International Journal of Recent Technology and Engineering (IJRTE)
ISSN: 2277-3878, Volume-8 Issue-4, November 2019

Pro-Active and Pre-Emptive Intelligent Network Management Strategies in Internet of Things

Majidha Fathima K M

Abstract— Whenever a user browses the internet, the content he sends or receives takes the form a Protocol Data Unit as packets according to the OSI (Open Systems Interconnection) layers. These packets travel from the source to the destination through the path chosen by the routing protocols as OSPF (Open Shortest Path First) and BGP (Border Gateway Protocol). OSPF is used for interior routing within an AS (Autonomous System) and BGP is used for exterior routing between two external AS. Some customers are dual-homed where they have connections to two AS with one as the primary and the other one as secondary. Such diversed enormous traffic generated by the end users and the Internet Service Providers (ISP) have to be efficiently managed and monitored for the purpose of billing, security, QoS (Quality of Service) and SLA(Service Level Agreement) parameters. Hence the existing routing algorithms need to provide intelligent routing. The Simple Network Management Protocol (SNMP) generates the corresponding packets called SNMP traps. These specific packets are exchanged between the server and the appropriate interfaces of the routers when they are being polled. This polling technique generates a utilization graph which indicates the incoming and outgoing traffic at the core layer, distribution layer and access layer. The last mile traffic also has to be examined for checking the the bandwidth utilization. The traditional SNMP also has to incorporate the machine learning technique. This paper focuses on implementing intelligent network management in an Internet of Things environment.

Keywords: OSPF (Open Shortest Path First), BGP (Border Gateway Protocol), SNMP (Simple Network Management Protocol), IoT (Internet of Things) , Sensors, Actuators, WAN (Wide Area Networks), Last mile, ISP (Internet Service Provider)

I. INTRODUCTION

rise to smart homes, smart irrigation, smart theft alarm, smart forest fire detection system.

In an internet, the end user connects to the ISP at the area known as last mile. The three types of connection are

- Leased Line
- ISDN (Integrated Services Digital Network)
- Broadband

The leased line at the customer's end device (router) terminates at the ISP's (Internet Service Provider) edge router. ISDN (Integrated Services Digital Network) is the second type of connectivity where the customer's device connects to the ISP's end. The difference here is that the router configuration has a dialer string. Only on demand basis, this string is dialed and the network connection establishes. In a broadband network (wireless), there is an AP (Access Point) at the ISP's end. The corresponding SU (Subscriber Unit) at the customer's end talks to the AP. The AP which serves SUs in the appropriate coverage area forwards the traffic to the base station router at the ISPs end. One or more APs can be connected a base station router (BS). The BS forwards the traffic to the aggregation router which takes the traffic to the backbone router.

The monitoring of a network includes monitoring of all these devices. They are

- End user's PC,
- Router
- Edge router (ISP)
- AP
- SU
- BST
- Aggragation router
- Backbone router

SNMP (Simple Network Management protocol) manages and monitors a network by a process called polling. The SNMP walk starts from the polling end (server) to the appropriate network device (switch, router, firewall).

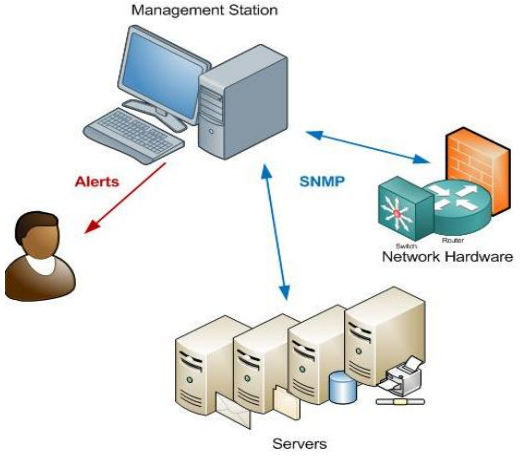

Fig. 1. Network Monitoring with SNMP

As shown in figure 1, the network administrator monitors the traffic between the network devices. The bandwidth utilization graph generated by SNMP is shown in figure 2.

Manuscript published on November 30, 2019.
* Correspondence Author
Majidha Fathima K M*, Assistant Professor,Department of Computer Science and EngineeringSri Krishna College of Engineering and Technology,Coimbatore.,TamilNadu,India.(Email:majidhafathimakm@skcet.ac.in)

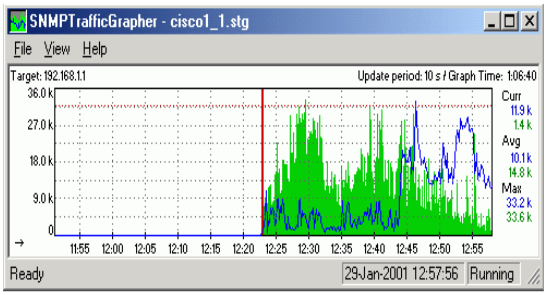

Fig. 2. Bandwidth Utilization Graph

As per figure 2, the bandwidth consumption of the network links are shown at various time intervals. This SNMP can be made to behave in an intelligent manner by using the decision tree learning algorithm. We can train the system for a set of known inputs. Then the knowledge base reverts to us the classification for the set of new unknown inputs. The Multi Router Traffic Grapher (MRTG) is gratuitous software for monitoring and quantifying the traffic load on network links. It sanctions the utilizer to optically discern traffic load on a network over time in graphical form. The routing protocols at the ISPs backbone such as OSPF, BGP can also be incorporated with the decision tree learning algorithm. This phenomenon can be applied at the network portion in an Internet of Things environment.

II. LITERATURE REVIEW

Francesco Colace et al [1] states that a SINMS (Slow Intelligence Network Manager can be built based on SNMP protocol). It is a ontology based network management.

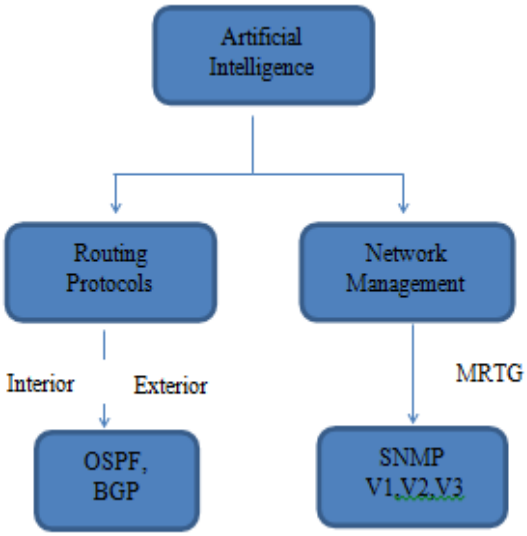

Fig. 3. Organization of the paper

As per Deepak K Sharma et al [2], to determine the probability of successful deliveries, a novel routing protocol for opportunistic networks is proposed. This uses machine learning algorithms namely decision trees and neural networks. Mallikarjun Talwar [3] quotes pros and cons of the mechanisms such as Pro-active versus Reactive, Hop-by-hop versus Source based routing and Information Centric. Approaches like Enery-Aware Routing, Multipath Routing, Probabilistic Routing are compared. Himadri Nath Saha et al [4] discusses the issues in Adhoc networks and proposes intelligent routing mechanisms using Ant Colony Optimization, Bee Colony Optimization and Termite Hill Building Technique. Purneshwari Varshni elaborates that Ant Colony Optimization is well-liked among other Swarm Intelligent Techniques. In this paper, routing protocols for MANETs are analyzed. This paper also introduces the preliminary studies for Mobile Ad Hoc Networks.

III. ROUTING IN PEER NETWORKS

A. Network Configuration

The end user devices are connected to the ISP in the last mile phenomenon. The devices will communicate only with IP (Internet Protocol) addresses in the internet. As per figure 4, the host 1, host 2 and host 3 are configured with private Ip addresses as 10.0.0.11/24, 10.0.0.12/24 and 10.0.0.13/24 respectively. As the private ip addresses are not visible in the network, a NAT (Network Address Translation) is performed at the gateway router. The communication outside has the translated public address as 192.168.1.2.

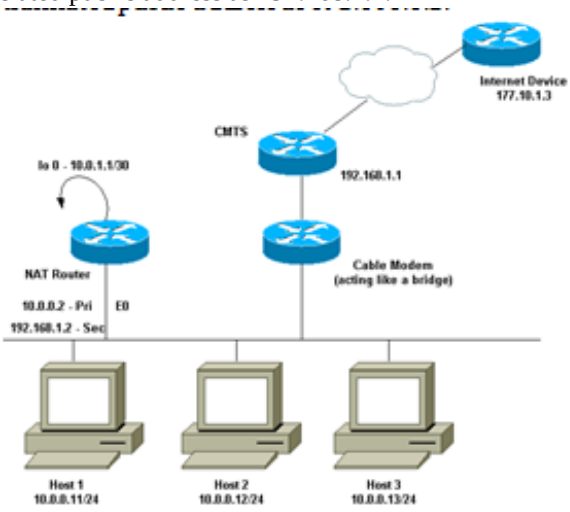

Fig. 4. Last Mile Connectivity

B. Autonomous Systems

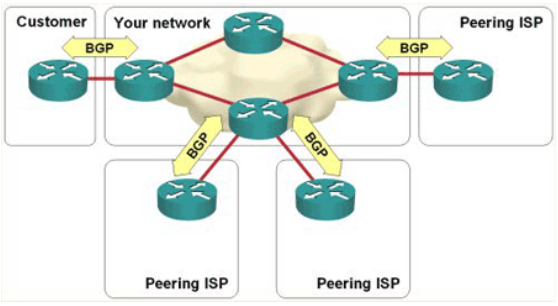

Fig. 5. Inter AS Communication

The network traffic progresses from the last mile towards the core backbone routers. The individual ISPs so called Autonomous Systems identify their corresponding traffic in the internet via AS numbers. Every AS has a neighbouring peer network with which it exxhanges the forward and reverse traffic. BGP is the protocol of the internet which runs between the peer network gateway routers as shown in figure 5.

C. BGP – Path Selection

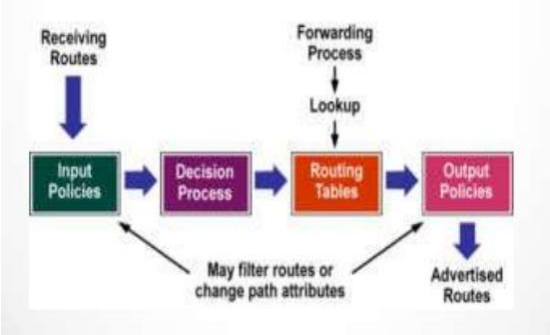

Fig. 6. Steps in BGP Route Selection

In the internet, the routes are received at the gateway routers of the corresponding ISP. They are again redistributed within the ISP with the help of interior routing protocol OSPF. In figure 6, hence the intelligent machine learning algorithm has to be incorporated before the routes are given to OSPF.

D. Layers of the Network

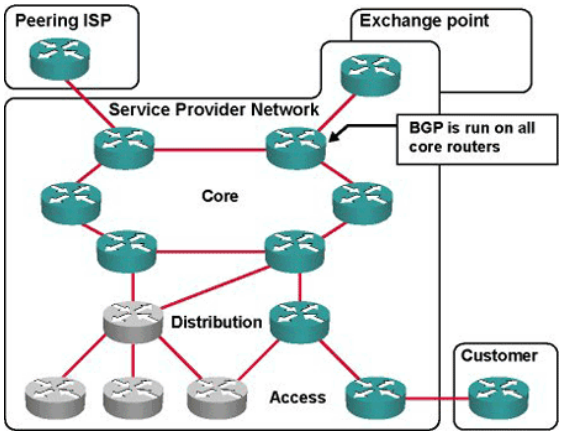

Fig. 7. Layered Communication

The network is distributed into three layers namely Access, Distribution and Core layer. The customer lands on the access layer i.e the last mile connects to access layer. The traffic is brought forward to the distribution layers which includes base station and aggregation routers. This traffic is further propagated towards the interior backbone routers identified as the core layer as shown in figure 7

E. MPLS VPN

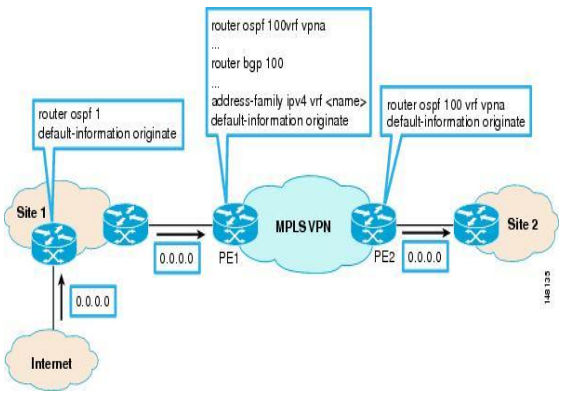

Fig. 8. MPLS Virtual Private Network

After the routes are received at the gateway routers in the peer networks they are redistributed inside the AS as shown in figure 8. While BGP is the exterior routing protocol, OSPF is the interior routing protocol. BGP routes are redistributed i.e identifying the destination within an AS. As per our system, the backbone routers are MPLS (Multi Protocol Label Switching) enabled. VRF (Virtual Routing and Forwarding) routes are aggregated and traversed across the MPLS network as individual traffic. MPLS injects and removes the labels at the PE (Provider Edge) routers at the entry and exit respectively. The label switching of VRF traffic is implemented.

F. Multihomed AS

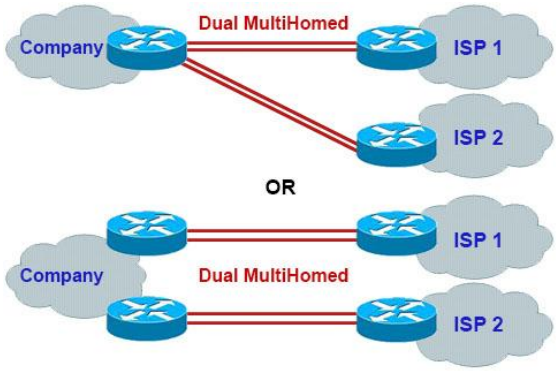

Fig. 9. Multihomed User

This is another scenario in the BGP community where one user can be connected to more than one ISP. The purpose is to have one connection as primary and the other as secondary. When the primary link fails, the traffic automatically switches to the secondary to avoid service outage as shown in figure 9.

IV. SNMP NETWORK MONITORING AND MANAGEMENT

A. SNMP Community

```
snmp-server community 14all4$$ RO 30
snmp-server community gds4chv1 RW 10
snmp-server community mrtg RO 1300
snmp-server community VBCCrep0rting RO 1333
snmp-server ifindex persist
snmp-server trap-source Loopback0
snmp-server location THHQCE1-3845: Facility-Code THHQ
snmp-server contact network operations 66-6428 xxxx
snmp-server enable traps tty
snmp-server enable traps config
snmp-server host 172.22.71.201 Voyence  config
snmp-server host 172.22.71.201 config
snmp-server host 172.22.9.201 config
!<----- SNMP SETTINGS
!<----- ACL 10 for Read Write, ACL 30 for Read Only
!
! ACL 10 – SNMP READ WRITE
!
no access-list 10
access-list 10 permit 172.27.124.18 log
access-list 10 deny any log
!
!
! ACL 30 – SNMP READ ONLY
!
no access-list 30
access-list 30 permit 172.40.46.89 log
access-list 30 permit 172.40.46.114 log
access-list 30 deny any log
!
```

Fig. 10. SNMP Configuration

As shown in figure 10, the individual devices and hosts are polled using SNMP. The communication establishment is called a SNMP walk which runs from the server to the network device. The SNMP server ip address is 172.22.71.201 and the hosts are 172.40.46.89 and 172.40.46.114. The individual ACL (Access Control List) are created for every SNMP walk identified by the appropriate community string.

B. Communication between an SNMP Agent and Manager

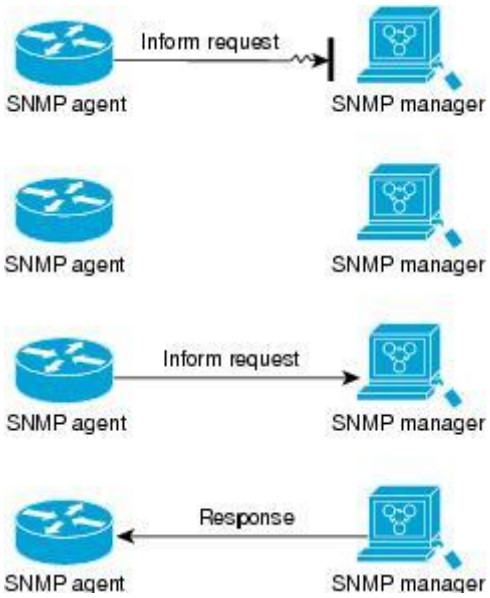

Fig. 11. SNMP Communication

The SNMP agent communicates with the SNMP manager The MIB (Management Information Base) values are got and set with the SNMP manager.

TABLE I. SNMP OPERATION

The values of a table are

- Gets the value for a variable
- Gets the value for next row
- Gets the huge amount of values
- Receives the response for a request
- Stores the value for a variable
- Unexpected messages are being captured

Operation	Description
get-request	Retrieves a value from a specific variable.
get-next-request	Retrieves a value from a variable within a table.
get-bulk-request	Retrieves large blocks of data, such as multiple rows in a table, that would otherwise require the transmission of many small blocks of data.
get-response	Replies to a get-request, get-next-request, and set-request sent by an NMS.
set-request	Stores a value in a specific variable
Trap	An unsolicited message sent by an SNMP agent to an SNMP manager when some event has occurred.

The responses and the SNMP traps are sent to the MIB SNMP agent as per figure 11. Table 1 shows the various SNMP operations. The network management here becomes pro-active i.e detects failures prior and pre-emptive i.e alternate paths are available and switches incase of failure.

C. SNMP V3 Features

SNMPv3: Version 3 of the SNMP is an interoperable standards-based protocol defined in RFCs 2273 to 2275. SNMPv3 provides secure access to devices by authenticating and encrypting packets over the network and includes these security features:

- Message integrity: The packet needs to reach the destination unaltered.
- Authentication: Ensuring only permitted sources can access the network.
- Encryption: The messages are converted into a different form so that authorized users only can access.

D. SNMP Configuration

The SNMP group of devices are identified by the community string. The three hosts that are being polled are 192.180.1.27, 192.180.1.111, 192.180.1.33. The community strings are specified as shown in figure 12. The messages are labelled as traps. The authentication type is MD5. The password is also set for the respective users. The entries are also restricted.

```
Switch(config)# snmp-server community public
Switch(config)# snmp-server community public
Switch(config)# snmp-server enable traps vtp
Switch(config)# snmp-server host 192.180.1.27 version 2c public
Switch(config)# snmp-server host 192.180.1.111 version 1 public
Switch(config)# snmp-server host 192.180.1.33 public
Switch(config)# snmp-server community comaccess ro 4
Switch(config)# snmp-server enable traps snmp authentication
Switch(config)# snmp-server host cisco.com version 2c public
Switch(config)# snmp-server enable traps entity
Switch(config)# snmp-server host cisco.com restricted entity
Switch(config)# snmp-server enable traps
Switch(config)# snmp-server host myhost.cisco.com public
Switch(config)# snmp-server engineID remote 192.180.1.27 00000063000100a1c0b4011b
Switch(config)# snmp-server group authgroup v3 auth
Switch(config)# snmp-server user authuser authgroup remote 192.180.1.27 v3 auth md5 mypassword
Switch(config)# snmp-server user authuser authgroup v3 auth md5 mypassword
Switch(config)# snmp-server host 192.180.1.27 informs version 3 auth authuser config
Switch(config)# snmp-server enable traps
Switch(config)# snmp-server inform retries 0
```

Fig. 12. SNMP Community

V. BEST EFFORT DELIVERY

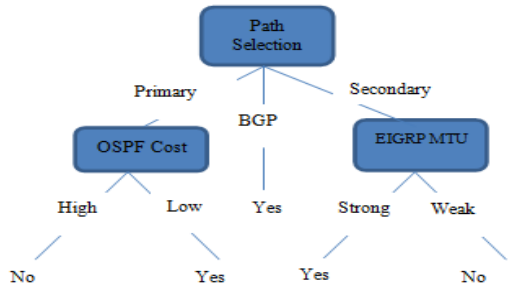

Fig. 13. Path Selection

As per figure 13, the decision tree is constructed based on the metrics of the routing protocols. The best path is chosen among the alternative ones. The routing metrics for OSPF is cost and bandwidth. The routing metrics for EIGRP are bandwidth, load, delay, reliability and MTU. The primary is OSPF path and when the costs are comparatively low, the path can be chosen. The secondary path is EIGRP. When the MTU (Maximum Transmission Unit) is strong, the path is chosen. Otherwise, it is rejected. The exterior routing is provided by BGP which choses path on the following attributes

- AS Path
- Origin
- Local Preference
- MED (Multi Exit Discriminator)
- Weight

VI. INTELLIGENT AGENT & RESULTS

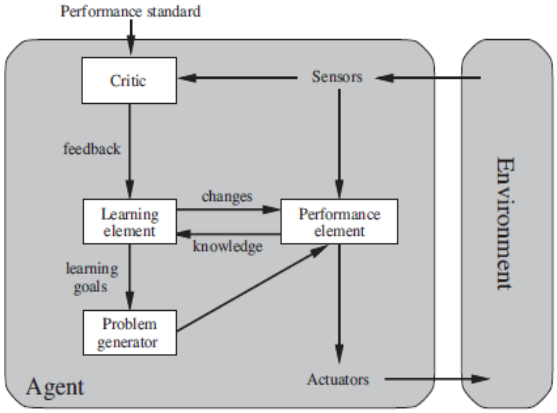

Fig. 14. A general learning agent

The Intelligent Agent shown in figure 14, receives input from the environment through sensors, processes with the routing algorithm and gives output to the environment through actuators.

- Sensors: Multiple Paths (provided by routers)
- Environment: Internet of Things
- Actuators: Best Path (provided by routers)

The problem solving performance is measured by the following features:

- Completeness
- Optimality
- Time Complexity
- Space Complexity

VII. DECISION TREE ALGORITHM

function DECISION-TREE-LEARNING (*examples*,*attributes*,*parent_examples*) **returns** a tree

If *examples* is empty **then return** PLURALITY-VALUE(*parent_examples*)

else if all *examples* have the same classification **then return** the classification

else if *attributes* is empty **then return** PLURALITY-VALUE(*examples*)

else

A<-argmax$_{a \in attributes}$ IMPORTANCE(a,*examples*)

tree<-a new decision tree with root test A

for each value v_k of *A* do

exs<-{*e: e* ∈ *examples* and *e.A* = v_k}

subtree<-DECISION-TREE-LEARNING(*exs*,*attributes-A*,*examples*)

add a branch to *tree* with label (A = v_k)

and subtree *subtree*

return *tree*

Fig. 14. Decision Tree

As per the algorithm in figure 14, the decision tree is constructed with parent and child nodes. The attributes are the routing metrics like bandwidth, delay, cost, delay and MTU. When the router is introduced into the network and the routes are explored, the branches to the tree are added. If an existing route fails, the branch is deleted and a new branch is constructed as per the alternative path.

VIII. NEURAL NETWORK

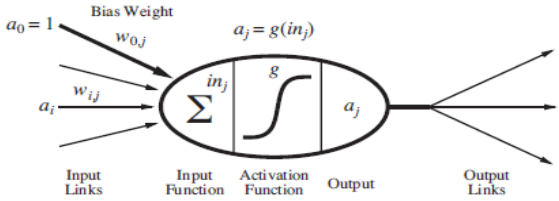

Fig. 16. Mapping with Neural Network

As shown in figure 16, the routing parameters are mapped with the neural network features. The multiple paths available in a network are the input links. Input function is the routing algorithms. The activation function is the QoS function which prioritizes the parameters like bandwidth, delay, jitter and packet loss. The ouput is the best path chosen. The divergent output links are the load balancing paths across multiple routers decided by the Sigmoid function

REFERENCES

1. Https://People.Cs.Pitt.Edu/~Chang/265/Proj10/56colace.Pdf
2. Francesco Colace1, Shi-Kuo Chang2 And Massimo De Santo1 ,"Sinms: A Slow Intelligence Network Manager Based On Snmp Protocol",2017
3. Deepak k.sharma, "a machine learning-based protocol for efficient routing in opportunistic networks", ieee systems journal (volume: 12 , issue: 3 , sept. 2018)
4. Mallikarjun talwar , "routing techniques and protocols for internet of things: a survey", proceeding of ncriet-2015 & indian j.sci.res. 12(1):417-423, 2015
5. Himadri Nath Saha ; Aparajita Chattopadhyay ; Debabrata Sarkar , "Review On Intelligent Routing In Manet", 2015 International Conference And Workshop On Computing And Communication (Iemcon)
6. Purneshwari Varshney, Dr. K. L. Sharma, "Intelligent Routing Techniques For Wireless Sensor Networks Using Swarm Intelligence : A Survey", International Journal Of Advance Research In Science And Engineering, Ijarse, Vol. No.4, Special Issue (01), March 2015
7. G. Di Caro, M. Dorigo, "Mobile Agents For Adaptive Routing,Technical Report", Iridia/97-12, Universit´E Libre Debruxelles, Belgium, 1997.
8. J. Baras, H. Mehta, "A Probabilistic Emergent Routing Algorithm For Mobile Ad-Hoc Networks, Wiopt '03: Modeling And Optimization In Mobile", Ad-Hoc, And Wireless Networks, 2003.

9. Rajeshwar Singh, Dharmendra K Singh And Lalan Kumar, "Performance Evaluation Of Aco Based On Demand Routing Algorithm For Mobile Ad Hoc Networks", Internal Journal Engineering Science And Technology(Ijest), Vol.3, Issue 3, Pp. 1809-1815, March 2011.
10. E. Baburaj And V. Vasudevan, "An Intelligent On Demand Multicast Routing Protocol For Manets", Ieee, First International Conference On Emerging Trends In Engineering And Technology, Pp. 214-217, 2008.
11. Mehrjoo, S., Sarrafzadeh, A., Mehrjoo, M., "Swarm Intelligent Compressive Routing In Wireless Sensor Networks", Computational Intelligence, 2014.

AUTHORS PROFILE

Ms.Majidha Fathima K M, has completed ME(CSE); PURSUING Phd; published two scopus indexed papers