Analyse and Mitigate Flooding Attacks in Distributed Locations

Medikonda Prathyusha*1, Kaipu Nagarjuna Reddy*2

M.Tech (CS) Student, Department of CS, QISCET, ONGOLE, Dist:Prakasam, AP, India

Assistant Professor, Department of CSE, QISCET, ONGOLE, Dist: Prakasam, AP, India

ABSTRACT:

Wireless sensor network contains different challenges like energy conservation and security. These two challenges are more important for get the reliable and life time solutions. Previously much number of techniques has been proposed for increases the life time and enhances the security purpose. Those approaches are not satisfiable and efficient. In this paper we propose priority based approach. After training of all nodes identify the reputation values. Less reputation value nodes we consider as a attacker nodes. We are not allow whenever to construct the network design. Using this approach minimize the energy spend and delay and increases the throughput and packet delivery ratio.

KEYWORDS: Wireless sensor networks, Priority based approach, energy conservation and security.

I.INTRODUCTION

Wireless sensor networks consist of different number of wireless sensors. Different wireless sensors collect the temperature and physical environment conditions etc. Using wireless sensor networks possible to exchanges the data from source to destination. Network designers are gets the different kinds of security problems. Dos Attackers are create the security issues.

Once dos attacker participate in network we get the problem like drop of packets. Dos attacks are hack the messages in transmission. We use priority based approach to extend the life time of networks and improve the security. Using priority assignment control the number of attackers nodes. We give the priority for high reputation nodes in creation network design. We get the advantages like reduce the delay and consumption of energy levels.

II.RELATED WORK:

Previously much number of techniques has been proposed for increase the life time of networks. One of most popular cluster head routing protocol was introduced here that is called LEACH. Large network divides into number of parts. In each and every part apply one round random the select the cluster head nodes. After perform the different rounds identify the energy balance solutions. This is not efficient approach for transmission of packets.

Next approach is duty cycling. We don’t have the work with node’s, nodes are move to sleeping mode and save the energy levels in our implementation process. This process we perform based on sleep/ wakeup scheduling algorithm. This algorithm also is not providing the robustness solution.

Now here we introduce the robustness approach using data aggregation process. Data aggregation provides using multi paths. These multi paths also are not suitable here in our implementation process. These approaches also are not increases the network lifetime.

Game theory analyzes the all nodes effectively in our network environment. It’s possible to increases the life time of network and save the energy levels. Here some of the decision rules we applies for provide the optimization solution in our implementation.

In total network nodes different categories of nodes are available. First category nodes contain high energy and other category nodes are low energy nodes. Configure the optimal nodes in network construction in our implementation. Using this
decision rules consume the energy levels. It’s not possible to control the attackers.

III. PROBLEM DEFINITION:

Attackers can choose the nodes randomly in network. Attackers are follows different strategies like remove node, packet loss, flood packets etc. Nodes are physically connected this is completely insecure environment. Traditionally many defense techniques are introduced in market. All techniques are inappropriate. Those approaches are theoretical graph and identity management. These are not work practically always. In this paper we propose the rigorous analysis approaches for providing the security. New approaches can introduce the new parameters for detection maximized flooding attacks in exchanges of data packets information. Those new parameters are priority based messages transmission. Using all parameters increases the network throughput and measuring performance content.

IV. PROPOSED METHODOLOGY:

Many schemes are proposed previously against overflow flooding attacks in different kinds of real time applications. Previous approaches control the different attacks like wormhole, selfish drop routing and black hole attacks. We define the some more new attacks in wireless sensor networks. Many number of authentication approaches are used like cryptographic techniques and signature verification concepts for controlling the insider and outsider attackers. In this paper we propose the priority based techniques.

4.1 Priority based Approach:

We form four clusters that are C1, C2, C3, and C4. Every cluster contains one cluster head node that is CH1, CH2, CH3, and CH4, and other sensor nodes are available. Wireless sensor network contains one base station also. In network one of the DDoS attack is present. Now wireless sensor network contains two types of nodes, those are normal nodes and attacker nodes. In wireless sensor network we provide the high priority for normal nodes, attackers nodes contains less priority. Network designers give the priority for normal nodes and construct the network. After construct the network then transfers the data efficiently without any flooding attacker’s disturbances. Here we are not allowed the attacker’s nodes in network design.

![Wireless Sensor Network Scenario](image)

**Fig: Wireless Sensor Network Scenario**

4.2 Priority Assignment

Wireless sensor network compare with game theory. Number of nodes we consider as players. We don’t have awareness about the players. It’s very complex to take the decision for construct the network. First identify the pay off related to each and every node. Filter the highest pay off nodes and construct one matrix. Using this matrix enhance the security and control the all different attacks. Identify the user’s requirement, choose the number of nodes from matrix and start the transmission. In network high priority normal nodes are participates. There is no packets loss of information. All packets are delivering in destination or sink node.

According to requirements choose the different kinds of nodes. Those kinds of nodes are arranged in table.

<table>
<thead>
<tr>
<th>Priority value</th>
<th>Packet status</th>
</tr>
</thead>
<tbody>
<tr>
<td>P1</td>
<td>Most important</td>
</tr>
<tr>
<td>P2</td>
<td>Important</td>
</tr>
<tr>
<td>P3</td>
<td>Medium important</td>
</tr>
<tr>
<td>P4</td>
<td>Less important</td>
</tr>
</tbody>
</table>

4.3 Assigning less priority for attacker nodes

Attacker’s nodes we define based on reputation method. Base station identifies the each
and every node reputation value. Base station contains high reputation values nodes and low reputation value nodes. In network preparation we provide the less priority for low reputation nodes.

4.4 Find out each and every node energy levels and generate the energy report

Identify the energy levels of each and every node and takes the forwarding decisions for transmission of packets. Every time calculate the all nodes energy levels and generate the power status report. Initially all nodes have 100% energy levels. Transmission start nodes energy depletes start.

V. PRIORITY ASSIGNMENT ALGORITHM

Step1. Start.
Step2. Initialize P.
Step3. Switch.
Case1. Find suitable neighbor node for packet forwarding; exit switch.
Case2. Find neighbor node with above 75% energy level; exit switch.
Case3. Find neighbor node with above 50% energy level; exit switch.
Case4. Find neighbor node with above 25% energy level; exit switch.
Step4. Request retransmission of packet from previous node.
Step5. Exit switch.
Step6. End.

VI. RESULTS AND DISCUSSIONS

This chapter present the simulation results of priority based approach when compare with other approaches. In simulation results we consider different parameters. Those parameters are average delay, energy spent, and throughput.

Fig 5.1 Average Delay Graph
VII. CONCLUSION AND FUTURE ENHANCEMENT

Security enhancement is the major challenge in WSN. In this paper we proposed priority based approach. Priority assignment work based on different parameters. Those parameters are each and every node energy and reputation value. Consider the requirement choose the different categories of energy levels. We can provide the less priority for less reputation nodes then improve the security for network. Priority based approach minimize the delay and energy spend and increases the throughput.

In future we increase the lifetime for our wireless sensor networks.

VIII. REFERENCES

[1] Qinghua Li, Wei Gao, Sencun Zhu, Guohong Cao, To Lie or to Comply: Defending against Flood Attacks in Disruption Tolerant Networks, 2013.

Authors Profile:

Name: Medikonda Prathyusha, M.Tech (CS) Student, QIS College of Engineering and Technology, Vengamukkapalem, Ongole, Prakasam, AP, India.

Name: Kaipu Nagarjuna Reddy, Assistant Professor, Department of CSE, QIS College of Engineering and Technology, Vengamukkapalem, Ongole, Dist: Prakasam, AP, India.