Selective Zone head based algorithm for Denial of service Attack in Wireless Sensor Network

Rakhi Jaiswal[1], Prof. Durgesh Wadbude[2]
[1]Department of Computer Science & Engineering, [2]HOD dept. of Computer Science & Engineering
Mittal Institute of Technology, Bhopal, India

Abstract—In Wireless Sensor Networks throughput, packet delivery ratio and routing overhead is a biggest issue in now a days. Conventional routing protocols are not up to the mark in denial of service attack. This proposed algorithm is address the issues of Denial of service Attacks like flooding attack, black hole attack and gray hole attack. In case of cluster based algorithm cluster head try to get better result on the parameters of packet delivery ratio, throughput and routing overhead, here selective zone head based algorithm for Denial of service attack in Wireless Sensor Network try to resolve the limitation of cluster head based algorithm.

Keywords—Wireless Sensor Network; Security; Denial of Service Attack; Flooding Attack.

I. INTRODUCTION

Efficient design and implementation of wireless sensor networks (WSN) has become a hot area of research in recent years, due to the vast potential of sensor networks to enable applications that connect the physical world to the virtual world. By networking large numbers of tiny sensor nodes, it is possible to obtain data about physical phenomena that was difficult or impossible to obtain in more conventional ways. In the coming years, as advances in micro-fabrication technology allow the cost of manufacturing sensor nodes to continue to drop, increasing deployments of wireless sensor networks are expected, with the networks eventually growing to large numbers of nodes (e.g., thousands). Potential applications for such large-scale wireless sensor networks exist in a variety of fields, including medical monitoring [1, 2, 3], environmental monitoring [4, 5], surveillance, home security, military operations, and industrial machine monitoring.

A. Applications of WSN

Following are some of salient areas of applications of WSN:

1) Military Applications

Sensor nodes admit battlefield surveillance, monitoring, and also lets in guiding systems of intelligent missiles and sensing of attack by weapons of mass wipe out.

2) Medical Application

Sensors can be wear by patient which wil highly useful in patient diagnosis and monitoring .Sensor devices will monitor the patient's physiological data such as heart rate, temperature, etc.

3) Environmental Applications

It includes Flood Detection, Precision Agriculture, traffic, Wild fire etc.

4) Industrial Applications

It includes industrial sensing and diagnostics. For example appliances, factory, supply chains etc.

5) Infrastructure Protection Application

It includes power grids monitoring, water distribution monitoring etc. routing of sensor networks is based on connectionless protocols and thus inherently [6]

B. Challenges of WSN

A wireless sensor network is a special network which has many constraint compared to a conventional computer network Security in wireless sensor networks has attracted a lot of attention in the recent years. Majority of resource constraints makes computer security more challenging task for these systems. The various challenges are discussed as follows [6], [7].

1) Limited Memory and Storage Capacity:

Sensor node is a tiny device with very small amount of memory and storage space for the code. It is necessary to limit the code size of the security algorithm in order to develop an effective security mechanism.

2) Unreliable Communication

Certainly, unreliable nature of communication channel is another challenging issue to sensor security. The security of the network depends heavily on a defined protocol, which in turn depends on communication.

3) Unreliable Transmission:

Sensor network follows packet-based routing approach for communication. Hence transmission is connectionless and therefore inherently unreliable.

4) Conflicts:

Although the channel is reliable, the communication may still be unreliable because of congestion of data packets. This is due to the broadcast nature of the wireless sensor network.

5) Unattended Operation

In certain cases, the sensor nodes are not operated and hence are left unattended for long periods of time. There are three main reasons to unattended sensor nodes.

6) Lack of Central Coordinator:

A sensor network should be a distributed network. Each sensor node should operate autonomously with no central point of control in the network. In case if designed inaccurately, it will make the network organization difficult, inefficient, and weak. A sensor node left unattended for longer time is more likely to be compromised by an adversary.

II. DENIAL OF SERVICE ATTACK

A Denial of service attack (DoS) is an explicit attempt to prevent the legitimate user of a service or data. The common method of attack involves overloading the target system with requests, such that it cannot respond to legitimate traffic. As a result, it makes the system or service unavailable for the user. The basic types of attack are: consumption of bandwidth or consumption of processor time, obstructing the communication between two machines, disruption of service to a specific system or person, disruption of routing information, disruption of physical components etc. If the sensor network encounters DoS attacks, the attack gradually reduces the functionality as well as the overall performance of the wireless sensor network. Projected use of sensor networks in sensitive and critical applications makes the prospect of DoS attacks even more alarming. [8]

A. Modes of attacks

The three basic types of attack are:

a. Consumption of limited or scares resources (network bandwidth, memory)

b. Alteration or destruction of configuration information.

c. Physical destruction of network components.

III. GRAY HOLE ATTACK

Gray Hole Attack is one of the network layer attacks. In multi-hop WSN, the nodes send packets to the neighboring nodes thinking that they forward messages to destination faithfully. In Gray Hole attack, a malicious or compromised node legitimately refuses some packets and drops them. A simple form of this attack is when a malicious node acts like a black hole and drops all the packets passing through it. However in such an attack, the nodes can easily detect the attack and can exclude attacker from routing. But, here in selective forwarding attack, malicious nodes selectively drop/forward packet which makes detection of the attack more complicated [9]

Gray Hole attack is an active type of attack in which attacking node first agrees to forward packets and then fails to do so, which leads to dropping of messages. In Gray Hole attack we can't predict the probability of losing data. In Gray Hole Attack a malicious node refuses to forward certain packets and merely drops them. The packets originating from a single IP address or a range of IP addresses selectively drops by attacker and forwards the remaining packets. Gray Hole nodes in MANETs are very dominant. Every node maintains a routing table that stores the next hop node information. When a source node wants to route a packet to the target node, it uses a specific route if such a route is available in its routing table. Otherwise, nodes start a route discovery process by broadcasting Route Request (RREQ) message to its neighbors. On receiving RREQ message, the intermediate nodes update their routing tables for a reverse

route to source node. A Route Reply (RREP) message is sent back to the source node when the RREQ query reaches either the destination node itself or any other node that has a current route to destination [10].

IV. LITERATURE SURVEY

Dharini et al (2015) [11], proposed a detection scheme for detecting flooding attack and gray hole attack. The proposed detection mechanism consumes less energy and also there is not much change in the throughput, packet delivery ratio and delay when compared to ideal hierarchical wireless sensor network scenario. Thus the proposed detection mechanism is light weight in nature, hence proving its efficiency. A light weight energy prediction algorithm is implemented to observe the abnormality of the nodes' behavior. Prediction accuracy obtained is quite high thereby the detection accuracy is also achieved. The proposed detection scheme will increase the detection ratio thereby achieving energy saving. By effectively detecting and isolating the intruders from the network, the network's lifetime is also enhanced.

Vikash Kumar et al (2014) [12], devised a few security prerequisites for Wireless Sensor Network. Further, as security being key to the acknowledgment and utilization of sensor systems for some applications; it has made a depth threat examination of Wireless Sensor Network. Further proposed some security components against these threat in Wireless Sensor Network.

Venkatraman et al (2013) [13], studied that a Group communications alludes to either point - to multi point (In which a packet is conveyed from a group member to alternate individuals) or multipoint-to multipoint communication (in which packet are sent from different individuals to different individuals concurrently). The attributes of distinctive wireless network - wireless infrastructure networks (WINs), ad-hoc networks (AHNs), and wireless sensor networks (WSNs) - are enormously diverse as far as group administration, packet sorts, and resources.

DeepaliA Lokare et al [14] slight changes are introduced in the AODV protocol and a novel algorithm Credit Based AODV (CBAODV), where a value known as credit value is assigned to every node for its neighbouring nodes. The value is incremented whenever a request packet (RREQ) is received and decrement on receiving the reply packet. Nodes detect the presence of gray hole whenever they encounters a negative value by one of its neighbours and discards all the present routes that are established by the suspicious nodes for its table.

Hizbullah Khattak et al [15], presented a solution for avoiding the occurrence of black and gray hole attacks. For this they eliminate the first encountered path and select the second minimal route for communication. Whenever source node receives the reply messages from various nodes that are connected with destination, it simply discards the first reply message arriving from any intermediate node that is connected with destination for the avoidance of the attacks.

V. PROBLEM STATEMENT

Existing work based on only energy consumption and cluster head selection scheme, each time when we change cluster head and transfer routing table in this procedure memory consumption high and increase memory overhead which is drawback of wireless sensor network in on the basis on energy consumption we cannot declare any node as a malicious.

VI. PROPOSED WORK

There is lots of limitation in sensor network like energy consumption and memory storage. Wireless sensor network deploy in many application widely, energy is more concerning area of sensor network. Because of flexibility of sensor network, it easily affected by attack. To design a solution that gives a best result and save energy and solution is very light weighted, especially for the denial of service (DoS) attack. Normally, the adversary's compromise sensors and launch the DoS attack by replaying redundant messages or making overdose of fake messages, problem in exiting work is based on only energy consumption and cluster head selection scheme, each time when we change cluster head and transfer routing table in this procedure memory consumption high and increase memory overhead which is drawback of wireless sensor network. On the basis on energy consumption we cannot declare any node as a malicious. In our propose work we elect a zone head on the basis of energy and distance of base station we put base station on the middle of zones.

A. Proposed Algorithm

Step1: initialize the network.

Step2: divide network in zones.

Step3: on the basis of energy and distance of base station we elect a zone head.

Step4: each zone has head of zone.

Step5: in each zone there is second zone head.

Step6: in zone all nodes are in inactive mode only zone head and second zone head are in active mode.

Step7: whenever attacker node behave abnormally head of zone identify miss behavior

Step8: we put base station in middle.

Step9: if zone head behave malicious then base station identify the malicious behavior.

Step10: exit.

VII. SIMULATION AND RESULTS

The simulation is carried out on Network Simulator-2 (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.

Throughput:

Per second transfer of data on bandwidth is known as throughput. The Fig.1 represents a throughput graph between base approach and proposed approach. The throughput of the proposed approach is good than the base approach.

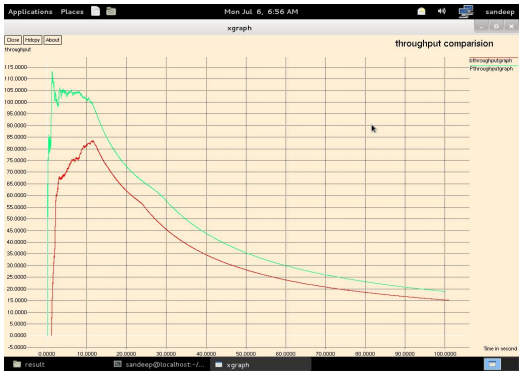


Fig. 1 Throughput graph between Base and Proposed

Packet Delivey Ratio:

Defined as the ratio of packets delivered from source to destination. The Fig.2 represents a PDR graph between base approach and proposed approach. The packet delivery ratio of the proposed approach is good than the base approach.

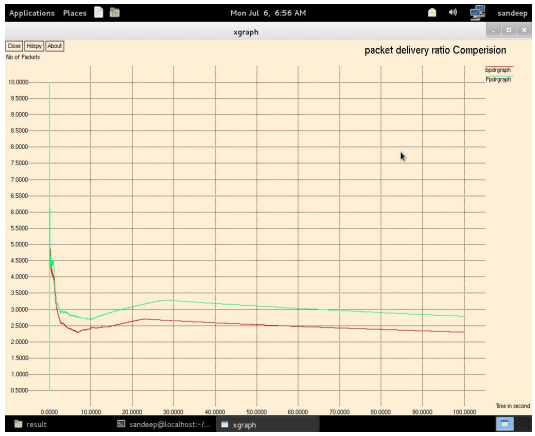
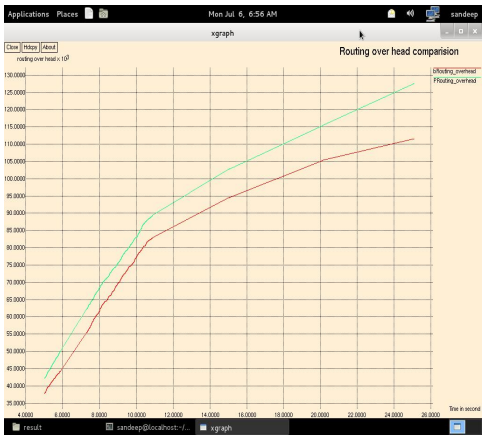


Fig.2 PDR graph between Base and Proposed

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.3 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.



VIII. CONCLUSION

Design or implementation of sensor network is most popular for research now days, energy of node is one of the hot area of research in sensor network because sensor nodes have small life time, because nodes have very small amount of battery power if they work like ad-hoc network it reduce more energy and in our network area number of dead nodes increase or performance of network decrease our proposed method increase network performance.

REFERENCES

[1] C. Kidd et al. The aware home: A living laboratory for ubiquitous computing research. In Proceedings of the Second International Workshop on Cooperative Buildings (CoBuild), 1999.

[2] S. Intille. Designing a home of the future. IEEE Pervasive Computing, 1(2):76–82, April 2002.

[3] L. Schwiebert, S. Gupta, and J.Weinmann. Research challenges in wireless networks of biomedical sensors. In Proceedings of the Seventh Annual International Conference on Mobile Computing and Networking (MobiCom), 2001.

[4] A. Mainwaring, J. Polastre, R. Szewczyk, D. Culler, and J. Anderson. Wireless sensor networks for habitat monitoring. In Proceedings of the ACM International Workshop on Wireless Sensor Networks and Applications (WSNA), 2002.

[5] D. Steere, A. Baptista, D. McNamee, C. Pu, and J. Walpole. Research challenges in environmental observation and forecasting systems. In Proceedings of the Sixth Annual International Conference on Mobile Computing and Networking (MobiCom), 2000.

[6] Vaishali Pahune, Sharda Khode; "Security Issues, Attacks And Challenges In Wireless Sensor Network". International Journal Of Engineering Sciences & Research Technology, 2015

[7] Suraiya Tarannum (2010) "Energy conservation Challenges in Wireless Sensor Networks: A Comprehensive Study", Wireless Sensor Network 2010, Scientific Research, Vol.2 PP. 483-491.

[8] Doddapaneni.krishna Chaitanya, Ghosh.Arindam;" Analysis of Denial-of-Service attacks on Wireless Sensor Networks Using Simulation".

[9] Jaspreet Kaur, Vinod Kumar;" An Effectual Defense Method against Gray Hole Attack in Wireless Sensor Networks". International Journal of Computer Science and Information Technologies, 2012

[10] J. Sen, M. G. Chandra, Harihara S.G., H. Reddy, P. Balamuralidhar "A Mechanism for Detection of Gray Hole Attack in Mobile Ad Hoc Networks" ICICS 2007

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

[12] Vikash Kumar, Anshu Jain,P N Barwal " Wireless Sensor Networks: Security Issues, Challenges and Solutions "International Journal of Information & Computation Technology, Vol. 4, Number 8 (2014), pp. 859-868.

[13] K.Venkatraman, J.Vijay Daniel, G.Murugaboopathi "Various Attacks in Wireless Sensor Network:Survey" International Journal of Soft Computing and Engineering, Vol.3,Issue-1, March 2013

[14] DeepaliA.Lokare,A.M Kanthe,Dina Simunic, "Cooperative Gray Hole Attack Discovery and Elimination using Credit based Technique in WSN", International Journal Of Computer Applications, 2014

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