International Journal of Engineering and Advanced Technology (IJEAT)
ISSN: 2249-8958 (Online), Volume-8 Issue-5, June 2019

Flooding Attack in Wireless Sensor Network-Analysis and Prevention

Lakshmi HN, Santosh Anand, Somnath Sinha

Abstract*: Wireless sensor network have risen as an essential utilization of the ad-hoc networks model for example, for checking physical condition of an environment. These sensor systems have restrictions of framework assets like battery control, communication range and preparing capacity These sensor systems have restrictions of framework assets like battery control, communication range and preparing capacity. Low handling power and wireless connectivity make such systems helpless against different kinds of system assaults. Due to the limitations of WSN they are susceptible to different types of attack. Denial of service attack (DOS attack) or flooding attack is one of them. In this paper, we are simulating and analysing RREQ flooding DOS attacks. The study is based on a generic NS2-based WSN model. The routing protocol code is changed in the specified WSN simulation model to simulate RREQ Flooding attack.

***Index Terms*: AODV, DOS, Flooding attack, NS2, WSN.**

I. INTRODUCTION

The wireless sensor network involves in huge collection of sensor nodes possess restricted resources of storage capacity and battery. These sensor nodes work independently without human interference in complicated environments [1]. WSN's main concern is to collect all information in a secure environment from the physical world. Mainly due to a densely deployed significant proportion of sensor nodes, neighboring nodes may be very close to each other. Therefore, communication is expected to consume less power in sensor networks than conventional communication. The most crucial obstacle to sensor nodes is the need for lower power. To maintain service quality (QoS), sensor nodes carry limited power sources, which are generally irreplaceable [2]. The main aim for developing WSN technology was to benefit the military organisation for tracking and surveillance with the idea of making a system which is low cost and faster to establish and simultaneously difficult to crash the system.

Flooding attack is a Denial of Service (DoS) type of attack. The vital problem of the flooding attack is that the flooder node is flooding the full network. The flooding attack is where the attacker generates the route request messages and floods the request simply by not even monitoring the routing table for the route. Once the legitimate node receives the RREQ, the nodes in-between in their routing table will attempt to focus on the destination route and eventually flood the request to their respective neighbors as nodes have a route to the destination. The flooding attack's major objective is to take power by consuming a huge amount of battery and network bandwidth. It will ultimately lead to small number of network performance - related issues. Flooding attack results in a breakdown in terms of output, battery power exhaustion and bandwidth inefficiency. AODV routing protocol is vulnerable to malicious attacks due its flexibility (on demand) in route discovery method. Due to the on-demand path discovery nature of AODV, it uses various metrics such as RREQ packets. A malicious node easily changes the contents of these packets to launch the attack. The AODV motivates WSN nodes to quickly acquire routes for new destinations, which do not need nodes to keep routes to non - networked destinations. RREQ message is the message that is sent to sink from the source to connect and send data to sink from the source [3].

II. RELATED WORK

Amin Hassanzadeh, Radu Stoleru and Jianer Chen [1],[17] proposed an efficient flooding with neighborhood keys in WSN secured. The research paper involves checking whether a flooding packet can achieve 100% network coverage when each node clearly selects one of its keys to unicast the message. It results in NP - hard, proposing an application development version of it, and implementing a MAX - SFN approximation algorithm. It exhibits the 100 percent network coverage that can be achieved by flooding packets at low cost through simulations. Ayaz Hassan Moon, Ummer Iqbal, G. Mohiuddin Bhat and Zaffer Iqbal [2],[18] proposed the overall consequences of RREQ flooding attacks on different network performance constrains such as initiated route request packets, energy consumption, buffer overflow, end - to - end delay and throughput was studied. RREQ flooding attack decreases the WSN's performance because it drains the network's restricted resources quickly. Throughout this analysis helps to design relevant mechanisms of security to thwart RREQ flooding attack. Shruti Bhalodiya and Krunal Vaghela [4] proposed a system finding number of devious network nodes and dropping entirely fake packets. This paper provided a flood attack solution using RREQ flood attack. The results of the simulation are accomplished using parameters such as throughput, end-end delay and packet delivery ratio. This solution can be used to recognize and eliminate any number of MANET malicious nodes and to locate a safer route from source to destination by redirecting the malicious nodes. The concern will be on analyzing the attack issue in further protocols in the future. Srividya Shanmugam [5] proposed a protocol for secure routing with preventive measures against known attacks.

Manuscript published on 30 June 2019.
***** Correspondence Author (s)
Lakshmi HN*, Department of Computer Science, Amrita School of Arts & Sciences, Amrita Vishwa Vidyapeetham, Mysuru, India.
Santosh Anand, Department of Computer Science, Amrita School of Arts & Sciences, Amrita Vishwa Vidyapeetham, Mysuru, India.
Somnath Sinha, Department of Computer Science, Amrita School of Arts & Sciences, Amrita Vishwa Vidyapeetham, Mysuru, India.

This paper includes a study on routing attacks in wireless sensor network, attributes of routing protocol and secure sensor network routing protocol. The protocol is implemented on the testbed of telos motes in TinyOS environment, the performance result is found to be in acceptable limits compared to the level of safety achieved.
Alok Ranjan Prusty [6],[16] proposed few interesting concepts and explains the concepts of wireless sensor networks, challenges, different security threats, network attacks, classification of attacks and countermeasures. This will generate interest in imagining new ideas for a reliable, robust and safer wireless sensor network among future researchers. Poonam Rolla, Manpreet Kaur, and Jabarweer Singh [7] proposed a review on several techniques for protecting DDoS attack. It is carried out by a brief explanation about the wireless sensor network and DDOS attack. Various prevention techniques for DoS attack are reviewed and a comparative analysis of different techniques tabularly designed. Yi Ping, Hou Ya fei, Bong Yiping ‘, Zhang Shiyong’, and Dui Zhoulin ‘[8**]** proposed the flooding Attack of ad hoc routing protocols on demand. The detailed view of ad-hoc flood attack and AODV routing protocols has been elaborated. There is a tabulated comparison of Ad hoc Flooding Attack and SYN Flooding Attack. In order to resist this attack, Flooding Attack Prevention (FAP) is designed to develop an algorithm using a neighbor suppression method. The results of the implementation show that the FAP is effectively defending the Ad hoc Flooding Attack with a slight overload. Neetu Singh Chouhan and Shweta Yadav [9] proposed effective way to identify and prevent the flooding attack. The efficient way of using AODV protocol to prevent flooding attack is analyzed. In order to combine efficient secure routing algorithms into the network, MANETs requires a brief understanding and structuring of the security attacks. An algorithm is developed for RREQ flooding attack. Further this study can be enhanced optimizing value of threshold and improving their performance. Shishir K. Shandilya and Sunita Sahu [10] proposed a distributive approach for detecting and preventing RREQ flooding. The effectiveness depends on the threshold values being selected. Together with the trust estimation function, the DSR routing protocol is used. The delay queue approach minimizes the node's chance of accidental blacklisting, But the detection of malicious nodes is also delayed by permitting them to forward more packets once slowdown queue time - out arises. Jeffery Undercoffer, Sasikanth Avancha, Anupam Joshi and John Pinkston [11] proposed a new method which defines perimeter protection as a sensor network application class. To identify threats to this application class, a security protocol that works in the sensor communication mode of the base station is identified and put in place. This is simulated applying SensorSim, and the results indicate that the protocol is practical and acceptable for class of implementation. Shikha Jindal and Raman Maini [12] proposed a study on two major attacks flooding and jamming. The types of the respective attack and how they affect the sensor network, some defense mechanism to prevent flooding attack is explained. The analysis is performed by comparing flooding and jamming attack, it is more difficult to detect jamming attacks compared to flooding attacks since jam attacks are targeted in a specific region or area. Parth C. Bhatiya and Hitesh M. Barot [13] proposed various intrusion detection techniques in MANET. Which helped to suggest a method for identifying MANET flood attack. Detection scheme such as router data structure, statistical packet flow and artificial intelligence (fuzzy logic and neural network) are used to detecting flooding attack. This leads to a better understanding and structuring of security attacks. Ankur Ashok Acharya, Arpitha K.M and Santhosh Kumar B.J [14] Proposed a system for detecting UDP floods and ping of death in MANET which leads to the channel congestion and denial of service. A system called intrusion detection is used here to monitor the malicious activities or violations in the network. The intrusion detection system will recognize the kind of packets and flow of the packets in the node, if it is more than the set threshold then it will recognize the source node which caused the flood attack or the ping of death attack and will notify about the attack. Santosh Anand and Akarsha RR [15] proposed a protocol-based study to use energy efficiently in the wireless sensor network. The system has three phases that upgrade WSN's lifetime such as path creation, optimization and sleeping technique with the maximum energy utilization of each unnecessary node in the network. Multi - hop and multi - path systems are implemented, in which all nodes will participate successfully in communication to enhance the lifespan, help reduce overhead and increase the WSN performance.

III. SIMULATION

Simulation of flooding attack is implemented on a Network simulator (version 2.35) is popularly referred to NS2. This is clearly an event – driven tool that has claimed to be functional in the study of communication networks of the dynamic type. The flooding attack is implemented where the attacker generates RREQ message and clearly floods the request leading to flooding attack. Once the legitimate node receives the RREQ, the nodes in-between will attempt to focus on the route for the destination in the routing table accordingly and eventually floods the request to their corresponding neighbours as none of the nodes have a route to the specific destination. For some time, the attacker awaits to control the rate of flooding occurrence in the network and restarts the flooding. During the simulation, the flood intervals are changed. Simulation scenario of flooding attack in NS2 is represented in the following figure 1.

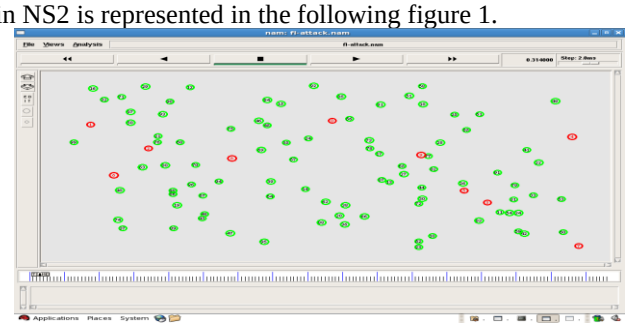

Fig. 1: Simulation scenario in NS2

Fig. 1. Indicates the simulation scenario in NS2 with 100 nodes and 10 malicious nodes with random distribution.

Table 1. Simulation Parameters

Parameters	Values
NS2	Versions 2.35
Simulation area	1000x500 (sq. m)
Simulation time	60,70,80,90,100sec
Mac Layer	802.11
Routing protocol	AODV
No of Nodes	100,120,140,160,180,200
Malicious Nodes	1-10

The system performance parameters have been observed in two scenarios like throughput and end-end delay.

a) Throughput: Network throughput is the amount of data successfully progressed over a specified time period from one position to another and typically calculated in kilobits per second (kbps), or megabits per second (Mbps)

b) End-end delay: It deals with the time taken to transmit a packet from source to destination across a network and is measured in milliseconds (ms).

The flooding attack is carried out by taking minimum of hundred nodes and maximum of two hundred nodes with the difference of twenty nodes (i.e. 100,120,140,160,180,200). The parameters are calculated by differing the node numbers, number of attackers (i.e. 0-10) and simulation time (i.e. 60-100sec) accordingly.

IV. Results and Analysis

The flooding attack takes place in a WSN environment, the arrangement of the nodes is completely random in nature, because of the varying node positions, the results may vary accordingly while increasing the no. of nodes and simulation time i.e. the distance between two nodes the source and sink may be far or near while the flooding attack is taken place. In figure 10, the end-end delay increases as the no. of attackers are increased. In figure 11, the throughput becomes zero when the no. of attackers is increased by 3, 4 and so on. Hence, the resultant of the throughput and end-end delay might fluctuate by increasing or decreasing its value. All the results are collected and represented in a graph for its analysis. End to end delay with number of nodes in absence of attacker and with the attacker is describe below (Fig. 2 and Fig. 3). Clearly increase of delay occurs in presence of attacker.

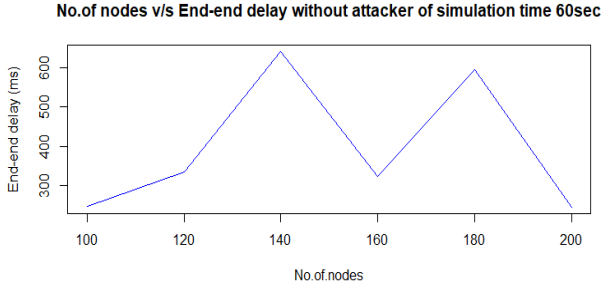

Fig. 2. No. of nodes v/s End-end delay without attacker.

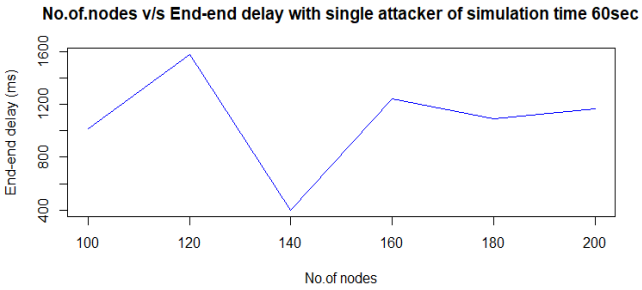

Fig. 3. No. of nodes v/s End- end delay with single attacker.

Throughput with number of nodes are presented below (Fig. 4 and Fig. 5). The result is not consistent because of taking random arrangement of the nodes. But the throughput become almost zero when the attacker comes into scenario.

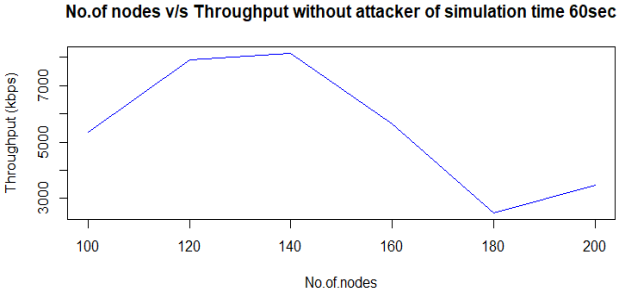

Fig. 4. No. of nodes v/s Throughput without attacker.

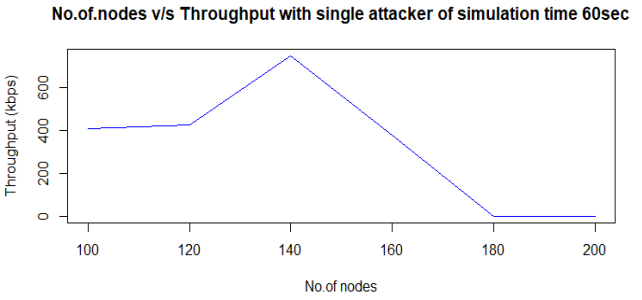

Fig. 5. No. of nodes v/s Throughput with single attacker.

Also, to check the effect of flooding attack we considered the variation of end to end delay and throughput by varying the time of simulation (from Fig. 6 to Fig 9). Delay become higher and throughput become almost zero in presence of attacker.

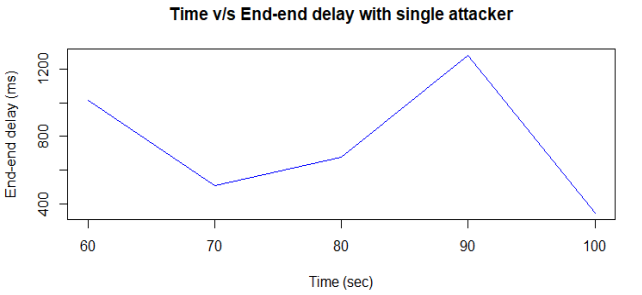

Fig. 6. Time v/s End-end delay with single attacker.

Published By:
Blue Eyes Intelligence Engineering
& Sciences Publication (BEIESP)

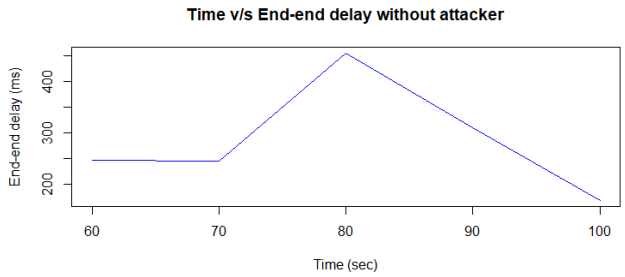

Fig. 7. Time v/s End-end delay without attacker.

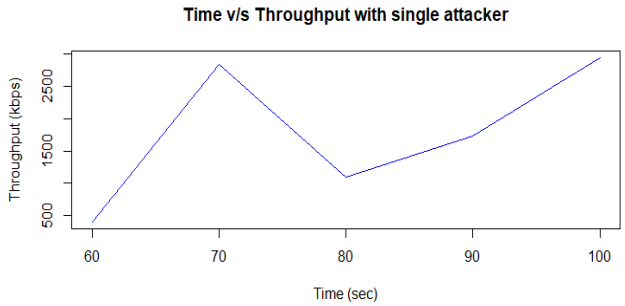

Fig. 8. Time v/s Throughput with single attacker.

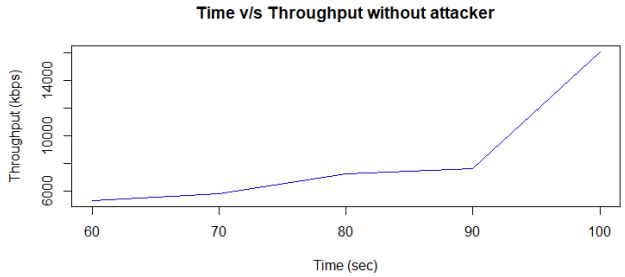

Fig. 9. Time v/s Throughput without attacker.

The effect of number of attackers on the simulation is represented (from Fig. 10 to Fig. 11) which shows increasing of delay and reduce of throughput during simulation.

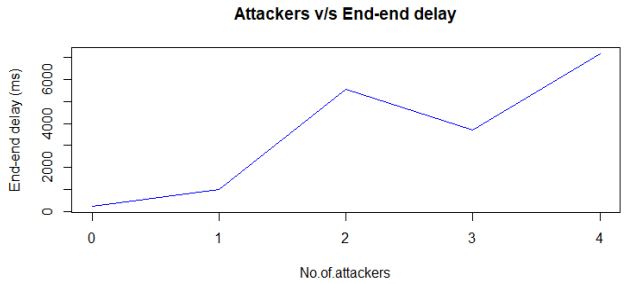

Fig. 10. No. of attacker's v/s End-end delay.

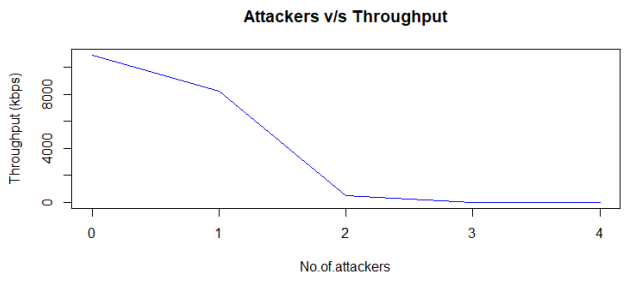

Fig. 11. No. of attacker's v/s Throughput.

V. METHODOLOGY

The main reason behind this severe attack in WSN is flooding of RREQ packet. Directly or indirectly the attacker or any compromised node unnecessarily floods RREQ packets to create congestion in the network. To prevent the attack the only way is to limit the flooding of this packet. We consider one limit or threshold value for each node that can be sending over a particular time span beyond which legitimate node cannot send the route request packet. The surroundings or neighboring nodes are used to count the RREQ response from any node. If the response goes above the threshold limit immediately the node is blacklisted. From the neighboring nodes the information is shared to the other nodes and the node is identified as malicious node and left out from the network.

VI. CONCLUSION AND FUTURE WORK

In this paper we have discussed on flooding attack in wireless sensor network. Also, we present through this paper how this attack can be created and the effects of this harmful attack in the network. We used NS2 for simulation of this attack. We considered random arrangement of the nodes to study the real effect of this attack. The effect of this attack on throughput and end to end delay is represented graphically which reveals the direct effect of flooding attack. The analysis of the graphical representation is helpful for detection of RREQ flooding attack in WSN. In this paper we also proposed a prevention method against this harmful attack. In future the authors will implement the prevention mechanism and study the effectiveness of this method by comparing with the other.

REFERENCES

1. Hassanzadeh, A., Stoleru, R., & Chen, J. (2011, October). Efficient flooding in wireless sensor networks secured with neighborhood keys. *IEEE Intelligent Systems* (pp. 119-126).
2. Moon, A. H., Iqbal, U., Bhat, G. M., & Iqbal, Z. (2016, March). Simulation and analysing RREQ flooding attack in Wireless Sensor Networks. *In Electrical, Electronics, and Optimization Techniques (ICEEOT), International Conference on* (pp. 3374-3377).
3. Pandikumar, T., & Desta, H. (2017, June). RREQ flooding attack mitigation in MANET using dynamic profile based technique. *International Journal of Engineering Science*, 12700.
4. Bhalodiya, S., & Vaghela, K. (2015, September). Enhanced Detection and Recovery from Flooding Attack in MANETs using AODV Routing Protocol. *International Journal of Computer Applications*, Vol. 125, No. 4.
5. Shanmugham, S. (2009, March). Secure Routing in Wireless Sensor Networks. *MS EE Scholarly Paper Spring*.
6. Prusty, A. R. (2012). The Network and Security Analysis for Wireless Sensor Network: A Survey. *International Journal of Computer Science and Information Technologies (IJCSIT)*, Vol.3, No. 3, 2012.
7. Rolla, P., & Kaur, M. (2016, June). Dynamic Forwarding Window Technique against DoS Attack in WSN. International Conference on Micro-Electronics and Telecommunication Engineering (ICMETE), Vol. 6, Issue 6.
8. Ping, Y., Yafei, H., Yiping, Z., Shiyong, Z., & Zhoulin, D. (2006). Flooding attack and defence in ad hoc networks. *Journal of Systems Engineering and Electronics*, Vol. 17, No. 2.
9. Chouhan, N. S., & Yadav, S. (2011). Flooding attacks prevention in MANET. *International Journal of Computer Technology and Electronics Engineering*, Vol. 1, Issue 3.

Published By:
Blue Eyes Intelligence Engineering
& Sciences Publication (BEIESP)

10. Shandilya, S. K., & Sahu, S. (2010, August). A trust based security scheme for RREQ flooding attack in MANET. *International Journal of Computer Applications*, Vol. 5, No. 12.
11. Undercoffer, J., Avancha, S., Joshi, A., & Pinkston, J. (2002, October). Security for sensor networks. *CADIP Research Symposium* (pp. 25-26).
12. Jindal, S., Maini, R. (2014, April). Comparative Analysis of Flooding and Jamming Attacks in Wireless Sensor Networks. *International journal of engineering research & technology (ijert)*, Vol. 03, Issue 04.
13. Bhatiya, P. C., Barot, H. M. (2013). Review of Flooding Attack Detection in AODV protocol For Mobile Ad-hoc Network. *International Journal for Scientific Research & Development (IJSRD)*, Vol. 1, Issue 3, 2013.
14. Acharya, A. A., Arpitha, K. M., & Santhosh Kumar, B. J. (2016). An intrusion detection system against UDP flood attack and ping of death attack (DDOS) in MANET. *International Journal of Engineering and Technology (IJET)*, Vol. 8, No. 2.
15. Anand, S., Akarsha, R. R. (2018). A, Protocol for the Utilization of Energy in Wireless Sensor Network. *International Journal of Engineering & Technology*, 7(3.3).
16. Y. Wang, G. Attebury, and B. Ramamurthy (2006). A Survey of Security Issues in Wireless Sensor Networks. *IEEE Commun. Surveys Tutorials*, vol. 8, pp. 2–23.
17. A. Perrig, J. Stankovic, and D. Wagner (2004, June). Security in wireless sensor networks. *Commun. ACM*, vol. 47, pp. 53–57.
18. Varsha Sahni, Pankaj Sharma, Jaspreet Kaur, Sohajdeep Singh (2012). Scenario Based Analysis of AODV and DSR Protocols Under Mobility in Wireless Sensor Networks .*2012 International Conference on Advances in Mobile Network, Communication and Its Applications*.

AUTHORS PROFILE

Lakshmi HN a student of Amrita school of arts and sciences, Mysuru. She has completed her BCA at Amrita Vishwa Vidyapeetham University, Mysuru and is currently pursuing her Masters in Computer Applications. Her area of research is Security and Wireless Sensor Network

Mr. Santosh Anand Assistant Professor, Department of Computer Science in Amrita school of arts and sciences, Mysuru. He has pursued his BE and MTech, His area of research is Cognitive Radia and Wireless Sensor Network.

Dr. Somnath Sinha Assistant Professor, Department of Computer Science in Amrita school of arts and sciences, Mysuru. He completed his PhD in Computer Science from Pacific University, Udaipur, India. He also completed his Master's in Computer Application in IIEST, West Bengal, India. His area of research is Artificial Intelligence, Wireless Sensor Network & Computer Graphics