International Journal on Recent and Innovation Trends in Computing and Communication ISSN: 2321-8169
Volume: 5 Issue: 4 148 – 151

Black Hole Attack detection in Zone based Wireless Sensor Networks

Dr. Shreenath K N
Associate Professor
Department of Computer Science and Engineering
Siddaganga Institute of Technology, Tumkur
shreenathk_n@sit.ac.in

Manasa V M
M.Tech Student
Computer Network Engineering
Siddaganga Institute of Technology,Tumkur
manasavm01@gmail.com

Abstract:- The Wireless Sensor Networks (WSNs) became an emerging promising technology deployed in an area for specific purpose and in the wide range of application area such as military application, control and tracking application, habitat monitoring, industry, medicine, health care, agriculture etc. Wireless sensor networks are prone to various attacks. One such type of attack is a black hole attack. A black hole attack is a type of denial of service attack where the node drops the packets fully or selectively, routed through this node which discards the sensitive data packets. This paper deals with the detection of black hole attack inzone basedwireless sensor network using the mobile agents.

Index Terms— *Wireless Sensor Networks (WSNs), Black Hole Attack, Zone, Zone Head (ZH), Mobile agent.*

*****

I. INTRODUCTION

Wireless Sensor Networks (WSNs) is an interconnection of sensor nodes, each sensor node has a ability to sense, process and compute. Sensor node consists of three things such as communication component, sensing component and computation or data processing component. These sensor nodes collect the data, process the data and transmit to sink node or base station by working together. Basic unit of a sensor networkissensor node whichconsistsof onboard sensors,power supply,memory, processor, and wireless modem. A sensor converts a physical phenomenon such as sound, light, heat etc into electrical or other signals which acts as a transducer.

Thus the wireless sensor networks became an emerging promising technology deployed in an area for specific purpose and in the wide range of application area such as military application, control and tracking application, habitat monitoring, industry, medicine, health care, agriculture etc. Wireless sensor networks also prone to various attacks. One such type of attack is a black hole attack.A black hole attack is a type of denial of service attack where the node drops the packets fully or selectively, routed through this node which discards the sensitive data packets. The nodes affected by the black hole attack are known as malicious nodes. By this black hole attack the network completely fails to send the information to the base station.By continuous monitoring the traffic,the black hole nodes can be detected by the lost traffic in the networkand these black hole nodes are invisible. Therefore, delivering the data packets successfully to the destination is better by detecting the black hole nodes and then isolating the black hole nodes from the network. Thus,even in the presence of black hole nodes in the networkthe data packets can be deliveredsuccessfully to the destination.

In this paper, we proposed a method that consists of mobile agent. The responsibility of mobile agent is tomove from one node to anotherfor checking the presence of the black hole nodes in their respective zones. This mobile agent is a self controlling software agent. Here we consider the Zoning method. Zoning is a method in which each sensor nodes present in the zones send data to their ZH thus a lot of energy transmission can be saved by preventing the each sensor node sending data directly to the base station. Hence the ZH collects these data packetsfrom all the sensor nodes in their zone and send these data packets to the sink node or base station. Each zone consists of Zone Head (ZH) along with their sensor nodes.All these exist in the zone head communication range. If a black hole node present in the zone means this black hole node collects the data packets from the sensor nodes but does not forward this data packets to the respective zone heads. Another case is, the ZH may be a black hole node, it also collects the data packets from all the sensor nodes in their zone and does not forward these collected data packets to the base station. Thus the black hole
node affects the network in delivering the packets to the destination. Hence our method helps in detecting the black hole node presence in the network and then it is isolated from the network. Thus the throughput of the network can be increased and end to end delay of packets can be prevented by our proposed method of detecting and isolating the black hole node from the network by the base station.

The rest of this paper is organized as follows: Section 2 consistsofliterature review, section 3 describesthe proposed methodology, section 4describes the implementationand

Section 5 concludes the given paper by listing the black hole detection approach.

II. LITERATURE REVIEW

In paper [1], authors proposed a Protocol for Mobile Sensor Networks (ZoroMSN) called as Zone based Routing Protocolfor the low mobility sensors. ZoroMSNconsiders two phases such as zone-based partition phasewhere the network is divided.Another phase is a clustering phase and then zone head (ZH) is elected. Thus the energy can be saved while transmission in the clustering phase.The ZoroMSNhelps in calculating the mobility factor of a sensor node which is necessary to select a ZH by considering both the moving speed and the localization of the sensors. TheZoroMSN considers the updation of the sensor node's information, for this they consider the update timer, if the update timer expires means then only the sensor nodes update their information and starts exchange the information with their neighbors. It also considers the level of definition when needed to send the data packets towards the sink node or Base Station (BS). The mobility of the nodes related with theupdate-timer and the zone size. They gave the simulation results of ZoroMSN, which has a better performance results for smaller zone sizes and also for the low speed sensors in wireless sensor networks. By the localization approaches, ZoroMSN calculates the coordinates of sensor nodes. ZoroMSN enriched their protocol by designing an energy efficient localization technique which is integrated with the ZoroMSN. Their aim is to integrate the data aggregation with the ZoroMSN protocol which results in reducing thecorrelated data amount transmitted to base station. Thus it helps in the detection of the black hole attack in the network.

In paper [2], authors proposed a method for theblack hole attackdetection which results in the loss of critical information in the wireless sensor network. It also considers the other proposedmethods for this attack in wireless sensor networkwhich usesthe concept of multipath routing and multiple base stations. These methods results in wastage of time. Hence they used the concept of UAV and SPRT method for the detectionof black hole attack and it also compared with the other methods, which results in less time wastagefor the acceptable energy consumption. Also they proposed the methodwith higher probability compared to other methods for the detection of black hole nodes. It considers the UAV for checking the sensor nodesrandomly in the network.

In paper [3], authorsproposed a effective method for the detection and prevention of black hole attacks in the network. It uses the routing algorithm. Consider routing via multiple base stations forthe detection of black hole attack in the network. In order to reduce the energy consumption in WSNs, it considers the routing carried out through the nearest base station only. It also uses the check agents which play a very important role in detection of black hole attacks in the network.Thus reduces network overhead and also it decreases the complexity of the messages. Usage of multiple base stations ensures the data delivery, thus gives the significant method compared to other methods.

In paper [4], authors proposed a approach which is based on two cluster heads in a cluster. In the detection phase the base station detects the malicious node. In removal phase the malicious node is removed by the base station. Various techniques for blackhole detection and prevention are presented.

In paper [5], authors proposed a OWCA (Optimized Weight-based Clustering Algorithm) to form clusters bydividing the network to reduce the energy consumption in the network. This proposes a method for preserving the energy while detection against the black hole node. It detects the node ID of the black hole node by the proposed detection mechanism. Then the black hole node is removed from the network.Thus the black hole node does not participate in any clustering algorithms. Hence theend to end delay, packet delivery ratio, energy and throughput are affected in the presence of the black hole node in the network. They also observed thatnetwork degraded very rapidly in the presence of black hole node in clustering based Wireless sensor network.

In paper [6], authorsproposed a scheme called an active detection. The scheme is novel security and trust routing. It contains the excellent properties such assecurity, scalability andhigh successful routing probability. The scheme Active Trusthelps for the detection of the nodal trust.It also helps in avoiding the suspicious nodes which results in 100% successful routing probability. It also exhibits the energy efficiency highly. It constructs the multiple detection routes by the Active Trust scheme which uses residue energy. It exhibits the theoretical analysis and experimental results where it improves the probability of routing successfully by 3 times and in some cases up to 10 times.

III. PROPOSED METHODOLOGY

We are considering the sensor field network area as a large square. Then divide thelarge square sensor field area into non overlapping square zones. These divided square zones are of same size and they have unique Zone ID where all these information is given by the base station. Corresponding to the coordinates of the origin point of the sensor field area, each zone has a unique Zone ID (i , j), as shown below (Fig 1) where darker nodes are sensor nodes and lighter nodes are zone head nodes in the respective zones.

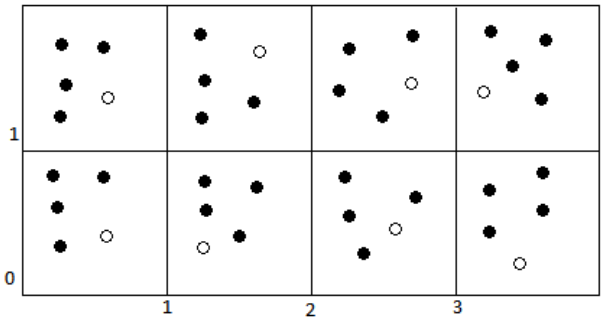

Figure 1: Zones with their sensor nodes and Zone Heads

Step 1: In the proposed mechanism, first consider the Zones creation [1] phase. In this phaseit divides the large sensor field area into a non overlapping square zones which are ofsame sizeand they have unique Zone ID.In the zones, the sensor nodes arelocated. Base Station sends the zonal information to all the sensor nodes present in the sensor field. The sensor nodes know their location by localization algorithm in their respective zones.

Step 2: The Zone Head Election phase is used where a node acts as a zone head (ZH) which has a responsibility of sending or forwarding the messages to the base station. The Zone Head is elected based on energy of the nodes. Initially the nodes having highest energy are chosen as Zone Head. Each sensor nodes exchange their energy values with their neighboring sensor nodes. Hence they become know about which is the node having the highest energy. Then the node having the highest energy sends the information to the base station and also to the zonal sensor nodes that, it is the zone head for a particular zone. Then the sensor nodes are connected to their respective Zone Heads in their Zones. The sensor nodes send data packets to their zone head. Then zone head process the data and send it to the base station.

Step 3: The mobile agent randomly visits the nodes and zone heads in their respective zones. The base station gives the information about the zones, sensor nodes and zone heads for the mobile agent. When the mobile agent visits a particular node, if it is not able to receive or forward the packets means then it suspects that, this node is black hole node. Then the suspected black hole node information is given to the zone head and later the zone head gives the information to the base station, afterwards that suspected node will be removed from the network by the base station. If the zone head node is the black hole node, then the mobile agent directly gives the information to the base station and then suspected zone head node will be removed by the base station. Afterwards a new Zone Head is elected based on the node which is having the highest energy among remaining sensor nodes in that zone.

Algorithm for Zone Creation:

Begin
Consider the sensor field network areaas a large square.
Then divide large square area into non overlapping square zones.
Each zones having the same size and a unique zone ID.
Base station sends the zonal information to each sensor nodes.
Then each node know their location by localization algorithm in that zone.
End

B. Algorithm for Zone Head Election:

Begin
In a particular zone,
Each sensor nodes exchange their energy values with their neighboring sensor nodes in that zone.
Hence they know about which is the node having the highest energy.
Node having the highest energy sends the information to the base station and also to the zonal sensor nodes.
End

C. Algorithm for Mobile Agent:

Begin
For a particular Zone,
Base station gives the information about the zones and zone heads for the mobile agent.
Mobile Agent visits every node randomly.
And checks every node whether it is sending or receiving the data packets.
If not means it suspects as a black hole node.
This suspected information is given to their respective zone head.
Then that zone head informs to the base station.
Base station removes the black hole node from the network.
else
Continue the normal process of detecting a black hole node.
If the suspected black hole node is a Zone head.
This suspected information is given to the base station by the mobile agent.
Base station removes the black hole node from the network.
Then a new zone head is elected based on the highest energy
End

IV. IMPLEMENTATION

Our proposed method is decidedto carried out in Network Simulator NS2 which is free and easy to use. NS2 advantages areinexpensive, costly equipments are not required, complex scenarios can be easily tested, results can be obtained quickly, more ideas can be testedin a smaller time frame, it supports variety of protocols, itsupportsdifferent platforms and it also

supports modularity. Reducingthe energy consumptionand system delay are the main goals of zone based sensor networks.

V. CONCLUSION

In this paper, we proposed a method for black hole nodes detection in the sensor field. Our method consistsof zone creation phase, it divides the sensor field into zones are of same size. Base Station sends the zonal information to the ZH, then these ZHs give zonal information to their respective sensor nodes. The sensor nodes know their location by localization algorithm in their respective zones. In zone head election phase a node acts as a zone head (ZH) which has a responsibility of forwarding the messages to the base station. The Zone Head is elected based on the energy of nodes. Initially the nodes having highest energy are chosen as Zone Head. Then the mobile agent randomly visits the nodes and the zone heads in their respective zones. When the mobile agent visits a particular node, if it is not able to receive or forward the packets means then it suspects that, this node is black hole node. Then the suspected black hole node will be removed from the network by the base station. If the zone head node is the black hole node, then it will be isolated by the base station in the network and a new Zone Head is elected based on the node which is having the highest energy among all the sensor nodes in that zone.

REFERENCES

[1] Nidal Nasser, Anwar Al-Yatama and Kassem Saleh "Zone-based routing protocol with mobility consideration for wireless sensor networks", Springer, 2012.

[2] Maryam Motamedi and Nasser Yazdani "Detection of the Black Hole Attack in Wireless Sensor Network Using UAV", International Conference on Information and Knowledge Technology, 2015.

[3] Reem Alattas "Detecting Black-Hole Attacks in WSNs using Multiple Base Stations and Check Agents", Future Technologies Conference, 2016.

[4] Prachi Dewal, Gagandeep Singh Narula and Vishal Jain "Detection and Prevention of Black Hole Attacks in Cluster Based Wireless sensor Networks", 2016.

[5] Chunnu Lal and Akash Shrivastava "An Energy Preserving Detection Mechanism for Blackhole Attack in Wireless Sensor Networks ", International Journal of Computer Applications, 2015.

[6] Yuxin Liu, Mianxiong Dong, Kaoru Ota and Anfeng Liu "ActiveTrust: Secure and Trustable Routing in Wireless Sensor Networks", IEEE Transactions on Information Forensics and Security, 2016.