PROFILE BASED PROTECTION SCHEME AGAINST DDOS ATTACK IN WSN WITH DUAL CLUSTERING ALGORITHM

Subhashini[1], G.Murali[2]

[1]*M. tech, Computer Science and Engineering, JNTUA College of Engineering, Pulivendula, Andhra Pradesh, India*
[2]*Assistant Professor, Computer Science and Engineering, JNTUA College of Engineering, Pulivendula, Andhra Pradesh, India*

Abstract

Wireless Sensor Network is combination of sensors to make a communication between sensors to control station. Sensors forward the data like a relay communication. Sensor nodes continuously inter changing the data from one node to another node. In this paper we are using the AODV Routing protocol for rout establishment. This protocol discovers the shortest path from source to destination. Most of the Wireless Sensor Network facing security issues in real scenario, and also there are many attacks in wireless sensor networks. DDOS (distributed Denial of Service) attack is a main attack it creates dummy packets and it flooded in network. Sensors receives the that packets and it also broadcast that packets into its neighbours. These need less packets consume the resources, reduce the traffic load, throughput as well as energy of each and every sensor. Here we proposed profile based protection scheme in wireless sensor networks. This technique checks the profile of the each node in WSN and valid this node is good or malicious node. Then malicious node is eliminated by CH (Cluster Head) by using dual clustering algorithm. Each cluster having the cluster head. Cluster head selected by that residual energy and cluster head collect the data and forward it to the sink node. Profile based protection scheme protect the network from DDOS attacks and decrease the loss of major resources like memory ,power, and the performance of the network is considered by traffic load, throughput etc.

Keywords: *Wireless sensor network, Dual clustering algorithm, AODV Routing protocol, DDOS Attacks Profile based Protection Scheme*

----------***----------

1. INTRODUCTION

A wireless sensor networks consists of spatially distributed autonomous sensor nodes to monitor physical or environmental conditions, such as temperature, sound, pressure, etc. And to cooperatively pass their data through the network to a main location. The most modern networks are bi-directional, also enabling control of sensor activity. The development of wireless sensor networks was motivated by military applications such as battlefield surveillance. Today such networks are used in many industrial and consumer applications, such as industrial process monitoring and control, machine health monitoring, and so on

In wireless sensor network Dos (Denial of service) attack creates weakness Network. The flooding packet travel again and again in the network. So, all the resources like energy, memory band width are wasted by these kinds of attacks. If we avoid this kind of attacks we can make most robust network.

The main aim of this project is rectifying the problems from various DOS attacks in wireless sensor network. When solving flooding amount of unnecessary packets by proposed technique profile Based protection scheme, it will reduce energy loss and also creates network more robustness.

2. APPLICATIONS

2.1 Forest Fire Detection

In wireless sensor network sensors are deployed in large aria to detect when fire is started and spread it. In forest aria nodes can be equipped with sensors to measure gas leakage, humidity, temperature etc. These are produced by vegetation or fire in the trees. In forest aria the early detection is crucial for success full action of the fire fighters.

2.2 Air Pollution Monitoring

For air pollution detection ad-hoc wireless networks can be deployed in many cities. In these cities wireless sensor networks monitor the concentration of dangerous gases. These can take advantage of the ad-hoc wireless links rather than wired installation, it also make them more mobile for testing readings in different arias.

2.3 Water Quality Monitoring

In many areas ad-hoc wireless sensor networks are deployed for analysing and monitoring the water properties in oceans, lacks, rivers and dams. This network enables the creation of more accurate map of the water status. And it allows the permanent deployment of monitoring station in location of difficult access.

3. ATTACKS IN WSN

In wireless sensor networks there are many tiny nodes in large area. These are in danger due to the broadcast nature of the transitions medium and also having the additional vulnerabilities because of the nodes are arranged in unreceptive environment. Here classified the attacks

3.1 Hello Flood Attack

In wireless sensor network attacker sends or reply hello packets from source to destination with high radio transition rang. Sensor nodes isolated in arranged area with in wireless sensor networks. So because of this problem sensors are inclined that the enemy node is their neighbour. So as a result while sending the information to the base station the malicious node is try to go through the attacker and they know that is their neighbour and ultimately spoofed by the attacker.

3.2 Distributed Denial of Service Attack

Distributed denial of service attack creates the weakness in wireless sensor networks. In this type of attacks an attacker flooded the unnecessary packets from source to destination in the network. Nodes receive that packets and transmit them to their neighbours. Because that problem any energy levels is not considered. It will loss the major resources like memory, bandwidth and energy levels of each and every node.

4. PROPOED SYSTEM

In this project we are proposed profile based protection scheme with dual clustering algorithm. This technique fully solves the DDOS attacks. Checks the profile of the each node whether this node are good or malicious. That Malicious node eliminated by respective cluster head. Here we are using AODV routing protocol

4.1 Working AODV

In this paper using Ad Hoc On-Demand Distance Vector Routing Protocol. This protocol discovers the routs from source to destination. If source node has no route to the destination, then source node initiate the route in an on demand fashion. Source node flooded the route request packets in the network. After sending rout request destination node send the rout replay packet to the source node. Source node may obtain the multiple routs to the different destinations. So here select best path to transmitting data. Here route request packet carries the source identifier (SrcID), the destination identifier (DestID), and the destination sequence number (DestSeqNum). If path link is brocken in the network select the another path for tranmiting the data.

4.2 Topology Formation

Initially we are placing nodes in the network and we choose a source and destination. If the source has no route to the destination, then source A initiates the route discovery in an on-demand fashion. After generating RREQ, node looks up its own neighbor table to find if it has any closer neighbor node toward the destination node. If a closer neighbor node is available, the RREQ packet is forwarded to that node. If no closer neighbour node is the RREQ packet is flooded to all neighbour nodes. When destinations receive

4.3 Cluster Creation

Nodes will form a group that is called us clusters. Each cluster has a cluster head for collecting the data and forwards it to the sink node. Cluster Head will randomly choose by depending upon its residual energy

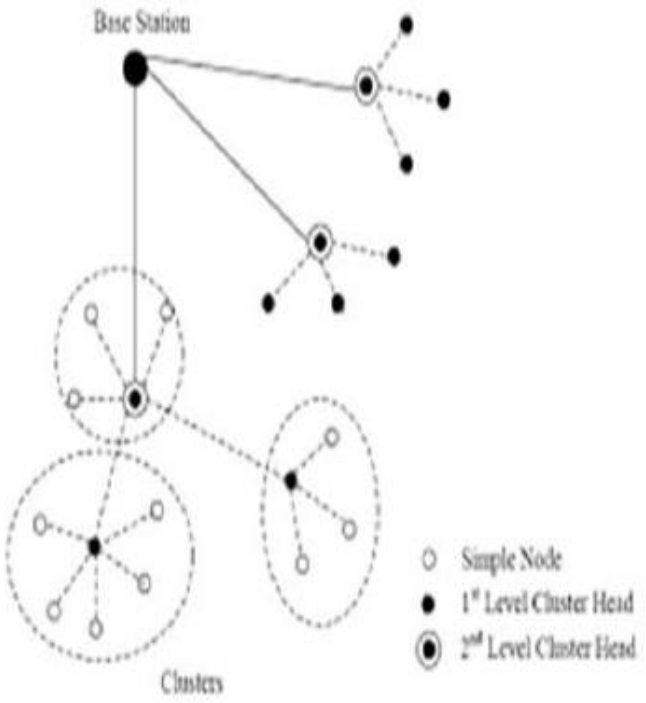

Fig-1 cluster creation

4.4 Dual Clustering Algorithm

In this paper we use the clustering Technique. This technique is effective technique to reduce power consumption and band width consumption in wireless sensor network. In clustering algorithm there are number of tiny nodes in the network. These nodes are choosing the cluster heads (CH) based on its residual energy. Remaining nodes are considered as the members of the cluster head. Cluster nodes connected with the corresponding cluster heads in the network. Cluster head collect The data from his cluster members and forward it to the base station.

Activity Diagram

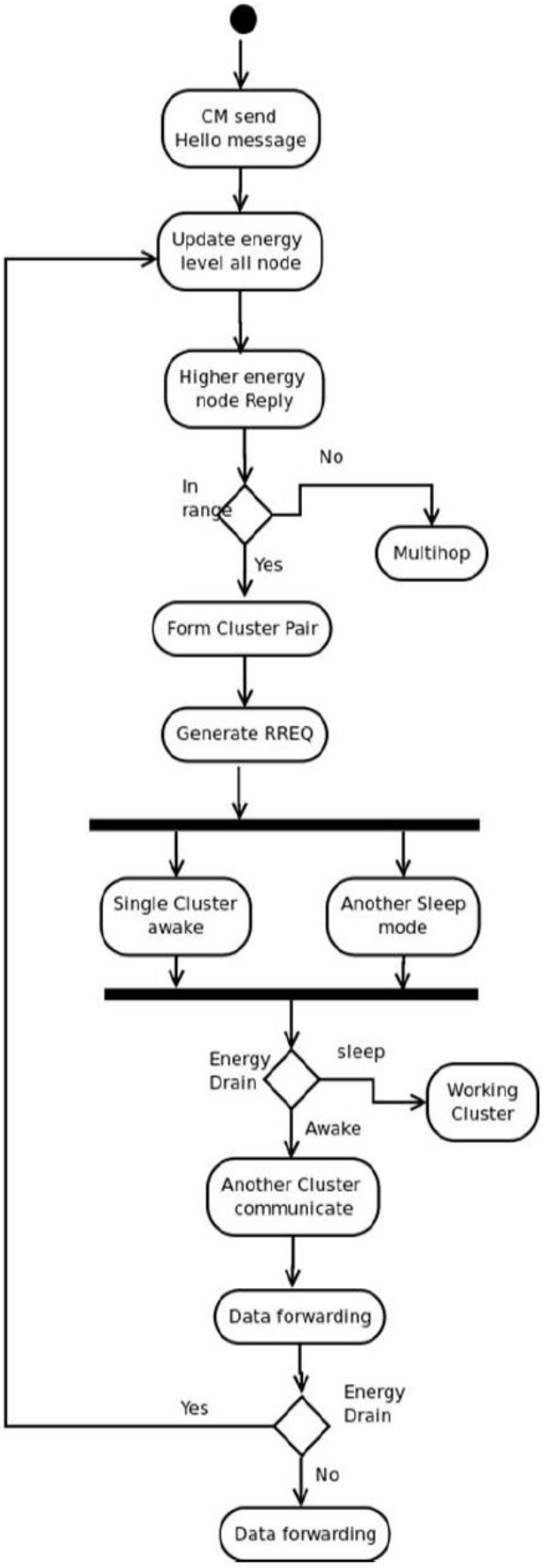

Fig-2 Activity diagram for dual clustering algorithm

Here we use two clusters for data forwarding scheme. It will be sleep mode in idle state and check the status periodically. If cluster node had drain energy, it will send a request to the next CH node. That node can begin to carry their information from neighbour

4.5 Profile Evidence Collection

Every time interval, member nodes will send the observations of nearby nodes. This evidence is send to Cluster Head. Evidence means the activities of node.

4.6 Cluster Auditing

Cluster Head check the received evidence. The validation process is done by number of evidence received against the particular node. Which node have high number of evidence against it activities that node consider as misbehavior node.

4.7 Eliminating Misbehaviour Node

Misbehaviour node is eliminated from the network by respective Cluster Heads. Finally the comparison is compared by both existing and proposed.

5. SIMULATION RESULTS

Here we are calculating the performance metrics by using network simulators ns2.3

Packet Delivery Ratio: Fraction of the number of packets send by the sender and number of packets received by the receiver is called packet delivery ratio

Throughput: when sending the packets by the sender number of packets received per unit of time.

Packet Loss: number of packets sending-number of packets received

Table-1 Experimental Results

Metrics	Attack Case	Profile based Scheme Case
Send Packet	2754	2754
Receive Packet	2042	2650
Packet Loss	712	72
Pdf	74.14	97.38
End to end delay	498.63	602.72

Here table and graph show the overall network performance. Table represented the values of the packet delivery ratio, packet loss end to end delay. Here compared the proposed scheme with the attack case. In attack case the shows 55% infection, when apply the proposed scheme it shows the better routing result compared with the attack case, and also reduce the infection analysis, reduce packet loss, increase the packet delivery ratio.

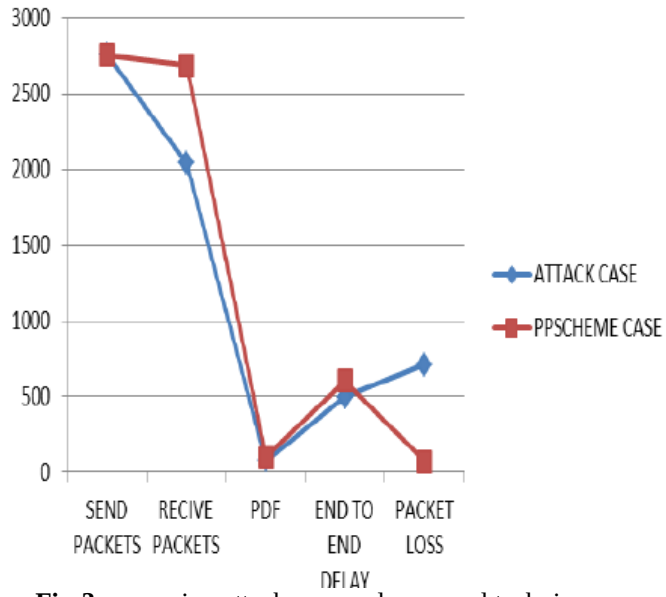

Fig-3 comparing attack case and proposed technique

6. CONCLUSION

In wireless sensor network contains the number of nodes, these are forward the information from one node to another node continuously, That information in the form of large packets, these packets flooded in the whole network and transmits it to their neighbours. So in that time network affected from the Distributed Denial of Service attacks. It creates the dummy packet and flooded in the network. This attack loss the major resources like energy bandwidth power etc. Here proposed scheme protect the network from these attacks. It checks the profile of the each node, and Misbehavior node is eliminated from the network by respective Cluster Heads. Finally the comparison is compared by both existing and proposed it provides the better performance to compare with the normal routing. It increases the packet delivery ratio, throughput, and reduces packet loss.

REFERENCES

[1] Charles E.Perkins et. al. has presented ―Adhoc On-Demand Distance Vector Routing‖ in 2003.

[2] A.P.Subramanian et. al. has presented ―Multipath Power Sensitive Routing Protocol for Mobile Ad hoc Networks‖ in 2004.

[3] Akhtar et. al. Has presented ―Energy Aware Intra Cluster Routing for Wireless sensor networks‖, in 2010.

[4] M. Younis et. al. has presented ―Energy- Aware Routing in Cluster-Based sensor networks‖, in 2002

[5] Ian F et. al. has presented ―A Survey on sensor networks" ieee communication Magazine in 2002

[6] Y. wang, g. attebuty, and B. Ramurthy, "A Survey of security issues in Wireless Sensor Networks" ieee communication Survey tutorials, in 2006

[7] C. Schurgers et. al. has presened ―Energy Efficient Routing in Wireless sensor networks‖, in 2002.