ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 5, May 2015

Detection and Isolation of Black Hole Attack in Wireless Sensor Networks

Kalaiselvan. K[1], Gurpreet Singh[2]

P.G. Student, Department of Computer Engineering, Lovely Professional University, Punjab, India[1]

Assistant Professor, Department of Computer Engineering,Lovely Professional University, Punjab, India[2]

ABSTRACT*:*The Sensor nodes are connected wirelessly to form a network called as the wireless sensor network (WSN). The nodes have confined battery power and the battery of the nodes cannot be replaced. These sensor nodes are used for collecting the sensor data and transmits them to the sink or base station. This data transmission from a node to the other node utilizes more energy if the data is broadcasted the from sensor nodes directly to the sink. The clustering method is used to reduce the energy utilization of the sensor nodes and the nodes are grouped into the clusters and the cluster-head in each cluster will gathers the data and transmits it to the sink. In the black hole attack, the attacker node broadcasts good paths to the node falsely during the route-establishment process. When a request is received by the attacker to the destination node for a route, it creates a reply for the short route and enters into the passageway to do something with the packets passing between them. If the Black Hole Node is present in the network, it will reduce the network performance along with the depletion of the energy in the network. In this paper, the technique presented is for detection and isolation of black hole nodes from the sensor network. In this technique, the black hole node is identified by monitoring the fake reply packets that are transmitted by the nodes and it will be removed from the network.

KEYWORDS*:*WSN, Cluster, Black Hole Node, Malicious node.

I. INTRODUCTION

A wireless sensor network (WSN) is a collection of sensor nodes spread over a particular area where the changes should be monitored. A wireless sensor network consists of sensing elements, storage unit, processing unit and these nodes can interact with the other nodes. All sensor nodes transmit through a wireless transmission. The sensor nodes are randomly distributed in the area. If the sensor node is not able to transmit to the other node through an explicit link, i.e. they are out of their broadcasting range; the packet can be sent to that node by using the intermediate nodes. The concept of using the intermediate nodes to transmit the data is called as multi-hopping. There is no requirement to provide an infrastructure to set up the network as the wireless sensor networks are not the centralized systems. The wireless sensor networks have the end-to-end communication between the nodes.

Wireless sensor networks have self-healing and self-organizing capabilities. Self-healing allows the sensor nodes to reconfigure themselves and try to discover an alternate path for the nodes when the link fails or powered-down. The sensor node collects and forwards the data to the information sink using the multi-hop wireless network. A sensor network is self-organizing because it permits the network to join a new node without any transmission interference. Sensors are the powerful accessories which are capable of gathering the data from different devices, stores them, sensing and transmitting the information to the sink or the base station. The sensor networks have the ability to withstand environmental conditions and it has the ability to cope with the node failure. In wireless sensor networks, the sensor nodes are cooperative in nature and are organized in a cooperative manner. In sensor network, nodes are not required to be installed, as they are easily deployed anywhere in the network. The data gathered from different devices can be retrieved from either the sink or the base station.

The sensor nodes have fixed batter power perceives the remaining power. Base Station (BS) can be distant from the field of sensor nodes and it doesn't have a power constraint. Sensor node senses the environment at a steady time interval and it will transmit the information to the base station. The sensor nodes utilize either multi-hop

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 5, May 2015

communication or directly forward to transmit to the base station. The nodes can scrutinize the transmission power of the wireless transmitter.

1.1 **Routing Protocol:**In wireless sensor network, routing is different from the general routing in the fixed network. As WSN doesn't have a fixed infrastructure and the links are uncertain due to the failure of the sensor nodes and the routing protocols should have to reconcile the requirements of energy saving in the wireless sensor networks. The objective of the routing protocol is to generate routes between the sensor nodes to the cluster head and the cluster head to the base station or the sink node. There are seven categories of routing protocols proposed for wireless sensor networks. They are location based, mobility based, multi-path based, heterogeneity based, QoS based, data centric and the hierarchical protocols. Of all the above mentioned categories of protocols, the hierarchy based protocol is used in this paper as the routing protocol. LEACH (Low Energy Adaptive Clustering Hierarchy) is an energy efficient hierarchical based routing protocol which is used for both the selection of cluster heads and as the routing protocol for the sensor networks.There are two phases in LEACH; they are a setup phase to partition the sensor network into clusters and a steady-state phase for the data fusion and the communication to the sink node. It minimizes the consumption of energy by reducing the transmission cost among the sensor nodes and the cluster heads. The single-hop routing is used by the LEACH in which the sensor node directly communicates to the cluster-head and the sink node.

1.2 Attacks in MANET:

1.2.1 Wormhole Attack

Malicious nodes create a wormhole. It is a link of less delay from one part of a network to another portion of the network in which the malicious node forwards the packets to the other malicious node. It is a network layer attack. In this type of attack, message is captured from the one region of network and replaying in other region. The attacker gather all message and other retransmits to make destination unreachable from network.

1.2.2 Black hole Attack

Attacker node broadcasts good paths to the node falsely during the route-establishment process in the case of reactive routing protocols, or in the form of route update messages in proactive routing protocols. When a request is received by the attacker to the destination node for a route, it creates a reply for the short route and enters into the passageway to do something with the packets passing between them. This make destination system unreachable in network like the denial of service attack.

1.2.3 Sybil Attack

Attacker node has many identities in a network. This attack is effective on routing protocols, aggregation of the data, fair resource allocation and misbehavior detection. Sybil attack is mostly straightforward to perform in wireless sensor networks where the transmission carrier is broadcast and frequencies used by the node are same.

1.2.4 Sinkhole Attack

A malicious node forges the routing information of the incriminated node and makes that node more attractive to the adjacent nodes. The adjacent nodes choose the incriminated nodes as their next-hop to route the data. An attacker can fake optimal path by broadcasting high prime paths. The nodes in the network move their traffic onto the attacker node as it is better than the currently used node.

1.2.5 Cloning Attack

A rival node uses the identity of a compromised node and it secretly introduces the copies of the compromised node. These nodes can commence an attack that will be the downfall of the sensor network.

II. BACKGROUND AND RELATED WORK

Anbuchelian. S et al proposed an energy saving clustering algorithm for the efficient energy consumption and it also detects the threats on the cluster heads in the wireless sensor networks.The Grayhole attack is a type of black hole attack in which the malicious node selectively drops packets that it receives. Balancing the network loading between the clusters and the uniform cluster location and extends the lifespan of the wireless sensor network [1].The performance variables used in the paper are average end-to-end delay, throughput and packet delivery ratio. The packet delivery ratio is the number of receiving packets to the generated packets.

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 5, May 2015

Dr. G. Padmavathi et aldiscussed the wide variety of security attacks in wireless sensor networks and the security mechanisms to handle themselves from the attacks. Security goals are confidentiality, time synchronization, integrity, secure localization, authentication, availability. Wireless sensor networks are susceptible to security attacks due to their transmitting nature of the communication carrier [2]. Monitoring the transmission channel by attackers is known as passive attacks. Attackers fabricate the data in the transmission channel is called active attack. Security schemes are used to detect, prevent and recover from any attacks. The challenges in the sensor networks are also discussed in this paper. The challenges in the sensor networks are also discussed in this paper. This paper summarizes the security attacks and the security mechanism to handle those attacks in the wireless sensor networks.

Vipul Sharma et al proposed the mechanism for the detection of black hole attack in Leach based sensor networks. The clusters are created from the sensor nodes on the basis of signal strength.The leach protocol is initiated to elect the cluster head for each round. Each sensor node in the particular cluster has the probability to be selected as the cluster head using the leach protocol [3]. It is an energy efficient cluster based hierarchy routing protocol. Base station maintain the ids of the cluster head at each round and if the cluster head repeats represents the network is under black hole attack. Base station sends the alert packet to the sensor nodes.If the cluster head is not repeated there is no black hole node in the network and the data transmission across network successfully. The proposed model is detecting whether the cluster head is the black hole node or not and it will not detect the sensor nodes as a black hole node.

Kalpana Sharma et al discussed the security threats and challenges that are faced by the wireless sensor networks. Sensor networks have an additional weakness as the sensors are deployed in an uncongenial location. This paper is also discussed about the counterattacks and the possible preventive measures for the various attacks. Attacks on the wireless sensor networks are categorized based on attacks against security mechanisms and the routing mechanisms [9]. The defense mechanisms for the attacks are using spread spectrum to prevent jamming and the client puzzles for flooding attacks. The defense mechanism for the attacks provides only the guidelines about the security threats and the exact solution depends on the type of application that the sensor network is deployed for.

Ju young Kim et al presented a study of the different threats, attacks and vulnerabilities for Wireless Sensor Networks (WSNs). In node capture attack, an attacker gains complete gain over a node by physically accessing the node. Then the attacker can remove the cryptographic functions and get the access to the data stored on that captured node. The countermeasures for reducing the risk of eavesdropping on wireless transmissions are the use of encryption to preserve confidentiality and it should be more difficult to locate and intercept the wireless signals [8]. Hardware attestation, software authentication and validation are the countermeasures against the software attacks. The different classes of these threats are defined to identify a possible countermeasure scheme applicable for each threat classification.

TEODOR-GRIGORE LUPU presented the different types of attacks in wireless sensor networks. Attacks on the different layers are categorized. The security attacks and the threats can be categorized based on the mechanisms used in those attacks [16]. Traffic analysis is the process of analyzing the messages in order to identify the data from patterns in the connection. Data from an authentic person who is entering into a network can be fabricated by an attacker and it can be replayed the next day. Compromised nodes within a network can cause the internal attack and it is hard to identify those compromised nodes in the network. Thinking like an attacker is a better choice for creating the intrusion detection system.

Ms.Manisha Rana et al proposed an approach to minimize power consumption by caching the data. In the proposed approach, unicasting is used instead of broadcasting. With the use of unicasting, energy consumption is saved and the network life is improved [11]. To provide information nearer to a sink, the information from it should be cached nearby the sink. Sensors have confined storage content; the nodes use a cooperative caching mechanism by utilizing a cache of the nearby nodes. Diagonal routing is used to reduce the length between the source nodes to a sink and it will reduce energy consumption in a network.

III. PROPOSED DESIGN

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 5, May 2015

A wireless sensor network is a group of scattered sensors to supervise the physiological phenomenon. Each sensor node is capable of sense, process and communicates with the other sensor nodes. The sensor nodes organize themselves to form a multi-hop wireless network that gathers the data and relays it to the sink. The sensor networks have the ability to withstand environmental conditions and it has the ability to cope with the node failure. The sensor networks are often deployed in the hostile environment. The sensors have limited battery power and it is hard to restore or retrieve the battery of the sensors. To increase the lifetime of the sensor nodes and to reduce the battery utilization in the nodes, various techniques had been proposed. In all of the proposed methods, clustering is the high energy effective technique. The cluster-heads are chosen in this technique and the cluster-heads take part in the communication to sink node. Different clustering algorithms are used for the selection of cluster-heads. The sensor networks are insecure to attacks and the attacks upon network availability, integrity, secrecy and authentication are the classification of the attacks. The cryptographical mechanisms can be used to preclude the attacks on privacy and legitimacy of the contents. The security mechanisms used in these networks are key management protocols, secure data aggregation and the trust management. Black hole attack is the dropping of the packets and it depletes the battery power in the network. The attack is carried out by either the compromised nodes or malicious nodes, which are present in the network. The cluster heads which are elected collect the information from the sensor nodes in the cluster and the cluster head will forward the collected information to the sink node or the base station. If the cluster head is the malicious or the black hole node, then there is no data exchange between the cluster head and the sink node as the malicious cluster head node drops the information which is received from the sensor nodes. Hence, there will be a higher degradation in the network performance of the sensor network.

A significant amount of research has been devoted to study security issues as well as countermeasures to various attacks in wireless sensor networks. However, there is still much research work needed to be done in the area. This paper propose a mechanism for identifying and isolating all the malicious nodes present in the sensor network to provide enhanced security and stability in the wireless sensor networks.

The proposed model for the identification and isolation of blackhole node involves the following steps. The wireless sensors are deployed in the field randomly. The K mean clustering method is applied for creating the clusters in the sensor network. The clusters are formed so the sensor nodes within that cluster will forward the sensed data to the cluster head of the corresponding cluster not directly to the sink node. The cluster head for each cluster are selected on the LEACH (Low Energy Adaptive Cluster Hierarchy) protocol. This protocol allows the sensor nodes the possibility to be selected as the cluster head. The network performance of the sensor network is analysed for the presence of the black hole node. If the network performance is lower than the threshold, then the black hole node is present in the network. The sensor nodes broadcast the route request messages to transmit to the other node in the network. Within the cluster, the cluster head gathers the sensed data from the sensor nodes and it will transmit to the sink. The source sensor node will wait for the reply messages to the route request messages sent by the source sensor node. If the black hole is present in the sensor network, the black hole node will send the fake reply packet with the distance to the destination node value is less. The source sensor node will acknowledge the black hole node as the neighbor node and it will transmit the data to the black hole node. The black hole node simply discards or drops the packet. The sensor nodes will check for the fake reply packets and identify the black hole node and it will inform the other nodes in the network that particular node is the black hole node. Thus, the black hole node is isolated from the network and if the black hole node transmits the reply packets to other sensor nodes, the nodes simply discard the reply messages. The proposed methodology is implemented in a simulated environment and the results are compared with the existing technique.The parameters which are considered in the proposed methodology for the detection and isolation of the black hole node are packet delivery ratio and the throughput of the sensor network.

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 5, May 2015

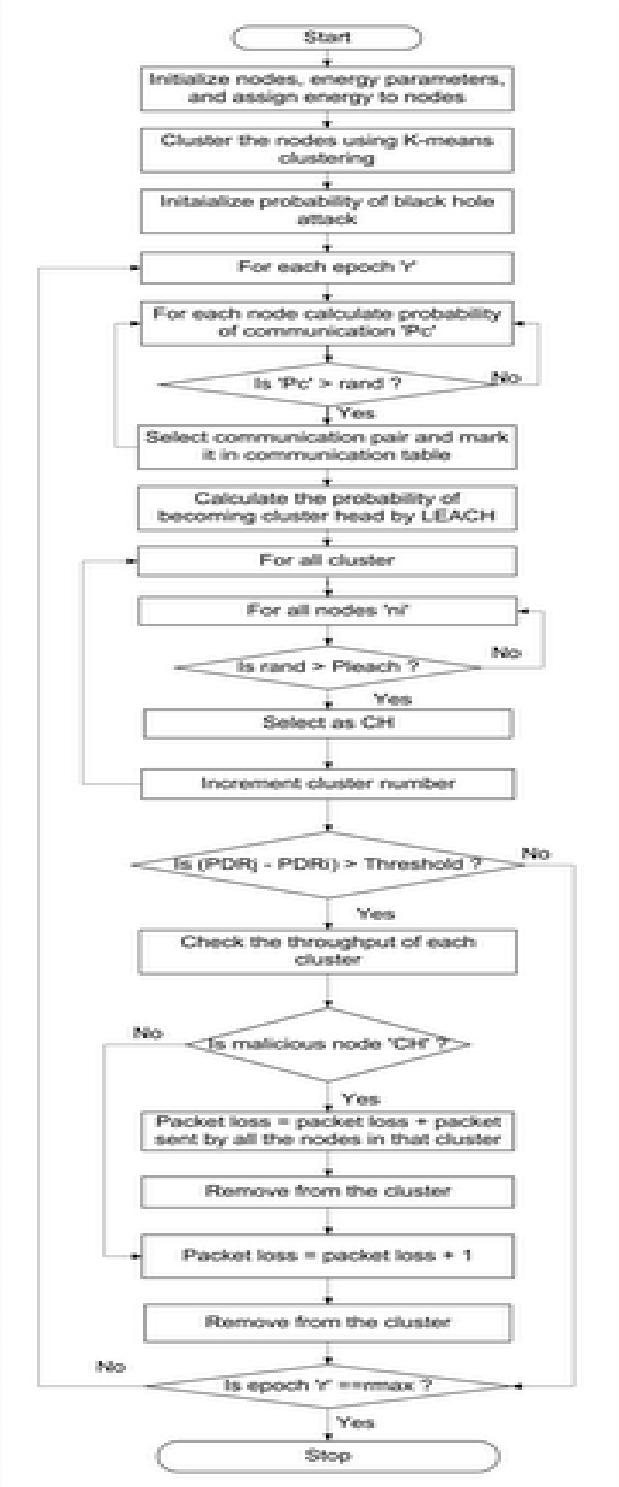

Figure 1Flowchart of our proposed algorithm

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 5, May 2015

IV. PERFORMANCE EVALUATION

1. Simulation Configuration:

The simulation for the proposed method has been carried out using the MATLAB (Matrix Laboratory). It is a high-level programming language developed by MathWorks.

In our simulation we are creating thesensor network consisting of 100nodes, the protocol used is LEACH, one malicious node in the sensor network and the graphs of the results are generated. The graphs are used to signify the variation in throughput and the packet delivery ratio using the proposed method. The blue line characterizes the change in case of the new scenario and the green colour represents the scenario without the detection mechanism for the black hole attack. These two parameters are a widely used for validating and confirming the use of particular methods. Throughput
can
be defined as the number of packet data received per unit time. Figure 4 shows the change in the packet delivery ratio after the deployment of the proposed method. It shows that the proposed method enhances the packet delivery ratio, while the packet is transmitted from the nodes to the base station or the sink node. In the previous schema, the packet delivery ratio is varying from high to low on the presence of malicious node in the sensor network whereas in absence of malicious node the packet delivery ratio is constant as the malicious activity isdetected and isolated from the network.

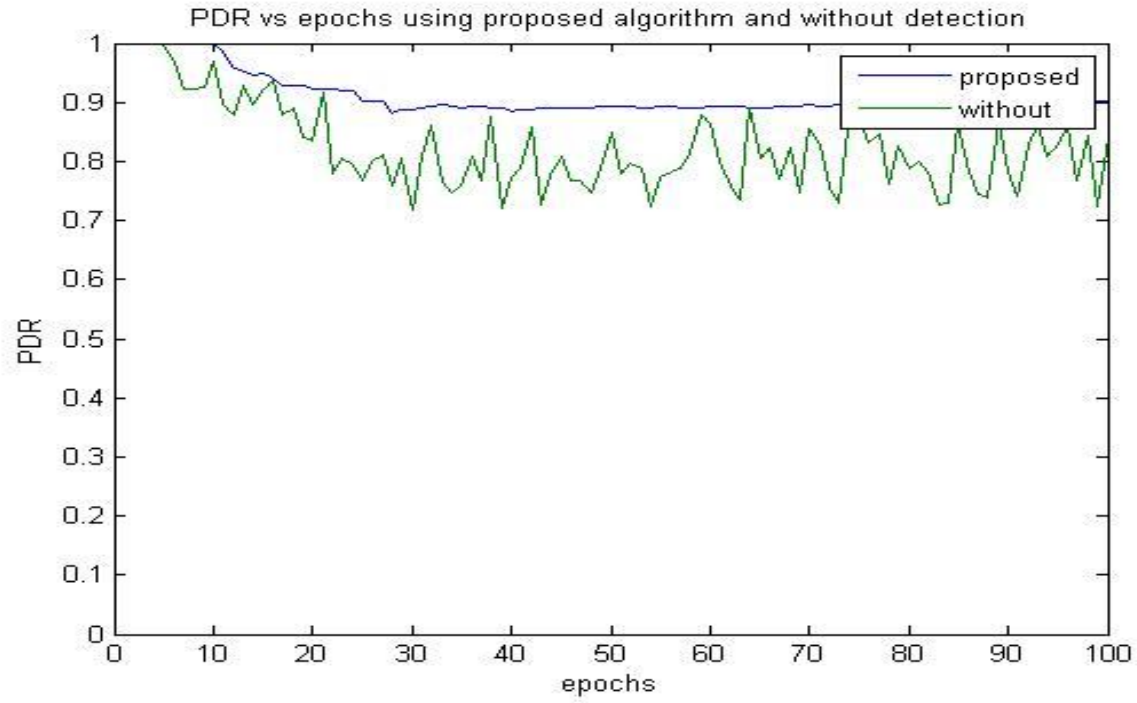

Figure 2 Packet Delivery Ratio

Figure 5 represents the network throughput after applying proposed method. As packet delivery ratio is constant in the sensor network because of isolation of malicious node, so throughput of the network is linearly increased after some pint of time. From the graph, we can see that when number of packet increase throughput is gradually increase with time in our proposed schema shown by the blue line. While green line represents schema where the detection mechanism is not implemented when the malicious node present in the network at that time packet continuous drop so the line is constant for some period of time.

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 5, May 2015

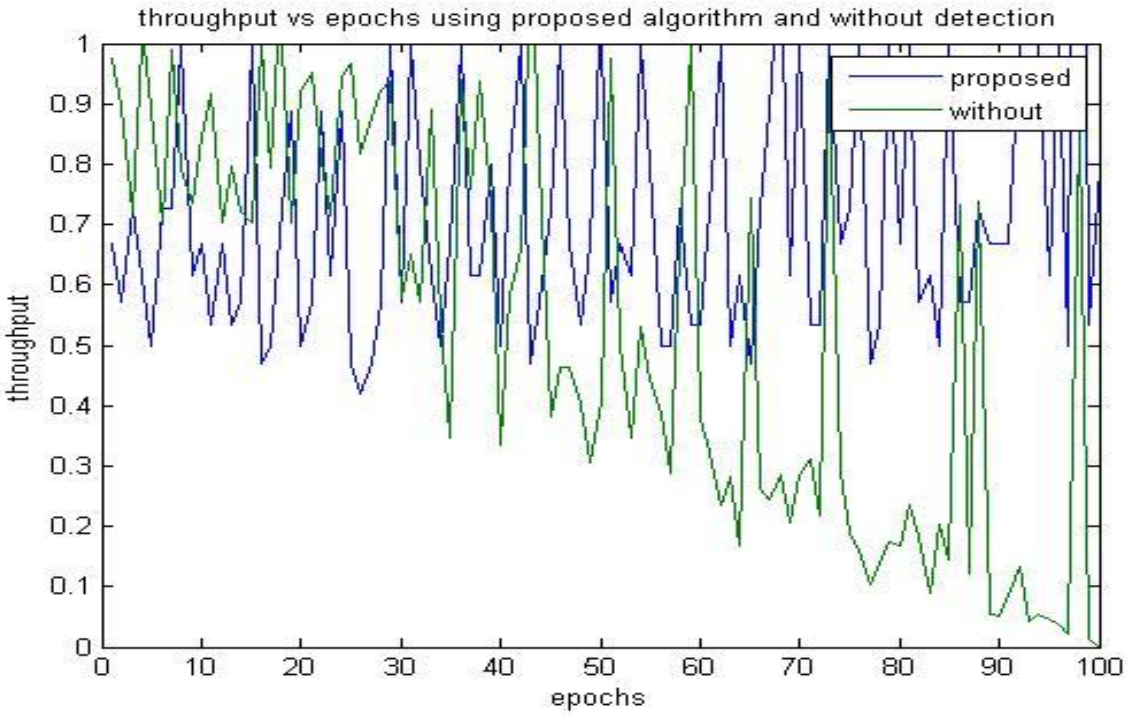

Figure 3 Throughput

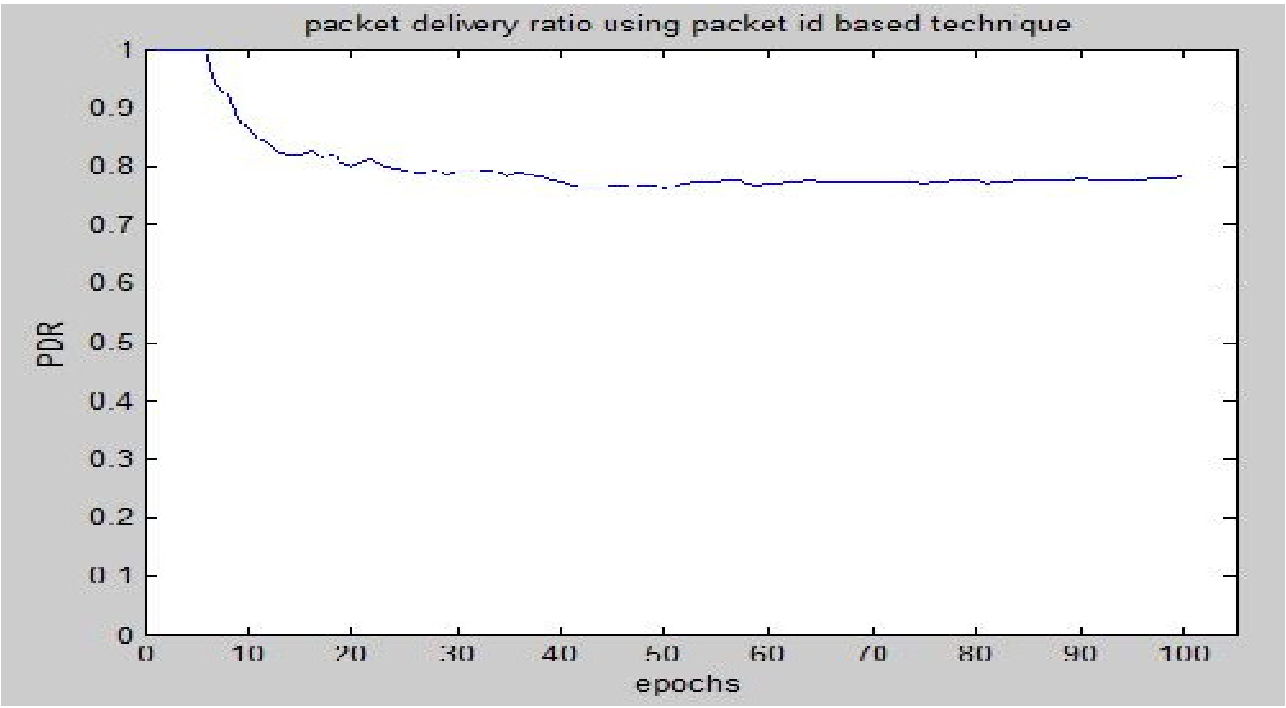

Figure 6 Packet delivery ratio using packet id based technique

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 5, May 2015

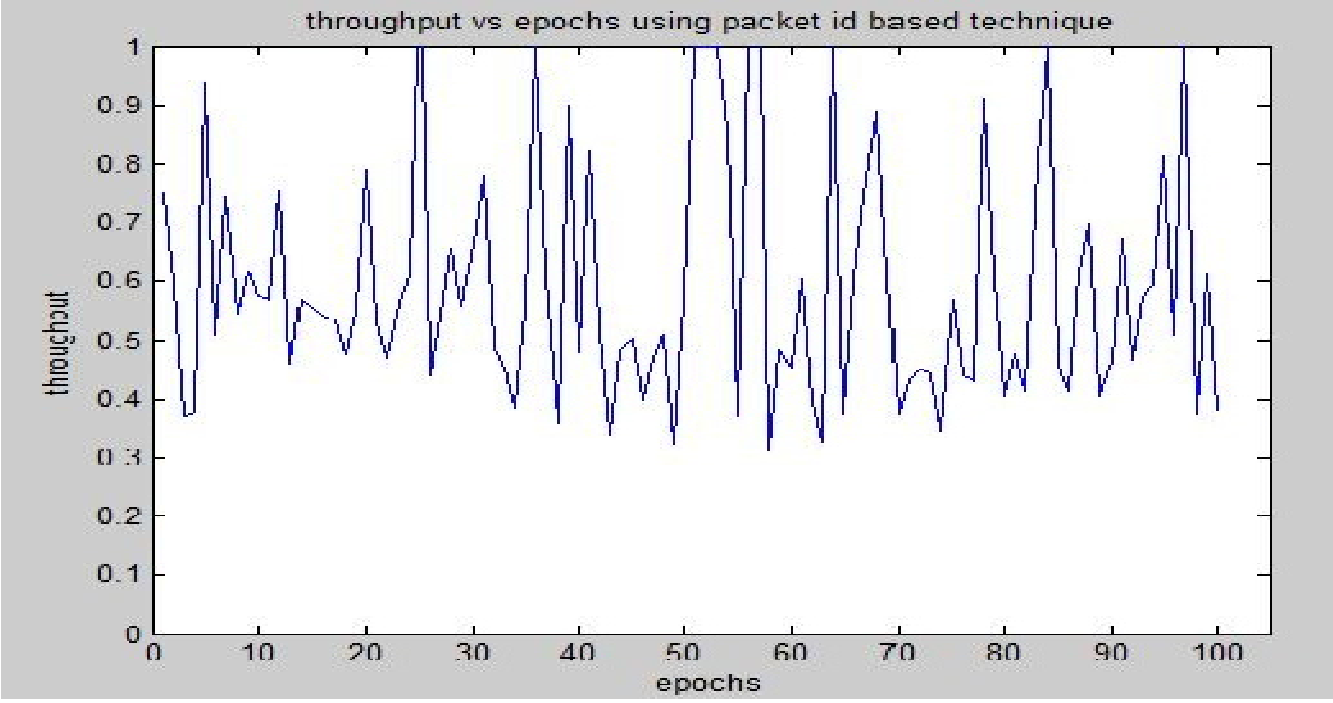

Figure 7 Throughput of packet id based technique

The Figure 6 represents the packet delivery ratio of the sensor network which contains of the 100 sensor nodes and the detection mechanism used is packet id based technique for the detection and the suppression of the black hole attack in the sensor network. The Figure 7 represents the throughput for the same network. In the packet id based technique, the cluster head can be detected as the black hole node. When the above graphs are compared with our proposed detection mechanism, the throughput and the packet delivery ratio are improved than the packet id based technique.

V. CONCLUSION

The replacement of the battery of the sensor nodes is difficult as the wireless sensor networks are deployed in a vast topographical territory. Clustering is used to improve the lifespan of the sensor nodes and to reduce the utilization of battery in the nodes. In the black hole attack, the attacker node maliciously drops the packet which is received by that attacker node. The black hole attack causes the depletion of energy (battery power) and the data inconsistency in the sensor network. The attacker node provides the false routing table information during the formation of paths between the nodes in the network. If there's a black hole node present within a network, then the overall performance of the network will be less. In the proposed method, if the network performance becomes less than the threshold performance, then the nodes will monitor the fake reply packets and identify the black hole node and removes it from the network. This will reduce the battery utilization of the sensor nodes and enhances the performance of the sensor network. Our future task will be to develop an algorithm which is capable in detecting the above mentioned attacks as well as collaborative black hole attacks in which nodes act in coordination with each other and are successful in evading detection.

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 5, May 2015

REFERENCES

[1] S. Anbuchelian, Selvamani. K, Chandarasekar. A "An Energy Efficient Multipath Routing Scheme by Preventing Threats in Wireless Sensor Networks", Electrical and Computer Engineering (CCECE), IEEE 27th Canadian Conference, 2014.
[2] Dr. G. Padmavathi, Mrs. D. Shanmugapriya"A Survey of Attacks, Security Mechanisms and Challenges in Wireless Sensor Networks", International Journal of Computer Science and Information Security, Vol. 4, No. 1 & 2, 2009.
[3] Vipul Sharma, KirtiPatil, Ashish Tiwari"Detection and Suppression of Blackhole Attack in Leach based Sensor Network", International Journal of Computer Technology and Applications, Vol 5 (6),1873-1877, 2014.
[4] Amir Shiri et al "New Active Caching Method to Guarantee Desired Communication Reliability in Wireless Sensor Networks", 2012.
[5] Arun K. Somani, ShubhaKher, Paul Speck and Jinran Chen, "Distributed Dynamic Clustering Algorithm in Uneven Distributed Wireless Sensor Network" 2006.
[6] Chris Karlof, David Wagner "Secure routing in wireless sensor networks: attacks and countermeasures", Elsevier, 2003.
[7] Giljae Lee, Jonguk Kong, Minsun Lee and OkhwanByeon"A Cluster-Based Energy-Efficient Routing Protocol without Location Information for Sensor Networks" International Journal of Information Processing Systems Vol.1 No.1, pp. 49-54, 2005.
[8] Ju young Kim, Ronnie D.Caytiles, Kyung Jung Kim "A Review of the Vulnerabilities and Attacks for Wireless Sensor Networks" Journal of Security Engineering, 2012.
[9] Kalpana Sharma and M K Ghose"Wireless Sensor Networks: An Overview on its Security Threats" IJCA Special Issue on "Mobile Ad-hoc Networks" MANETs, 2010.
[10] MdAshiqurRahman and SajidHussain"Effective Caching in Wireless Sensor Network", 2007.
[11] MsManishaRana, Gurpreet Kaur "Improved Circular Caching Based On WSN With Multisink", INTERNATIONAL JOURNAL OF ENGINEERING SCIENCE & HUMANITIES, Vol. 2 Issue 2, pp. 1-4, 2012.
[12] Mudasser Iqbal "An Energy-Aware Dynamic Clustering Algorithm for Load Balancing in Wireless Sensor Networks", JOURNAL OF COMMUNICATIONS, VOL. 1, NO. 3, 2006.
[13] Narottam Chand "Cooperative Data Caching in WSN", World Academy of Science, Engineering and Technology 63, pp. 90-94, 2012.
[14] Naveen Chauhan "Cluster Based Efficient Caching Technique for Wireless Sensor Networks", (ICLCT'2012).
[15] Sheela. D, Srividhya. V. R, Asma Begum, Anjali and Chidanand G.M. "Detecting Black Hole Attacks in Wireless Sensor Networks using Mobile Agent" International Conference on Artificial Intelligence and Embedded Systems (ICAIES'2012).
[16] TEODOR-GRIGORE LUPU "Main Types of Attacks in Wireless Sensor Network", Recent Advances in Signals and Systems, ISSN: 1790-5109.
[17] Virendra Pal Singh Sweta Jain and JyotiSinghai**"**Hello Flood Attack and its Countermeasures in Wireless Sensor Networks", IJCSI International Journal of Computer Science Issues, Vol. 7, Issue 3, No 11, May 2010.