Detection or Prevention of DDOS Attack in WSN using Clustering

Ravi Parashar[1] Rajesh Singh[2]
[1,2]Department of Computer Science Engineering/ Information Technology
[1,2] NITM Gwalior, India

Abstract— Wireless Sensor Network (WSN) is a large network of sensor nodes. Wireless Sensor Networks are very popular and have their special characteristics such as limited battery, limited power and limited storage that makes the energy consumption. Although there are some limitations, but there are many advantages of Wireless Sensor Networks. Some advantages are robustness, scalability, flexibility. WSN also reduces the cabling cost. Now a days WSN is mostly used in modern technologies to gain, the output in the most efficient way. Some applications of WSN are area monitoring, health care monitoring, Earth is sensing, Landslide detection etc. This paper presents a approach for detecting and preventing dos as well as gray hole attack.

Key words: WSN; Dos; Gray hole; AODV

I. INTRODUCTION

In the most recent couple of years wireless sensor network (WSNs) have drawn an influential impact on the research area relating its challenges and applications [1]. This dynamic examination in WSNs investigated different new applications empowered a bigger scale network of sensor nodes equipped for detecting data from nature, handle the detected information and transmits it to the remote area [2-4]. WSNs are for the most part utilized as a part of, low transmission capacity and delay tolerant, applications running from common and military to ecological and social insurance observation.

WSN node is low-power detecting devices, inserted processor, and communication channel and control module. The installed processor is for the most part utilized for gathering and handling the sign information taken from the sensors. Sensor component creates a quantifiable reaction to an adjustment in the physical condition like temperature, humidity.

A. System Requirements

Here we discuss some of the characteristic requirements of a system comprising wireless sensor nodes. The system should be:

1) Fault tolerant: the system should be robust against node failure (running out of energy, physical destruction, H/W, S/W issues etc.) Some beep mechanism should be incorporated to indicate that the node is not functioning properly.
2) Scalable: The system should support large number of sensor nodes to cater for different applications.
3) Long life: The node's life-time entirely defines the network's life-time and it should be high enough.
4) The sensor node should be power efficient against the limited power resource that it have since it is difficult to replace or recharge thousands of nodes. The node's communication, computing, sensing and actuating operations should be energy efficient too.
5) Programmable: the reprogramming of sensor nodes in the field might be necessary to improve flexibility.
6) Secure: the node should support the following
   1. Access Control: to prevent unauthorized attempts to access the node.
   2. Message Integrity: to detect and prevent unauthorized changes to the message.
   3. Confidentiality: to assure that sensor node should encrypt messages so only those nodes would listen who have the secret key.
   4. Replay Protection: to assure that sensor node should provide protection against an adversary reusing an authentic packet for gaining confidence/network access, man in the middle attack can be prevented by time stamped data packets.
7) Affordable: the system should use low cost devices for the network comprises of thousand of sensor nodes, tags and apparatus. Installation and maintenance of system elements should also be significantly lower to make its deployment realistic.

B. Challenges of WSN

Scalable and flexible architecture- On the sensor network the number of sensor nodes deployed may be ordered of hundred, thousands or millions so that we can easily extend the network size. The communication protocols must be designed in such a manner that deploying many nodes in the network does not affect clustering and routing. In other words, the network must preserve its stability. Introducing more nodes in the network means that additional communication messages will be exchanged, so that these nodes are integrated into the existing network [5].

1) Fault tolerance and adaptability- Fault tolerance intends to keep up sensor system functionalities with no intrusion because of failure of sensor node in light of the fact that in sensor arrange each node have restricted force of vitality so the failure of single node doesn't impact the general errand of the sensor system. Adaptable protocols can set up new connections in the event of node failure or link breakage. The system can ready to adjust by changing its network if there should be an occurrence of any issue. All things considered, well-proficient routing algorithm is connected to change the general arrangement of system.
2) Infrastructure- Sensors network are framework less in which nodes can communicate without a base station. It uses multi-hop radio relaying and number of base station relies on zone secured by node and its radio reach.
3) Dynamic changes- As in sensor system nodes are equipped with no topology and they are versatile to changes because of expansion of new nodes or failure of nodes. In this manner, not at all like conventional systems, where the objective is to augment the channel throughput or minimize the node deployment, yet in a sensor system center is to expand the framework lifetime and the framework power.

4) Power Consumption- Wireless sensor node is tiny device means it is deployed with a restricted amount of power source. Nodes relays on battery for their power. Thus power preservation and power supervision is an essential issue in WSN.
5) Security- Security is a key parameter in the sensor system since sensor systems are information driven so there is no specific id connected with sensor nodes and attacker can undoubtedly embedded him into the system and stole the essential information by turning into the piece of system without the learning of sensor nodes of the system. So it is hard to recognize whether the data is confirmed or not.

II. AODV OVERVIEW

AODV [6] has a place in the class of Distance Vector Routing Protocols (DV). In a DV each node knows its neighbours and the cost to reaching them. A node keeps up its own routing table, putting away all nodes in the system, the distance and the following hop to them. On the off chance that a node is not reachable the distance to it is set to interminability. Each node sends its neighbours intermittently its entire routing table. So they can check if there is a valuable path to another node utilizing this neighbour as next hop. At the point when a connection breaks a Count-To-Infinity could happen.

AODV is an 'on demand convention' with little delay. That implies that routes are just settled when expected to lessen activity overhead. AODV bolsters Unicast, Broadcast and Multicast with no further conventions. The Count-To-Infinity issue is fathomed with sequence numbers and the registration of the expenses. In AODV each hop has the consistent expense of one. The courses age rapidly with a specific end goal to oblige the development of the movable nodes. Link breakages can locally be repaired proficiently.

For unicast routing three control messages are utilized: RREQ (Route REPly), RREP (Route REPly), RERR (Route ERRor).If a node wants to send a packet to a node for which no route is available it broadcasts a RREQ to find one. A RREP includes a unique identifier, the destination IP address and sequence number, the source IP address and sequence number as well as a hop count initialized with zero and some flags. Node gets a RREQ which it hasn't seen before it sets up a reverse path to the sender. On the off chance that it doesn't know a path to the destination, it rebroadcasts the overhauled RREQ particularly increasing the hop check. In the event that it knows a path to the destination, it makes a RREP. The RREP is unicasted to the cause node exploiting the reverse path. A RREP contains the destination IP address and sequence number, the source IP address, a time to live, a hop considers well as a prefix utilized for subnets and a few flags. At the point when a node gets a RREP it checks if the hop count in the RREP for the emitter of the message is lower than the one in its own particular routing table or the destination succession number in the message is higher than the one in its own particular routing table. In the event that none of them is genuine it just discards the packet. Else it overhauls its routing table and on the off chance that it is not the destination it reunicasts the RREP.

In such networks link breakage is exceptionally normal. In the event that a node understands that different nodes are not any more reachable it telecasts a RERR containing a rundown of the inaccessible nodes with their IP addresses and sequence number and a few flags. A node who receives a RERR repeats over the list of inaccessible destinations, checking if a next hop in its routing table contains one of these nodes. In the event that yes it upgrades its routing table. On the off chance that the accepting node still keeps up routes to inaccessible nodes it telecasts its own particular RERR containing this data. Routes and connect lifetime are stretched out by sending a packet over it and by hello messages. A hello is a unique RRER which is substantial for its neighbours. A node might telecast intermittently a hello message so that no connection breakages are accepted by its neighbors when they don't hear anything from it for quite a while. In the event that a connection in a dynamic route breaks a node can attempt to repair the defeat locally. To do this, it discharges a RREQ to locate another path to the destination on the broken connection side not touching the other bearing of the path. It exist another uncommon packet a RREP-ACK which is utilized for inconsistent or unidirectional connections. Additionally some other unique components are utilized like forerunners to track the rundown of dynamic path for utilizing as a part of RERR discharge.

III. DENIAL OF SERVICE ATTACK

A Denial of Service attack is an attempt that makes a computer framework (server or client) or certain other assets unavailable to authentic clients. Ordinarily, this assault is thought to be an issue of PC system, yet for a solitary CPU additionally it can be available among different assets. The objective of this attack may differ from individual yet it major task is to avoid certain services from operating effectively either for the moment or for an indefinite period. Normally, this attack immerses the victim by very high transmission demands and because of this the targeted source can't reply the authentic all or reply gradually, vanishing its viability. It might reset the victim or involves the greater part of its assets hindering its transmission route [7]

The existence of DoS can be recognized:

- Slows the network performance
- Spam mails are increased
- Unavailability of certain websites.

Fundamentally the DoS attack can be characterized into the accompanying sorts as per the kind of destruction it does:

- Utilization of assets such as memory space, processor time, bandwidth etc
- Modification or removal of routing data
- By resetting TCP session disrupts state information
- Physical elements are destroyed

IV. GRAY HOLE ATTACK

In gray hole attack, nodes sometimes acts as authentic node as well as malicious. When a node forwards the packet it operates as authentic node, where it drop packet becomes malicious. Gray hole attack is a attack that selectively drops packet. [8].

V. LITERATURE SURVEY

Dharini et al (2015) in [9], devised an approach for detecting flooding attack and gray hole attack. The devised detection mechanism consumes much less power and likewise there is no longer so much exchange within the metrics and extend

when compared to quality hierarchical wireless sensor community state of affairs. As a consequence the devised detection mechanism is gentle weight in nature, thus proving it effective. A mild weight, vigor prediction algorithm is carried out to become aware of the abnormality of the nodes' habits. Prediction accuracy got is rather immoderate thereby the detection accuracy can be performed. The devised detection scheme will advance the detection ratio, thereby accomplishing power saving.

Muhammad Amir et al (2014) in [10],analyzed more than a few methods to avoid ddos attacks headquartered on site traffic anomaly parameters, botnet flux identifications, neural networks, entropy variants, application layer ddos security and gadget level safeguard. The paper additionally discussed some typical methods comparable to trace again and packet filtering procedures.

Saman Tahavi Zargar et al (2013) in [11] have investigated the scope of DoS flooding attack situations and tried to defy it and classify the DoS flooding attack and characterize existing countermeasures relayed on where and after they count on, respect, and react to the DoS flooding attack.

HizbullahKhattak et al [12], provided a solution for eliminating the existence of black and gray hole attacks. For this the primary encountered path is avoided and prefers the second minimal route for communication. At any time when source node receives the reply messages from more than a few nodes which might be related with destination, it without problems discards the first reply message arriving from any intermediate node that is connected with destination for the avoidance of the attacks.

Avenash Kumar et al [13], this procedure incorporate three principle ventures for successful measure for distinguishing and also maintaining a strategic distance from the attack. The initial step is to save the answer packet second step is checking the bounce separations of the hub that is seen to be suspected and the last step is to dismiss the answer parcel. For perceiving the suspected node, the venerated neighbor of before node and the node that is suspected checks the two hop separation node ability to achieve the destination.

VI. PROBLEM STATEMENT

Existing work is depended upon energy utilization and selection criteria of cluster head, at every instance when change cluster head transfers routing table in this method memory utilization is high and memory overhead is increased which is shortcoming of WSN relaying on consumption of energy we cannot declare any node as a suspicious.

VII. PROPOSED WORK

For overcome this problem we give the solution that is based on clustering named "detection or prevention of ddos in WSN using clustering". In this approach first electing cluster head (CH) than after each 10 rounds changing CH. Only CH communicate with other cluster head RREQ of each node check if does not receive RREP than only cluster node broad cast the node id of this node and node block this node same as when acknowledgement does not get by shortest path than cluster head check this node and then broadcast node id so that all node block this node.

PROPOSED FLOWCHART

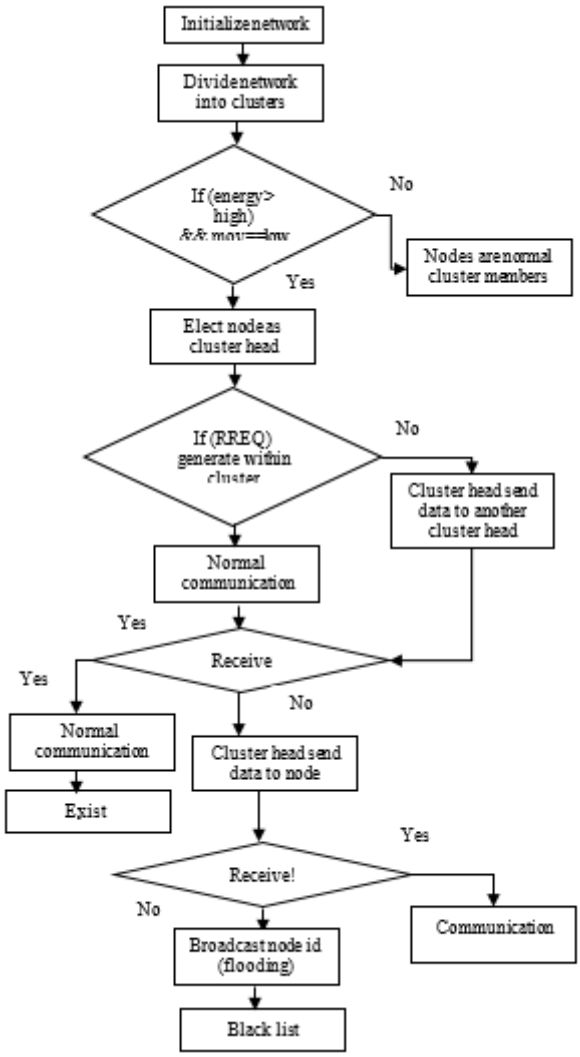

Fig. 1: Flowchart of Proposed approach

VIII. SIMULATION AND RESULTS

The simulation is carried out on ns-2. The number of node used is 50 nodes. The xy-dimension is of size 2000X2000. The initial energy is 0.5joules. The start of simulation is 0.1miliseconds and the end of simulation is 100.0miliseconds.

Parameters	Values
XY Dimension	2000X2000
Number of nodes	50
Initial energy	0.5joules
Start simulation	0.1miliseconds
End simulation	100.0 milliseconds

Table 1: Simulation Parameters

Throughput:

Per second transfer of data on bandwidth is known as throughput. The Fig.2 represents a throughput graph between base approach and proposed approach. The throughput of the proposed approach is good than the base approach.

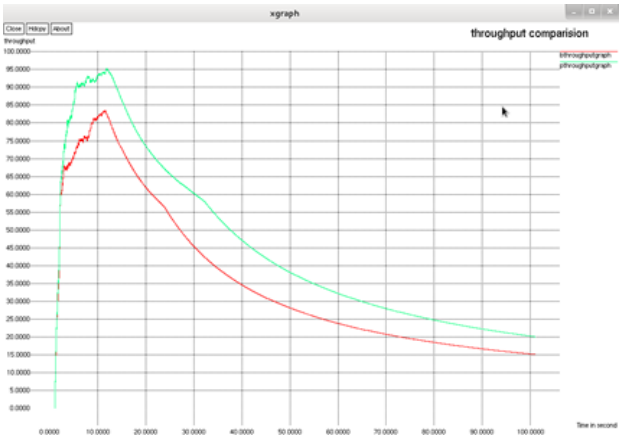

Fig. 2: Throughput Comparison Between Base and Propose Approach

Packet delivery ratio:

Defined as the ratio of packets delivered from source to destination. The Fig.3 represents a PDR graph between base approach and proposed approach. The packet delivery ratio of the proposed approach is good than the base approach.

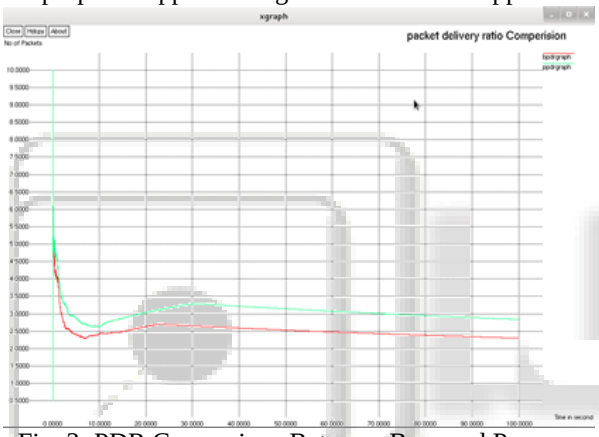

Fig. 3: PDR Comparison Between Base and Propose Approach

Routing Overhead:

The routing overhead is defined as data of data and flooding of data in the network transmitted by application, which utilizes a bit of accessible transfer rate of communication protocols. The Fig.4 represents a routing overhead graph between base approach and proposed approach. The overhead of the proposed approach is more than the base approach. Since the overhead should be minimum but as the routing increases in the proposed work the overhead also increases.

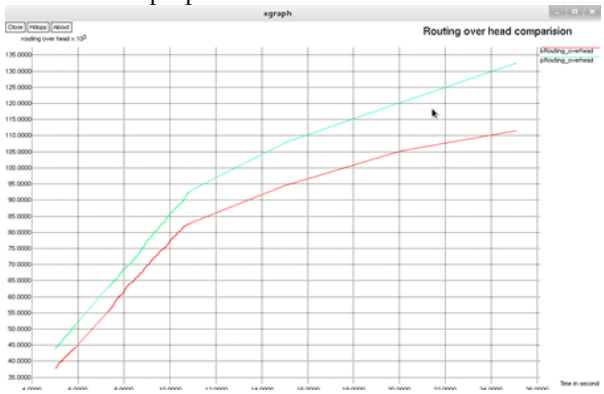

Fig. 4: Routing Overhead Comparison Between Base and Propose Approach

IX. Conclusion

WSN is a framework less network tiny nodes known as sensors are deployed. The major drawback of such network is security. Attacks are easily deployed. Here discussing the major dos attack which disrupts network performances and consumes a lot of energy of a node. For detecting malicious behaviour of nodes providing a solution named detection or prevention of ddos attack in WSN using clustering. This approach results in better outcomes in terms of packet delivery ratio, throughput, routing overhead. In future, this approach can be implemented on different routing protocols.

References

[1] I.F. Akyildiz, T. Melodia, and K.R. Chowdhury, "A Survey on wireless multimedia sensor networks," Computer Networks (Elsevier) J., vol. 51, pp. 921-960, 2007.

[2] J. Feng, F. Koushanfar, M. Potkonjak,"System-Architectures for Sensor Networks Issues, Alternatives, and Directions", IEEE International Conf on Computer Design (ICCD), Germany, 2002. pp. 226- 231

[3] D. Culler, D. Estrin, M. Srivastava, "Overview of Sensor Networks", IEEE Computer, USA, vol 37, pp. 41-49, August 2004.

[4] K. Raja, I. Daskalopoulos, H. Diall, S. Hailes, T. Torfs, C. Van Hoof and G.Roussos, "Sensor Cubes: A Modular, Ultra-Compact, Power-Aware Platform for Sensor Networks", Int Conf on Inf Proc in Sensor Networks (IPSN SPOTS), USA, pp. 2065-2075, vol 48, No6, April 2007.

[5] Ajay Jangra Swati, Richa, Priyanka; "Wireless Sensor Network (WSN): Architectural Design issues and Challenges ".International Journal on Computer Science and Engineering, 2010.

[6] AODV, Presentation at ETH Zürich April 02 © Rainer Baumann, baumann@hypert.net

[7] Dhara Buch, D. C. Jinwala;" Denial of Service Attacks in Wireless Sensor Networks". INSTITUTE OF TECHNOLOGY, NIRMA UNIVERSITY, AHMEDABAD – 382 481, 09-11 DECEMBER, 2010

[8] Ruchita Dhulkar, Ajit Pokharkar, Mrs. Rohini Pise;" Survey on different attacks in Wireless Sensor Networks and their prevention system". International Research Journal of Engineering and Technology (IRJET), 2015

[9] N. Dharini, Ranjith Balakrishnan And A. Pravin Renold;" Distributed Detection Of Flooding And Gray Hole AttacksIn Wireless Sensor Network". International Conference On Smart Technologies And ManagementFor Computing, Communication, Controls, Energy And Materials (ICSTM),2015

[10] Muhammad Aamir and Mustafa Ali Zaidi, "DDoS Attack and Defense: Review of Some Traditional and Current Techniques", SZABIST, Karachi, Pakistan,2014

[11] Khatt ak, Nizamuddin, Fahad Khurshid, Noor ul Amin "Preventing Black and Gray Hole Attacks in AODV using Optimal Path Routing and Hash." IEEE, 2013

[12] Saman Taghavi Zargar, James Joshi, David Tipper, "Defense Mechanisms Against Distributed Denial of

Service (DDoS)Flooding Attacks" IEEE communications surveys 2013

[13] Avenash Kumar, Meenu Chawla; "Destination based group gray hole attack detection in WSN through AODV". Internationl Journal of Computer Science,2012

