecturer Gurpreet Kaur they proposes that sensor nodes in Wireless Sensor Network are battery powered devices which consumes energy during data transmission, processing, etc. The critical task in WSN is to deal with optimizing power consumption. One possible way to minimize power consumption is by the use of caching the data. Generally data transmission in WSN consumes more energy than processing so it is good to utilize the benefits of caching so that data access can be made faster [5].

Aishwarya Sagar Anand Ukey1, Meenu Chawla had proposed a new reputation based that detect the nodes which is responsible for packet dropping this approach is based on the threshold cryptography. In this approach we count the number of packets send and number of acknowledgments received. This new approach can be integrated on the top of any routing protocol [6].

N.Bhalaji and Dr.A.Shanmugam had proposed the new routing mechanism to isolate the packet dropping attack. Associations between nodes are used to identify and isolate the malicious nodes. Simulation results show the effectiveness of our scheme compared with conventional scheme[7] .

## III. CACHING IN WIRELESS NETWORK

The battery life of the sensor nodes can be extended if we manage to reduce the amount of communication, caching is the approach through which we can reduce the communication and extend the battery life of the sensor node. The traffic in the wireless sensor network depends on number of query generated by the sink and sensor nodes respond to the query message. The sink floods the query message in the sensor network when the query message reaches to the source nodes, source node respond to the query message. The caching is the approach through which we can reduce the traffic on the sensor network. The data is collected by various sensor nodes and collected data is cached in the Inter-discriminate nodes, inter-discriminate node is responsible for maintaining the cache .When the data sink generates the query message, sink will not floods the network with the query messages. It will directly send query message to the Inter-discriminate node. Inter-discriminate node responds back to the sink. The query and data flow in cache based sensor network is shown in the figure 3:

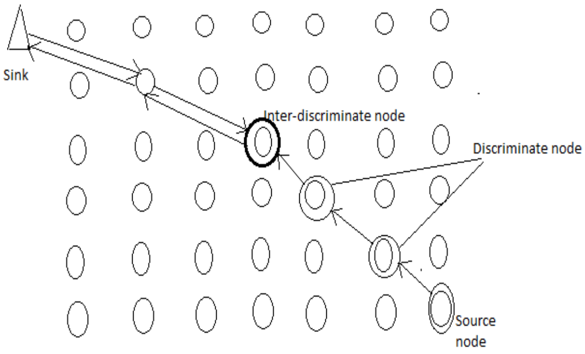

**Fig3**: Data Flow in cache based wireless sensor network

## IV. WIRELESS ATTACKS

Attacks are generally defined as the activities carried out by the hacker or by the malicious node to disrupt the normal behavior of the network. There are a variety of attacks possible in MANET. The attacks can be classified as active or passive attacks, internal or external attacks, or different attacks classified on the basis of different protocols. A passive attack does not disrupt the normal operation of the network. The attacker only snoops the data exchanged in the network without altering it. It includes Eavesdropping, jamming and traffic analysis and monitoring. In case of active attacks, the attacker attempts to alter or destroy the data being exchanged in the network. This attack disrupts the normal functioning of the network. Active attacks can be internal or external. External attacks are carried out by nodes that do not belong to the network. Internal attacks are from compromised nodes that are part of the network. Since the attacker is already part of the network, internal attacks are more severe and hard to detect than external attacks .The ultimate goals of the security solutions for MANETs is to provide security services, such as authentication, confidentiality, integrity, authentication, non-repudiation, and availability to mobile users. The various possible attacks are:-

Black hole attack:- According to this attack, an attacker uses the routing protocol to advertise itself as having the shortest path to the node whose packets it wants to intercept. When the attacker receives a request for a route to the destination node, it creates a reply message which advertises itself as a valid path to destination. The attacker consumes the intercepted packets without any forwarding.

Gray hole Attack:- The gray hole attack is also termed as misbehaving attack. In this attack, the attacker selectively drops the packet with certain probability. Also, in this attack the intruder node behaves maliciously for the time it selectively drops the packets and then switches to its normal behavior.

Wormhole attack:- In this attack, an attacker records the packets at one location in the network and tunnels them to another location. The routing can be disrupted when routing control messages are tunneled. This tunnel between two colluding attackers is referred as a wormhole.

Byzantine attack:- In this attack, a compromised intermediate node or a set of compromised intermediate nodes works in collusion and carries out attacks such as creating routing loops, forwarding packets on non-optimal paths and selectively dropping packets which results in disruption or degradation of the routing services.

Information Disclosure:- . An attacker may leak the confidential or important information to unauthorized nodes present in the network. The secret information may the information about network topology, geographic location of nodes or optimal routes to authorized nodes in the network.

Resource Consummation attack:- In this attack, an attacker attempts to consume or waste away resources of other nodes present in the network. The resources can be the battery power, bandwidth, and computational power, which are only limitedly available in ad hoc wireless networks. An attacker can consume the batteries by requesting routes and unnecessary packet forwarding to the nodes.

Impersonation: - In this attack, an attacker can pretend to be an authorized user and can access the secret information. The attacker may snoop information regarding the identity and authentication of the target node from the previous communication.

Routing Table Overflow:- : In the case of routing table overflow, the attacker creates routes to nodes which does not exist. The goal is to create enough routes to prevent new routes from being created.

Packet Dropping Attack:-When two nodes are not in the range of each other, they can communicate with each with the help of intermediate nodes. The intermediate nodes are responsible for data forwarding. Intermediate nodes must be trusted nodes, if intermediate nodes are not trusted one, confidentiality and integrity factors will be compromised. The un-trusted will also response for packet dropping means it will not forward data to the receiver node, it will may leads to the DOS attack. When intermediate node will not forward the data to the receiver node and responsible for packet dropping this attack is called Packet dropping attack. The node which is responsible for packet dropping is also called the selfish node, as it will not follow the MAC layer rules. Packet dropping attack is shown in the figure 4:

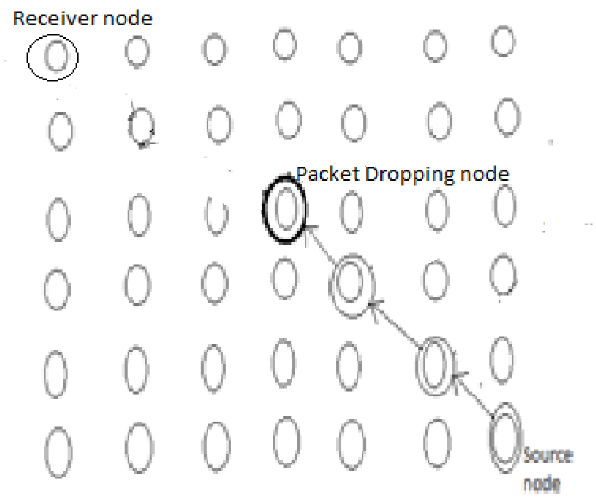

**Fig4**: Packet dropping attack

## V. COCLUSIONS AND FUTURE WORK

In this paper, we review the “IMPROVED CIRCULAR CACHING BASED ON WSN WITH MULTISINK” approach. According to our best knowledge with the use of this approach the battery life of the sensor network will be extended. As, with the use of approach the traffic on the network will reduced which leads to extend the battery life of the sensor node. But the packet dropping attack is possible in this approach. If the discriminate nodes are selfish and will not forward data to the inter-discriminate node then the inter-discriminate will not able to get the collected data, then the query generated by the sink will not complete and it leads to the DOS (denial of service attack) attack.

## REFERENCES

[1] Zolt´an Vincze, Rolland Vida, Attila Vid´acs “Deploying Multiple Sinks in Multi-hop Wireless Sensor Networks”

[2] Narottam Chand “Cooperative Data Caching in WSN”.

[3] Amir Shiri , Shahram Babaie , Javad Hasan-zadeh “New Active Caching Method to Guarantee Desired Communication Reliability in Wireless Sensor Networks” . Journal of Basic and Applied Scientific Research, 2012.

[4] Long Cheng, Yimin Chen and Canfeng Chen and Jian Ma “Query-Based Data
Collection in Wireless Sensor Networks with Mobile Sinks**”**

[5] Ms Manisha Rana , Senior Lecturer Gurpreet Kaur “IMPROVED CIRCULAR
CACHING BASED ON WSN WITH MULTISINK” 2012.

[6] Aishwarya Sagar Anand Ukey, Meenu Chawla “Detection of Packet Dropping Attack Using Improved Acknowledgement Based Scheme in MANET”

[7] N.Bhalaji, Dr.A.Shanmugam “Reliable Routing against Selective Packet Drop Attack in DSR based MANET”

[8] Xu Li *et.al*(2007),” Sink Mobility in Wireless Sensor Networks”

[9] Chee-Yee Chong *et.al*(2003),”Sensor Networks”has presented MEMS technology and low-cost manufacturing, more reliable communication, wireless have resulted in small, inexpensive, and powerful sensors with embedded processing and wireless networking capability.