ISSN Application No. 2321-6921

Global Journal of Networks and Applications

Volume No. 12

Issue No. 3

September - December 2024

ENRICHED PUBLICATIONS PVT.LTD

JE - 18,Gupta Colony, Khirki Extn,
Malviya Nagar, New Delhi - 110017.
E- Mail: info@enrichedpublication.com
Phone :- +91-8877340707

Global Journal of Networks and Applications

Aims and Scope

Global Journal of Networks and Applications welcomes research contributions, surveys and notes in all areas relating to computer networks and applications thereof. The following list of sample-topics is by no means to be understood as restricting contributions to the topics mentioned:

- New design techniques, interesting or novel applications, components or standards.
- Interface issues including special consideration for handicapped persons.
- Computer graphics, 3-D modeling and virtual reality multi-and hypermedia including electronic publishing and digital libraries.
- Computer networks with tools such as WWW or Hyper wave.
- Emerging standards for internet presentation levels (such as XML) and Internet protocol level, new compression standards for still pictures, movies, audio and vector data, 3-D data and cartographic data.
- Work on metadata and its applications.
- Applications of networked and stand-alone multimedia systems to computer assisted presentations.
- Applications of an educational, transactional and co-operational nature.
- Gateways between databases and security, privacy and societal aspects of network and computer technology.

Global Journal of Networks and Applications

Global Journal of Networks and Applications

(Volume No. 12, Issue No. 3, September - December 2024)

Contents

Performance Evaluation of OSPF, EIGRP and Rip Protocols in Multiprotocol Label Switching

Mudathir A. O. Fagiri[*1], Mohamed H. M. Nerma[*2]

[*] *Sudan University of Science and Technology – College of Engineering – School of Electronics Engineering, Khartoum, SUDAN. Eastern Diems.*

ABSTRACT

Multiprotocol Label Switching (MPLS) is an emerging technology which ensures the reliable delivery of the Internet services with high transmission speed and lower delays. The key feature of MPLS is the Layer 3 VPN service that can provide a secure connection to any enterprise between its sites around the world. GNS3 has been used to build a network topology of internet service provider (ISP) MPLS core network. Moreover, OPNET 17.5 modeler which is network simulation tool software has been used to compare the performance of three different routing protocols; Routing Information Protocol (RIP), Open Shortest Path First (OSPF) and Enhanced Interior Gateway Protocol (EIGRP) in order to show the most suitable routing protocol needed in the small ISP MPLS core network. The results shows that the RIP has the highest time average end- to-end delay which is 0.19µs and the OSPF has the highest network convergence time which is 18.5 Seconds during the first minute of the all simulation period.

Keywords: MPLS, RIP, OSPF, EIGRP, ISP, VPN and Routing Protocols.

1. INTRODUCTION

Now a days Internet is playing a vital role in most of the people's life due to wide variety of applications and services provided on Internet. The increased number of Internet users made the popular services like TVs and telephone use the Internet as a medium to reach their customers. These services are provided by convergence of voice and data communications over single network infrastructure known as Next generations networks (NGN). [1] Providing the real-time applications on Internet is a challenging task for the conventional IP networks as it uses best- effort services which doesn't provide guarantee of services and Traffic Engineering (TE). Moreover IP networks offer minimum predictability of services which is unacceptable for the applications like telephony and multimedia services. [2]

The success of MPLS is undoubtedly a result of the fact that it enables the network to carry all kinds of traffic, ranging from IP traffic to Voice over IP (VoIP) traffic to Layer 2 traffic. MPLS is the means for an IP network to consolidate many networks into one. [3] MPLS can consolidate the ATM, Frame Relay, Voice, and IP networks into one unified network infrastructure, thereby generating a huge cost advantage.

In only a few years, Multi-Protocol Label Switching (MPLS) has evolved from an exotic technology to a mainstream tool used by service providers to create revenue-generating services. [4] There is rapid deployment of MPLS-enabled services and active development of new mechanisms and applications for MPLS in the standards bodies. The aims to describe the fundamental Mechanisms used by MPLS and the main service types that MPLS enables, such as Virtual Private Network (MPLS VPN). [5] MPLS has matured a lot and is a stable technology, seeing many new deployments and new features. Given the fact that MPLS is based on IP, and the Internet is based on IP technology, it seems that the future of MPLS is ensured for quite a while to come. [6]

The main aim of this paper is to investigate the general study of MPLS and then the implementation of MPLS layer 3 VPN which is the main aim of this paper by connecting one company that has two sites interconnected across the common service provider MPLS infrastructure.

- Designing a small (ISP) internet service provider core network topology.
- Implementing (MPLS) multi protocol label switching to the core network.
- Configuring MPLS L3 VPN between two sites using GNS3 simulator.
- Then implementing three different scenarios with three different routing protocols in the MPLS network using OPNET IT GURU simulator.
- Comparing the performance of each routing protocols in the MPLS network using OPNET IT GURU as results.

A simulation study is performed by using GNS3 to demonstrate the topology of the network and the MPLS L3 VPN connectivity between the sites and OPNET IT GURU for routing protocols comparison to get statistical results or data. [7]

In this paper is mainly focused on performance of the real-time MPLS L3 VPN. Simulation is done with a networking simulator called GNS3. The operation of the MPLS L3 PVN network was ensured with customer sites fully connected. Also using OPNET modeler to show the behavior of the packet through the core network like throughput, delay and network convergence as performance parameters. Simulation results are analyzed and shown in table and in graphical manner. It is to be realized that MPLS is not a replacement of IP but it is designed to add a set of rules to IP so that the traffic can be classified and policed.

2. NETWORK TOPOLOGY DIAGRAM

An ISP simulated MPLS Core network was implemented to enable Layer 3 VPN service for large number of customers.

In this paper two customers where offered for VPN service. Each customer has two sites, which has to be connected between them using MPLS core network.

Customer CA has two sites one site is the Headquarter (HQ) located in Dubai, other site is the branch which is located in Khartoum, Sudan. Also Customer CB has two sites, the HQ located in Dubai and the branch site located in Khartoum, Sudan. Look at figure 1 for the network topology diagram.

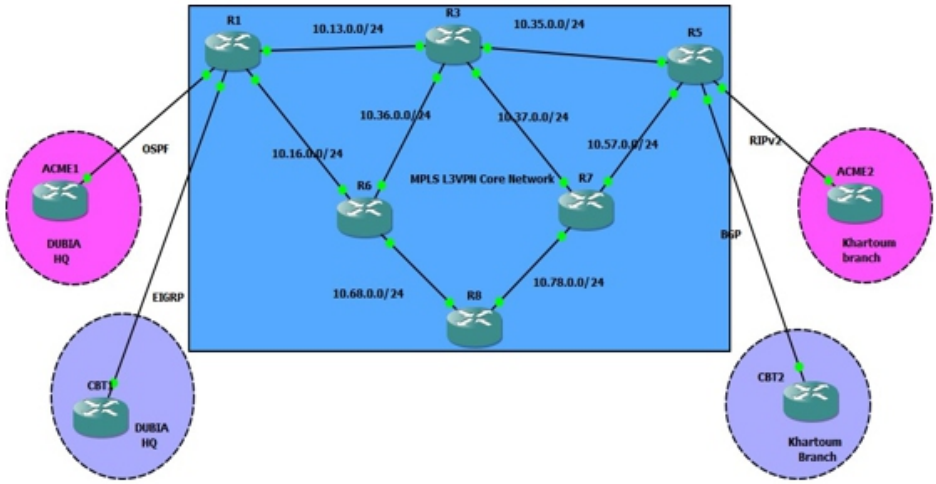


Figure 1 MPLS core network

3. MPLS CORE NETWORK RESULTS

Forwarding of packets in MPLS core is based on labels instead of IP address which is a great benefit reducing the processor overhead of the routers. The first label is imposed on the ingress LSR R1 and the label belongs to one LSP. The path of the packet through the MPLS network is bound to that one LSP. All that changes is that the top label in the label stack is swapped at each hop. The ingress LSR imposes one or more labels on the packet. The intermediate LSRs swap the top label (the incoming label) of the received labeled packet with another label (the outgoing label) and transmit the packet on the outgoing link. The egress LSR of the LSP strips off the labels of this LSP and forwards the packet.

Using core Router R6 as example to show MPLS enabled interfaces is shown in Table1. Output is given by using Cisco ISO command.

Table 1 MPLS Interfaces

```
R6#show mpls interfaces
Interface              IP         Tunnel   BGP Static Operational
GigabitEthernet1/0     Yes (ldp)  Yes      No  No     Yes
GigabitEthernet2/0     Yes (ldp)  Yes      No  No     Yes
GigabitEthernet3/0     Yes (ldp)  Yes      No  No     Yes
```

Using core Router R6 as an example to illustrate MPLS labels used to forward traffic for all MPLS Core network destination IP addresses is shown in Table 2.

Table 2 MPLS Forwarding

```
R6#
R6#show mpls forwarding-table
Local      Outgoing   Prefix           Bytes Label   Outgoing   Next Hop
Label      Label      or Tunnel Id     Switched      interface
600        302        5.5.5.5/32       0             Gi2/0      10.36.0.3
601        Pop Label  3.3.3.3/32       0             Gi2/0      10.36.0.3
602        303        10.57.0.0/24     0             Gi2/0      10.36.0.3
           806        10.57.0.0/24     0             Gi3/0      10.68.0.8
603        Pop Label  10.37.0.0/24     0             Gi2/0      10.36.0.3
604        Pop Label  10.13.0.0/24     0             Gi1/0      10.16.0.1
           Pop Label  10.13.0.0/24     0             Gi2/0      10.36.0.3
605        Pop Label  10.35.0.0/24     0             Gi2/0      10.36.0.3
606        307        7.7.7.7/32       0             Gi2/0      10.36.0.3
           800        7.7.7.7/32       0             Gi3/0      10.68.0.8
607        Pop Label  10.78.0.0/24     0             Gi3/0      10.68.0.8
608        Pop Label  1.1.1.1/32       0             Gi1/0      10.16.0.1
609        Pop Label  88.88.88.88/32   0             Gi3/0      10.68.0.8
610        Pop Label  5.5.5.5 1 [29]   25058         Gi1/0      10.16.0.1
611        811        1.1.1.1 1 [17]   26019         Gi3/0      10.68.0.8
```

Using Router R6 as example to illustrate MPLS label bindings for all MPLS Core destinations is shown in Table 3.

Table 3 MPLS label bindings

```
R6#show mpls ldp bindings
  lib entry: 1.1.1.1/32, rev 26
        local binding:  label: 608
        remote binding: lsr: 88.88.88.88:0, label: 804
        remote binding: lsr: 3.3.3.3:0, label: 308
        remote binding: lsr: 1.1.1.1:0, label: imp-null
  lib entry: 3.3.3.3/32, rev 12
        local binding:  label: 601
        remote binding: lsr: 88.88.88.88:0, label: 803
        remote binding: lsr: 3.3.3.3:0, label: imp-null
        remote binding: lsr: 1.1.1.1:0, label: 115
  lib entry: 5.5.5.5/32, rev 10
        local binding:  label: 600
        remote binding: lsr: 88.88.88.88:0, label: 802
        remote binding: lsr: 3.3.3.3:0, label: 302
        remote binding: lsr: 1.1.1.1:0, label: 116
  lib entry: 6.6.6.0/24, rev 8
        local binding:  label: imp-null
  lib entry: 6.6.6.6/32, rev 29
        remote binding: lsr: 88.88.88.88:0, label: 801
        remote binding: lsr: 3.3.3.3:0, label: 304
        remote binding: lsr: 1.1.1.1:0, label: 117
  lib entry: 7.7.7.7/32, rev 22
        local binding:  label: 606
        remote binding: lsr: 88.88.88.88:0, label: 800
        remote binding: lsr: 3.3.3.3:0, label: 307
        remote binding: lsr: 1.1.1.1:0, label: 118
  lib entry: 10.13.0.0/24, rev 18
        local binding:  label: 604
```

To show end-to-end VPN connectivity between customer CA sites look at table 4.

Table 4 End-to-End Connectivity between CA sites

```
ACME2#
ACME2#ping 172.16.111.2 repeat 10

Type escape sequence to abort.
Sending 10, 100-byte ICMP Echos to 172.16.111.2, timeout is 2 seconds:
!!!!!!!!!!
Success rate is 100 percent (10/10), round-trip min/avg/max = 120/172/248 ms
ACME2#
```

4. COMPARISON BETWEEN ROUTING PROTOCOLS

Now that the connectivity is done between the sites are going to do some comparison between routing protocols by using OPNET IT GURU v17.5 software this will generate some result. In order to understand further behaviour of the network, the network will be three different Scenarios:

- OSPF scenario
- RIP scenario
- EIGRP scenario

Using OPNET build three networks with the same specification only the routing protocol will be change during the simulation and then by comparing the three scenarios in order to find the major difference between these protocols.

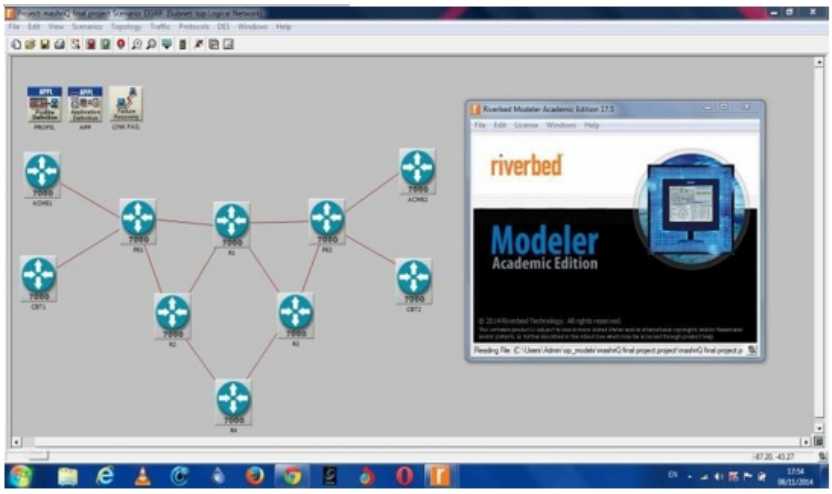


Figure 2 OPNET modeller

As show in the figure 2 the same network of the simulator GNS3 is been built again Using OPNET modeller to compare the routing protocols that is running in the network. Routers used in this scenario is Cisco 7000 core routers represented as node in OPNET simulator and the links is Ethernet 10Gbit links which is practicality used in the core network .In this network, the first scenario will be RIP scenario then OSPF and then EIGRP it's easy to navigate between scenarios in OPNET modeller. In order to show the comparison in each network the link between R1 and PE (Provider edge) will be going under eight states of fail and recovery as shown in table 5.

Table 5 Fail/Recovery states

LINK	FAIL (Second)	RECOVERY (Second)
$R_1 \rightarrow PE_2$	240	420
$R_1 \rightarrow PE_2$	520	580
$R_1 \rightarrow PE_2$	610	620
$R_1 \rightarrow PE_2$	625	626

The link between R1 and PE2 will fail at 240 seconds and will recover at 650 seconds; the duration time of simulation will be 10 minutes.

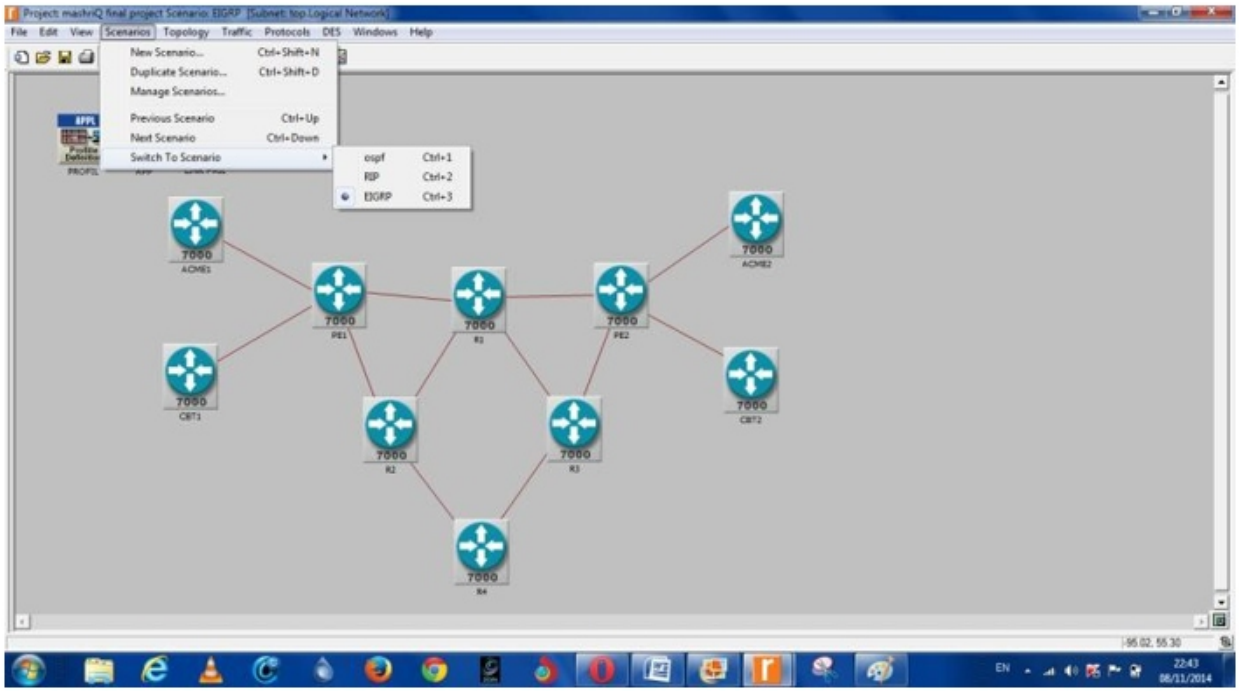


Figure 3 Navigation between scenarios

After implementing the routing protocol in each network the simulation will be running in order to get results of the comparison but first let's show each network. There are no differences between the GNS3 topology and the OPNET topology only the protocol has been changed during each scenario in order to record result, and also the fail and recovery apply each scenario.

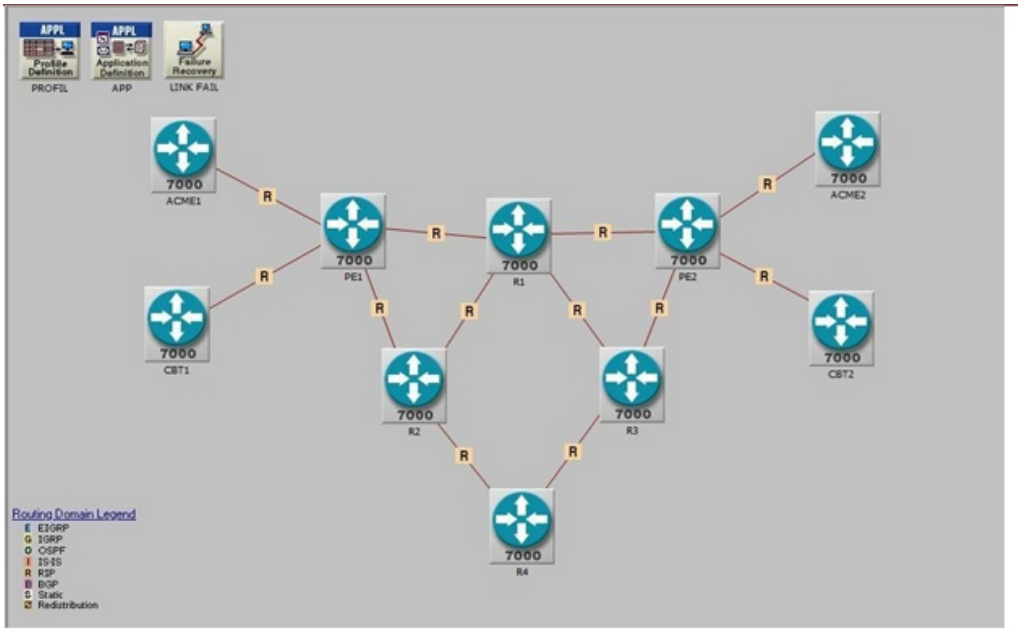


Figure 4 RIP network scenario

RIP has been configured in the network the 'R' between each pair of routers represent actual running protocol in the network which also clearly shows in figure 4.

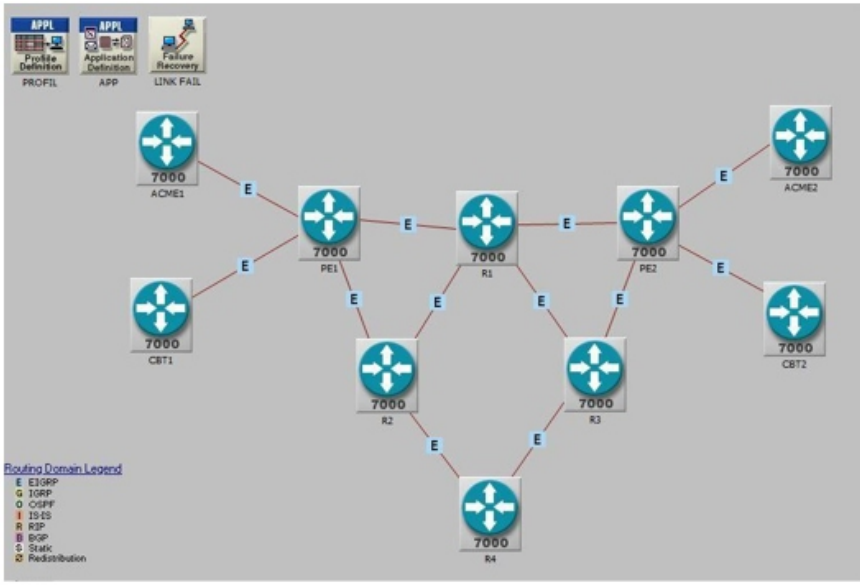


Figure 5 EIGRP network scenario

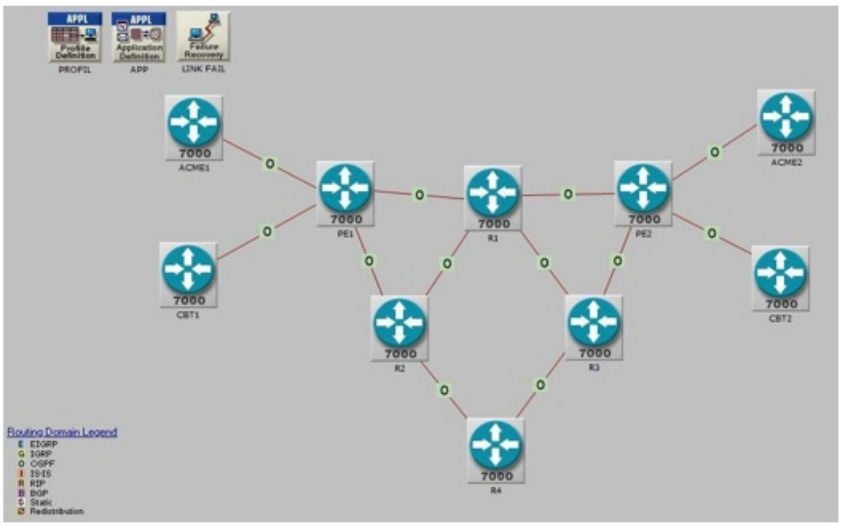


Figure 6 OSPF scenario

Figure 5 and figure 6, shows EIGRP and OSPF network scenarios respectively. Finally by running the simulation results has been found illustrated as a graphs which is easy to understand the difference between protocols as simulation goes on in this project the major differences will be show in this project.

5. THE PERFORMANCE RESULT

The first result is the network convergence duration of all three protocols (RIP, OSPF, and EIGRP) shown as overlaid. Convergence is important when dealing with routing protocols, the convergence of a routing protocol is the state of a set of routers that have the same topological information about the internetwork in which they operate, for a set of router to have converged they must have collected all available topology information from each other via the implemented routing protocol.

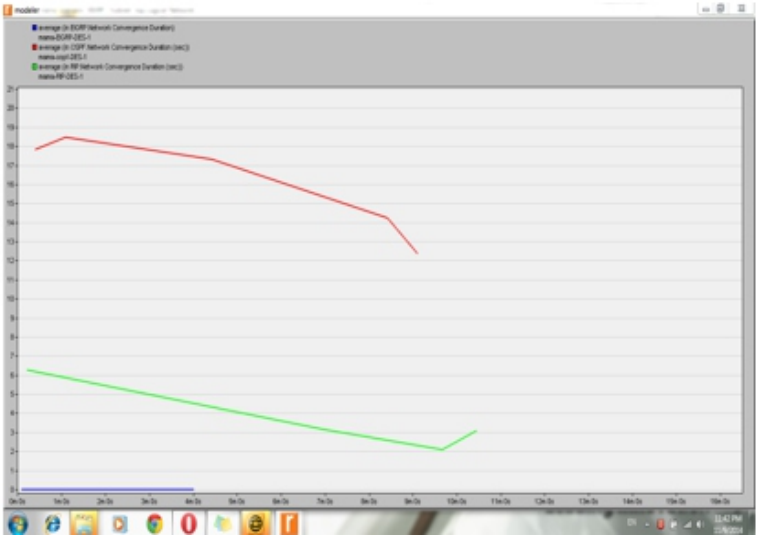


Figure 7 network convergence duration

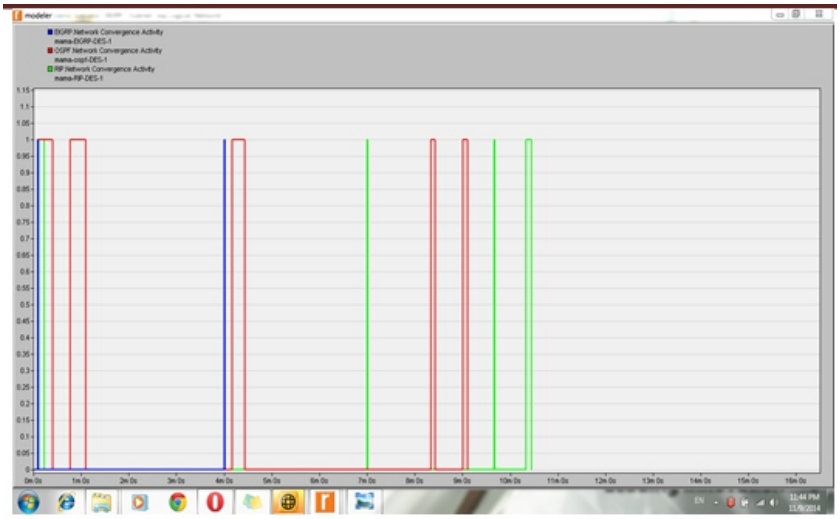


Figure 8 network convergence activities

As show in figure 7 this graph shows the average network convergence duration between RIP, OSPF and EIGRP. The fastest network convergence duration goes to the EIGRP (Blue line) which approach to zero seconds. RIP (green line) in our scenario converges faster than OSPF (red line) because the link failure is just one hop far so RIP has less convergence duration time then OSPF, in addition to that OSPF is link state protocol which depends on topology database flooded throughout the network area.

Figure 8 shows second comparison which is the network convergence activity it's a bit different from the network convergence duration.

Figure 8 show the three scenarios convergence activity is illustrated and the OSPF it has the slowest activity convergence the red line pulse has bigger width that show the OSPF is slow compare to RIP and EIGRP, the blue line represent EIGRP which has only two peaks which means has the fastest

convergence activity. After convergence the next performance is the point-to- point throughput which is a very important parameter in order to compare our three scenarios a network throughput is the average number of bits successfully received or transmitted in bits per second. The data these messages belong to may be delivered over a physical logical link or it can pass a certain network node. Throughput is usually measured in bit per second (bit/s) and sometimes in data packets per second or data packets per time slot.

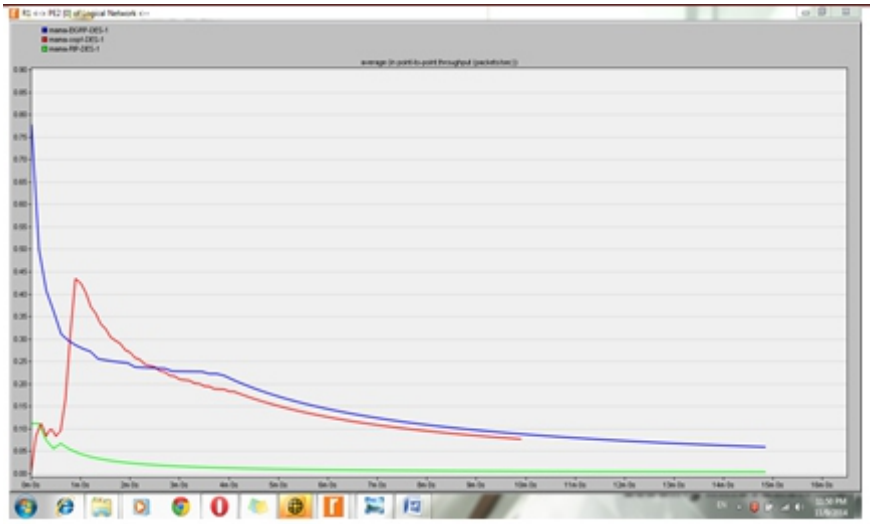


Figure 9 Average Point-to-Point Throughputs

As shown in figure 9 the average point-to-point throughput the EIGRP (blue line) has high throughput in the first minute and stabilize with time goes on, just because the protocol learn the network topology in the beginning it send high date rate. The RIP (green line) has the less point- to-point throughput.

The last performance is the Ethernet delay this statistic represents the end to end delay of all packets received by all the stations. It very important when designing a network to know the end to end delay in our case the core network delay overlaid in three different cases.

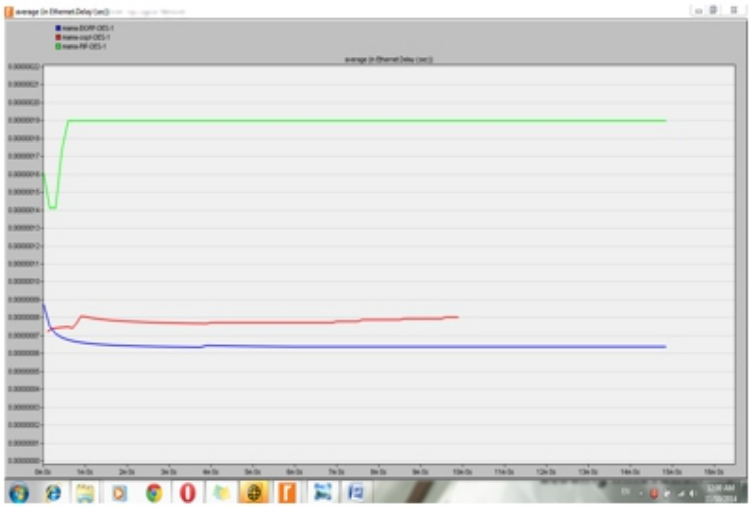


Figure 10 Time average end-to-end delay

The graph shown in figure 10 is the end-to-end delay of each three scenarios the higher delay goes to RIP (green line) it's clearly show the lack of intelligence in the RIP protocol, the OSPF(red line) start less delay than the EIGRP(blue line) and then increases where EIGRP starts higher and then decreases with time goes on. So in the network when EIGRP is implemented less delay is given.

6. CONCLUSION

The connectivity between sites of the customers has been ensured and the MPLS core network was running successfully. Next, scope of the work of the paper was extended to include study of the performance of three IP routing protocols; RIP, OSPF and EIGRP. In fact, IP routing protocols is a key condition to implement every network whether it's pure IP network or MPLS network.

In order to be able to compare the performance of the protocols, results of network convergence, throughput and end-to-end delay was found as graphs. Simulation results were confirmed that EIGRP has the fastest convergence for all network topologies. It has been observed that EIGRP and OSPF both efficiently utilize the bandwidth because both protocols do not periodically send updates as the case of RIP protocol. The RIP sends full routing information through periodic updates, which floods the network and unnecessarily wastes of bandwidth.

REFERENCES

[1] Todd Lammle, Cisco Certified Network Associate Study Guide, 4th Edition, Sybex press, 2003

[2] Eric Osborne and Ajay Simha, Traffic Engineering with MPLS, Cisco Press, 2002.

[3] Andersson L., Acreo AB Kista and Bryant S., " The IETF Multiprotocol Label Switching Standard: The MPLS Transport Profile Case", Internet Computing, IEEE, Vol. 12, No. 4, PP: 69 – 73, 2008.

[4] Luc De Ghein, MPLS Fundamentals, Cisco Press, 2006.

[5] Gurpreet Kaur and Dinesh Kumar, MPLS Technology on IP Backbone Network, International Journal of Computer Applications, Vol. 5– No.1, August 2010.

[6] Ivan Pepeinajak and Jim Guichard, MPLS and VPN architectures CCIP edition, Cisco Press, 2002

[7] Abid Shahzad and Mureed Hussain, IP Backbone Security: MPLS VPN Technology, International Journal of future generation communication and networking, Vol. 6 No. 5, 2013.

Clustering and Classification of Satellite Images using Moving KFCM and Neural Network Classifier

S. Praveena
Asst.Prof ECE Dept, M.G.I.T,
Hyderabad,A.P.

ABSTRACT

This paper presents an improvised Moving kernel based fuzzy C-means(MKFCM) for clustering of trees, shade, building and road. It starts with the single step preprocessing procedure in which first the input image is passed through a median filter to reduce the noise and get a better image fit for segmentation. The pre-processed image is segmented using the Moving KFCM algorithm and classified using feed forward neural network classifier. KFCM with moving property is used to improve the object segmentation in satellite images. Simulation result show that classification accuracy for different regions using Moving KFCM is better than KFCM using Neural Network Classifier.

Keywords : Segmentation, classification ,feature extraction, Moving KFCM

1. INTRODUCTION

Clustering has long been a popular approach to unsupervised pattern recognition. In this paper, it is focused on clustering methods by minimization of objective function and apply them to segment images. In the last decades, fuzzy segmentation methods, especially the fuzzy c-means algorithm (FCM) [1], have been widely used in the image segmentation [2], [3] and such a success chiefly attributes to the introduction of fuzziness for the belongingness of each image pixel. This allows for the ability to make the clustering methods able to retain more information from the original image than the crisp or hard segmentation methods [4].In this paper, a kernel-based fuzzy c-means algorithm (KFCM) is used. KFCM adopts a new kernel-induced metric in the data space to replace the original Euclidean norm metric in FCM. By replacing the inner product with an appropriate 'kernel' function, one can implicitly perform a nonlinear mapping to a high dimensional feature space without increasing the number of parameters. The Kernel-based FCM clustering algorithm was not considered the moving properties for segmenting the satellite image. Hence, the Kernel-based FCM clustering algorithm will be modified such a way that the moving property will be used in it to improve the object segmentation in high resolution satellite images. In this paper, an efficient classification technique using satellite image with Moving KFCM and Naïve Bayes classifier is developed and used for segmentation. The rest of the paper is organized as follows:. The proposed work is presented in Section 2. Results and discussions are presented in Section 3. Conclusions are summed up in Section 4.

2. NEW SEGMENTATION TECHNIQUE OF TREE, SHADOW, BUILDING AND ROAD USING MOVING KFCM

Satellite image segmentation technique is one of the challenging problems in image segmentation process. In proposed work, new segmentation technique of tree, shadow, building and road using moving KFCM.

2.1 PREPROCESSING

Satellite images cannot be given directly as the input for the proposed technique. Thus, it is indispensable to perform pre-processing on the input image, so that the image gets transformed to be relevant for the further processing

2.2 CLUSTERING

Clustering is done using two clustering techniques..

2.2.1 Segmentation Using KFCM

KFCM confines that the prototypes in the kernel space are actually mapped from the original data space or the feature space. That is, the objective function is defined as

$$Q = \sum_{i=1}^{c} \sum_{j=1}^{n} u_{ij}^{m} \left(1 - k(x_{j,} o_{j})\right)$$

Usually, only the Gaussian kernel $k(x, y) = \exp(-\|x - y\|^2 / r^2$ is applied in KFCM. Here, $1 - k(xj, oi)$ can be considered as a robust distance measurement derived in the kernel space [12]. For these KFCM applying Gaussian kernels [13], we iteratively update the prototypes and memberships as

$$o_i = \frac{\sum_{l=1}^{n} u_{il}^{m} k(x_l, o_i) x_l}{\sum_{l=1}^{n} u_{il}^{m} k(x_l, o_i)}$$

$$u_{ij} = \frac{(1 - k(x_j, o_i))^{-1/m-1}}{\sum_{l=1}^{c} (1 - k(x_j, o_l))^{-1/m-1}}$$

2.2.3 Segmentation Using Moving KFCM

The algorithm is called moving KFCM because during the clustering process, the fitness of each centre is constantly checked and if the centre fails to satisfy a specified criterion the centre will be moved to the region that has the most active centre.

The algorithm is designed to have the following properties:

a) There is no dead centre as the centers will have the same fitness in term of the fitness criteria.

b)More centers will be allocated at the heavily populated data area but some of the centers will also be assigned to the rest of the data so that all data are within an acceptable distance from the centers.

c) The algorithm is capable of avoiding poor local minima as the algorithm can reduce the sensitivity to the initial centers Consider a problem that has N data that have to be clustered into n_c centers. Let x_i be the i- th data and o_i be the i-th centre where i= 1, 2, ..., N and j = 1, 2, ..., n_c. Initially, centers o_i are initialized to some values and each data is assigned to the nearest centre and the position of the centre o_i is calculated according to:

$$o_i = \frac{\sum_{l=1}^{n} u_{il}^m k(x_l, o_i) x_l}{\sum_{l=1}^{n} u_{il}^m k(x_l, o_i)} \qquad (1)$$

Where,

$$u_{ij} = \frac{(1 - k(x_j, o_i))^{-1/m-1}}{\sum_{l=1}^{c} (1 - k(x_j, o_i))^{-1/m-1}} \qquad (2)$$

In above equation, following kernel function can be used

$$k(x_i, x_j) = \exp\left(- \frac{\left\| x_i - x_j \right\|^2}{r^2} \right) \qquad (3)$$

After all data are assigned to the nearest centers, the fitness of the centers is verified by using a distance function. The distance function is based on the total Euclidean distance between the centre and all the data that are assigned to the centre and update the equation

$$f(c_j) = \sum_{i \in c_j} (\left\| x_i - o_j \right\|)^2 \qquad (4)$$

The moving KFCM can be implemented as:

(1) Initialize the centers and V_0 and set $V_a = V_b = V_c$

(2) Assign all the data to nearest center and calculate center positions using eq (1)

(3) Check the fitness of each centre using equation(4)

(4) Find c_s and c_1, the centre that has the smallest and the largest value of $f(\bullet)$

(5) If $f(c_s) < \alpha_a f(c_l)$,

(5.1) Assign the members of o_s to o_l if $x_i < o_l$, where $i \in o_l$, and leave the rest of the members to o_1.

(5.2) Recalculate the positions cl according to:

$$o_i = \frac{\sum_{l=1}^{n} u_{il}^m k(x_l, o_i) x_l}{\sum_{l=1}^{n} u_{il}^m k(x_l, o_i)}$$

$$u_{ij} = \frac{(1 - k(x_j, o_i))^{-1/m-1}}{\sum_{l=1}^{c} (1 - k(x_j, o_i))^{-1/m-1}}$$

Note that o_s will give up its members before step (5.1) and, o_s and o_1 in equation (5) are the number of the new members of c_s and c_1 respectively, after the reassigning process in step (5.1).

(6) Update α_a according to $v_a = v_a - v_a / n_c$ and repeat step (4) and (5) until $f(o_s) \geq v_a f(o_l)$

(7) Reassign all data to the nearest centre and recalculate the centre positions using eq (1)

(8) Update v_a and v_b according to $v_a = v_0$ and $v_b = v_b - v_b / n_c$ respectively, and repeat step (3) to (7) until $f(o_s) \geq v_a f(o_l)$.

2.3 Feature Extraction

From the 36 segments we are combining the corresponding segments and obtaining the corresponding 4 new segments such as tree, shade, road and building. These 4 new segments are used for the feature extraction process. These regions features are given as input to Classifier. Feature extraction step is formulated in the following step.

- For feature extraction calculate the histogram of h layer, s layer and l layer. A set of histogram values are obtained.
- The normalized histogram values are found out by dividing each value in the histogram with the sum of all values in the histogram.
- Sort the histogram values in descending order. Record the first three values from the values obtained in the above step.
- The values obtained are used for feature extraction.

2.4 Classification Using Neural Network Classifier

These features are given to Neural Network classifier to identify buildings ,shades, trees and roads in a given image as data base images are pretrained using neural network classifer.

3. RESULTS AND DISCUSSION

In this section, results of the proposed technique are discussed. Satellite image is used as the input image which is to be classified into the regions of tree, shade, road and building. In proposed technique, the input image is subjected to a set of pre-processing steps which make the image is more suitable for segmentation. This image is segmented using the Moving KFCM algorithm. Bayesian classifier with four different kernels is used for classification. The classification accuracy obtained for tree, shade, road and building by the above four classifiers are better when compared with the segmented images obtained by KFCM.

The Figure 2 shows the input satellite image of an area taken from the satellite and contains the tree, shade, road and building which is to be classified into four regions using proposed technique.

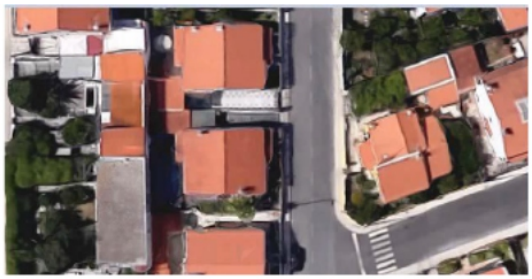


Fig 2.Input satellite image

The Figure 3 shows the final classified tree image from the input image.

Fig 3: Classified tree region from input image

The Figure 4 shows the final classified shade image from the input image.

Fig 4: Classified shade region from input

The Figure 5 shows the final classified road region from the input image.

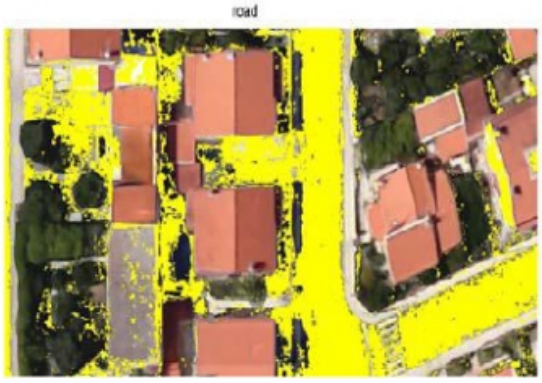


Fig 5: Classified road region from input

The Figure 6 shows the final classified build region from t he input image.

Fig 6: Classified build region from input

4. EVALUATION OF CLASSIFIER'S PERFORMANCE

The comparative analysis shows the performance analysis of the proposed technique with moving KFCM algorithm. The accuracy value is computed by dividing the total number of similar pixels identified as land use to the number of pixels in the tree, shade, building and road region. The following graphs signify the performance of the proposed technique compared with KFCM. Figure 7 shows the plot of accuracy graph- tree, shade, road and building region classification. It clearly indicates that MKFCM accuracy is greater than KFCM accuracy.

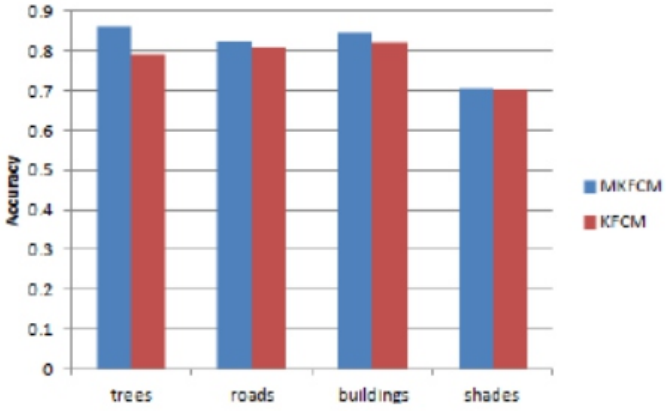


Fig 9:Accuracy graph-tree,shade ,road and building region classification

5. CONCLUSION

In this paper, an efficient image classification technique for satellite images with the aid of MKFCM is proposed. Here in proposed classification technique is made of four phases namely pre-processing, segmentation, feature extraction and final classification using Naïve Bayes classifier. In the pre-processing step, the input image is subjected a set of pre-processing steps which includes median filtering. The pre-processing results in transforming the input image into an image fit for segmentation. After the preprocessing, the image is clustered using Moving KFCM. For the clustered image all features are calculated and applied to neural network classifier. The neural network classifier identifies the different regions in the image. The experimental results have demonstrated the effectiveness of the

proposed classification technique in classifying into road, building, trees and shade regions. The experimentation is carried out using the satellite images and the analysis ensures that the performance of the proposed technique is improved compared with KFCM.

7.REFERENCES

[1] J. C. Bezdek,Pattern Recognition With Fuzzy Objective Function Algorithms .New York: Plenum, 1981..

[2] J. K. Udupa and S. Samarasekera, "Fuzzy connectedness and object definition: theory, algorithm and applications in image segmentation," Graph. Models Image Process. , vol. 58, no. 3, pp. 246 – 261, 199 6.

[3] S. M.Yamany, A. A. Farag, and S. Hsu, "A fuzzy hyperspectral classifierfor automatic target recognition (ATR) systems, " Pattern Recognit. Lett. ,vol. 20, pp. 1431 – 1438, 1999

[4] D. L. Pham and J. L. Prince, "An adaptive fuzzy C -means algorithm for image segmentation in the presence of intensity inhomogeneities," Pattern Recognit. Lett. , vol. 20, pp. 57 – 68, 1999. .

[5] . Q. Zhang an d S. C. Chen, "A novel kernelized fuzzy C -means algorithm with application in medical image segmentation," Artif. Intell. Med. , vol. 32, no. 1, pp. 37 – 50, Sep. 2004..

[6] D. Graves and W. Pedrycz, "Kernel -based fuzzy clustering and fuzzy clustering: A comparat ive experimental study," Fuzzy Sets Syst. , vol. 161,no. 4, pp. 522 – 543, Feb. 16, 2010

[7] George H. John and Pat Langley" Estimating Continuous Distributions in Bayesian Classifiers," Proceedings of the Eleventh Conference on Uncertainty in Artificial Intelligence. pp. 338-345. Morgan Kaufmann, San Mateo, 1995

[8] PCI Enterprises Inc., "SAR Radiometric Correction", RadarSoft Course notes. pp. 80-91, 1997.

[9] Young, S. S. and Wang, C. Y., "Land-cover change analysis of China using global-scale Pathfinder AVHRR Landcover (PAL) data", International Journal of Remote Sensing, Vol. 22, No. 8, pp. 1457-1477, 2001.

[10] Lillesand, T. M. and Kiefer, R. W, (1994) "Remote Sensing and Image Linter Predation", John Wiley and Sons Press.

[11] Tso B. and Mather P. M., "Classification Methods for Remotely Sensed Data", Taylor and Francis, London, 2001.

[12] Chang C. I. "Hyperspectral Imaging: Techniques for Spectral Detection and classification", Kluwer Academic Publishers, 2001.

[20] Varshney, P. K. and Arora, M. K., "Advanced Image Processing Techniques for Remote Sensed Hyperspectral Data", Springer-Verlag, Germany, 2004.

Role of Wireless Sensor Networks in Agriculture

Deep Mala, Dr. Suhas H. Patil
Research Scholar, JJTU(Rajasthan)
Professor, Bharti Vidyapeeth University (College of Engineering), Pune

ABSTRACT

The Wireless Sensors Network (WSN) is now-a-days widely used to build decision support systems to overcome many problems in the real-world. This paper presents WSN as the best way to solve the agricultural problems related to crops identification, crop condition, yield estimation etc. This approach provides real-time information about the lands and crops that will help farmers make right decisions. The software monitors data from the sensors in a feedback loop which activates the control devices based on threshold value. Implementation of WSN in agriculture will optimize the usage of water fertilizer and also maximized the yield of the crops.WSN is an intelligent system which can monitor the agricultural environments of crops and provides service to farmers. The wireless sensor network (WSN) technique attracts increasing attention in recent years. The purpose of such systems is to improve the outputs of crops by means of managing and monitoring the growth period.

Keywords: agriculture, crop, monitoring, sensors, soil, wireless.

1) INTRODUCTION

Wireless sensor networks are being used in a wide variety of critical applications such as military and healthcare applications, agriculture and industrial process monitoring. WSN is an intelligent private network made by a large number of sensor nodes which do specific functions. Wireless transmission allows deploy the sensors at remote, dangerous, and hazardous location. WSN has several advantages including easy installation, cost-effectiveness, small size and low power consumption. In recent years, agriculture faces many challenges, while humanity depends on agriculture and water for survival, so precision agriculture monitoring is critical and the demand for environmental monitoring and remote controlling in agriculture is rapidly growing. However, there have been few researches on the applications of WSN for agriculture.

2) HOW THE SENSOR NETWORK TECHNOLOGY WORKS

The sensor nodes are planted in the area which is under experiment. They sense the different parameters for which they are meant. These all individual nodes perform the minimal data processing and then send back the data via a base station to a single server where they are processed further. Data is transmitted between the individual nodes via a wireless sensor link. Then between the head nodes and the base station through some other link depending on the technology which suits most. At last there is

Access Subsystem in which a web-based interface is used for the display and upload of both raw and processed data. As most of the farmers do not have access to the web, those data are made available at a local village center in the form of graphs and spread-sheets.

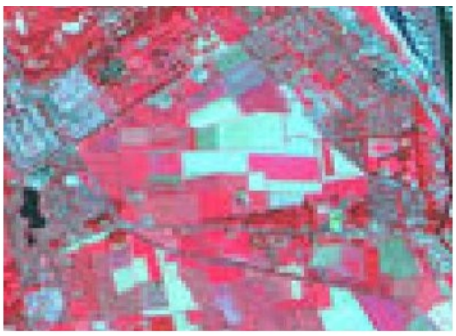
3) CONTRIBUTION OF SENSORS IN AGRICULTURE

Different sensors are employed for sensing various parameters like soil moisture, water levels, climate change, pest detection, humidity to various other things in the fields. For sensing these parameters, the sensors are deployed in the field. They are spread in such a way that they cover the whole field. Now these sensors can be used in many different ways. The basic technology employed in the sensors is the same. Only the way they are spread out differs. But this different arrangement plays an important role as when used efficiently these sensors save time, save the required power and also may decrease the channel congestion, thus increasing the overall efficiency of the whole network.

3.1) Crop identification

It is based on the fact that each crop has unique spectral signature. Typical spectral reflectance of a crop shows absorption due to pigments in the visible region, high reflectance in the near infrared region because of internal cellular structure of the leaves and absorption at 1.45, 1.95 and 2.6m spectral bands due to water content. If we compare the same fields in the two images, we can see that in some cases the signal is different. Fields that appear red (high near-infrared reflectance) are full of vegetation, whereas those that appear blue (low near-infrared reflectance) either have very little or no vegetation at all. In that case the recorded signal is originating from the ground. Having the knowledge of when each crop is planted and harvested, we can estimate the percentage of vegetation cover through the growth period, assuming no external factors affect its growth. With this knowledge and by studying two or more images from the same growth period, we can look at the multispectral reflectance signal at each growth stage and identify what crops are grown in each field.

Crop field in May



Crop field in May

3.2) Crop Acreage estimation

It is the procedure which composed of identifies the various crops/ land on the image based on the ground. Traditionally acquiring data about yield and acreage of crops is an extremely tedious job,

including extensive travel and various interpolation methods based on the sample taken. Currently the agriculture department officials visit the village or Tehsil where they inquire about crop acreage and expected yield. Based on these types of sampling the results are projected to acquire the acreage and yield information. This methodology, though prevalent from a long time is neither very accurate nor very scientific. On the other hand, it is predicted on the basic production pattern over the previous year. Yield depends on various factors, like climatic, physical etc. Apart from being cumbersome, counter cost effective and lengthy, these traditional methods are also too generalized and can't be fully relied upon. Alternatively, sensing is a very important tool for acreage estimation. With the help of sensing it is possible in a short time with much accuracy to measure the crop acreage estimation. [4]

3.3) Crop condition assessment /Yield Estimation

Accurate, early estimation of grain yield is an important skill. Farmers require accurate yield estimates for a number of reasons:

- Crop insurance purposes
- Delivery estimates
- Planning harvest and storage requirements
- Cash-flow budgeting

Extensive personal experience is essential for estimating yield at early stages of growth. As crops near maturity, it becomes easier to estimate yield with greater accuracy. Use of remote sensing to estimate biological crop yield is being explored in many countries and likely will become the basis of agricultural statistics in the future (Zhao et al., 2007). Crop yield estimation using remote sensing is based on the principle of spectral reflectance of green plants, which can be captured in satellite images as spectral data, depends on the state, structure and composition of the plant. The spectral data can be used to construct several vegetation indices such as normalized difference vegetation index (NDVI) which indicates the green biomass that can be used as proxy indicator of the yield (Prasad et al., 2006). The limitation in the use of satellite images to estimate crop yields of smallholder farmers is that the resolution of available satellite imagery (pixel size) is not sufficiently detailed to capture the variability of crops and crop performance in smallholder fields, (Fermont and Benson, 2011). In India, for example, vegetation indices from satellite images show only a moderate correlation (R2 between 0.45 to 0.54) with crop cut data (Singh, 2013). [6]

3.4) Identification of planting and harvesting dates

Electronic-nose devices have been utilized in a wide range of diverse applications in the agriculture and forestry industries to improve the effectiveness, efficiency and safety of processes involved in the

production of quality food and fibre plant-based products. Sensors help to identify the best suiting time for each and every vegetation for planting and harvesting. It directly affects the production of crop. The sensor network technology will help the farmers to know the exact values of the requirements that they need to improve the crop productivity. It will help them in taking better decisions at the right time. This will save their time and labor also. The basic aim here is to transport the Indian farmers from prediction to the exact values which are beneficial for their farms. [2]

3.5) Identification of Pest and Disease Infestation

Pest detection and control is at least as old as agriculture because there has always been a need to keep crops free from pests. A number of techniques so far proposed for pest control in agriculture using wireless sensor network. There is a solution for monitoring traps which they used to capture pest by means of image sensors. A low-cost system based on battery powered wireless image sensors, which are able to capture and send images of the trap contents to a remote control station with specific frequency demanded by trapping application. These image sensors accurately monitor pest population with a higher temporal resolution. During this monitoring process no human intervention is demanded. There is a significant reduction in monitoring cost as well. Trap monitoring process which works on unattended mode has some extra benefits like it reduces the monitoring cost: it is programmable and higher temporal resolution of trap monitoring data. In addition, monitoring data can be available in real time through an internet connection. There have been a number of valuable studies to monitor pest insect using latest technologies. However, none of these studies provide a self-sufficient monitoring system based on low cost image sensors covering areas with very low energy utilization. High scalability with low power consumption made it possible to deploy both green houses and larger plantations. It is also used for several kinds of insects instead of some specific insects.

3.6) Soil moisture estimation

Estimating soil properties, including soil moisture, is important for many water-budgeting processes, and for meteorological and agricultural applications. Soil-moisture information can also be used as an indicator for the prediction of natural disasters, such as flooding and droughts, and for environment changing, such as dust storms and erosions. The most accurate results are achieved when there is no or low soil cover, especially when the test area is flat. On the basis of the active remote sensing methods, estimating soil moisture on bare soil or soil with less vegetation gives more accurate results, as compared to using the methods on a mixture of land-cover soil. Moreover, the estimation process becomes more challenging when the vegetation cover is dense. From the other side, under similar soil cover conditions, retrieving soil moisture using a combination of both active and passive soil information gives reasonably accurate results. [5]

3.7) Irrigation Monitoring and management

This monitoring can be accomplished by different techniques, including sensors in the soil, like a C-Probe, or a water budget modeling approach using climate parameters, such as evapotranspiration and rainfall. All of these techniques have been tested and validated for different crops around the world, showing promising results. By adopting irrigation monitoring techniques growers will be able to irrigate rationally, improving crop yield and quality, increasing the effectiveness of fertilizers and encouraging the proper balance of micro-organisms. In addition, the proper management of irrigation will reduce soil salinity and increase soil oxygen content, improving root activity. Irrigation monitoring allows for improved crop performance and can reduce the grower's water bill directly in maximizing water usage along with extending the lifetime usage of the irrigation equipment. [9]

3.8) Soil Mapping

Soil survey provides an accurate and scientific inventory of different soils, their kind and nature, and extent of distribution so that one can make prediction about their characters and potentialities. It also provides adequate information in terms of land form, terraces, vegetation as well as characteristics of soils (viz., texture, depth, structure, stoniness, drainage, acidity, salinity and so on) which can be utilized for the planning and development. The use of digital image processing for soil survey and mapping was initiated with the establishment of National Remote Sensing Agency and Regional Remote Sensing Service Centres. The initial works carried out by Venkatratnam (1980); Kudrat et al (1990) and Karale (1992) demonstrated the potential of digital image processing techniques for soil survey. A number of modelling studies were simultaneously carried out to derive a variety of information from soil maps, e.g. land evaluation, land productivity, soil erosion and hydrologic budget (Kudrat et al 1990; Saha et al 1991; Kudrat 1996; Kudrat et al 1995, Kudrat et al 1997). The soil maps are required on different scales varying from 1:1 million to 1:4,000 to meet the requirements of planning at various levels. Because the scale of a soil map has direct correlation with the information content and field investigations that are carried out. Small scale soil maps of 1:1 million are needed for macro level planning at national level. The soil maps at 1:250,000 scales provide information for planning at regional or state level with generalized interpretation of soil information for determining the suitability and limitations for several agricultural uses and require less intensity of soil observations and time. The soil maps at 1:50,000 scales where association of soil series are depicted serve the purpose for planning resources conservation and optimum land use at district level and require moderate intensity of observations in the field. The large scale soil maps at 1:8,000 or 1:4,000 scale are specific purpose maps which can be generated through high intensity of field observations based on maps at 1:50,000 scale of large scale aerial photographs or very high resolution satellite data. Similarly, information on degraded lands like salt affected soils, eroded soils, waterlogged areas, shifting cultivation etc., is required at different scales for planning strategies for reclamation and conservation of degraded lands (Venkataratnam 1999). [7]

3.9) Monitoring of Draughts

Monitoring and assessment of drought through remote sensing and GIS depend on the factors that cause drought and the factors of drought impact. Based on the causative factors, drought can be classified into Meteorological, Hydrological and Agricultural droughts. An extensive survey of the definition of droughts by WMO found that droughts are classified on the basis of: (i) rainfall, (ii) combinations of rainfall with temperature, humidity and or evaporation, (iii) soil moisture and crop parameter, (iv) climatic indices and estimates of evapotranspiration, and finally (v) the general definitions and statements. Drought is a normal, recurrent feature of climate and occurs in all climatic zones, although its characteristics vary significantly from one region to another. Drought produces a complex web of impacts that span many sectors of the economy and reach well beyond the area experiencing physical drought. Drought impacts are commonly referred to as direct or indirect. Reduced crop, rangeland, and forest productivity; increased fire hazard; reduced water levels; increased livestock and wildlife mortality rates; and damage to wildlife and fish habitat are a few examples of direct impacts. The consequences of these impacts illustrate indirect impacts. The remote sensing and GIS technology significantly contributes to all the activities of drought management. [10]

3.10) Land cover and land degradation mapping

Land degradation caused by deforestation, overgrazing, and inappropriate irrigation practices. It causes decline in productive capacity of the land. It encompasses the whole environment but includes individual factors concerning soils, water resources (surface, ground), forests (woodlands), grasslands (rangelands), croplands (rainfed, irrigated) and biodiversity (animals, vegetative cover, soil). It is complex and involves the interaction of changes in the physical, chemical and biological properties of the soil and vegetation. The complexity of land degradation means its definition differs from area to area, depending on the subject to be emphasized. [8]The knowledge of land use and land cover is important for many planning and management activities as it is considered as an essential element for modelling and understanding the earth feature system. Land use is defined as to the human activity or economy related function associated with a specific piece of land, while the term land cover relates to the type of feature present on the surface of the earth (Lillesand and Kiefer, 2000). [3]

3.11) Identification of problematic soil

Soil salinity caused by natural or human-induced processes is certainly a severe environmental problem that already affects 400 million hectares and seriously threatens an equivalent surface. Stalinization causes negative effects on the ground; it affects agricultural production, infrastructure, water resources and biodiversity. In semi-arid and arid areas, 21% of irrigated lands suffer from water logging, salinity and/or sodicity that reduce their yields. 77 million hectares are saline soils induced by

human activity, including 58% in the irrigated areas. In the irrigated perimeter of Tadla plain (central Morocco), the increased use of saline groundwater and surface water, coupled with agricultural intensification leads to the deterioration of soil quality. Experimental methods for monitoring soil salinity by direct measurements in situ are very demanding of time and resources, and also very limited in terms of spatial coverage. Several studies have described the usefulness of remote sensing for mapping salinity by its synoptic coverage and the sensitivity of the electromagnetic signal to surface soil parameters. [1]

4) CONCLUSION

The wireless sensors networks helps in agricultural monitoring at remote sites and reachable locations. It increases the crop yield and improvement in the quality in the agricultural field by supporting the decision making of producers through the analysis of the collected information. Various methods are used to identify the problematic soil which prevents the farmers from loss of money and time. Monitoring of draughts and proper irrigation time help the farmers for better yield of the crop.

5) REFERENCES

1) *Rachid Lhissou , Abderrazak El Harti , Karem Chokmani ," Mapping soil salinity in irrigated land using optical remote sensing data","Eurasian Journal of Social Science",pp.82-88(2014).*
2) *Rashid Hussain, J L Sahgal, Purvi Mishra, Babita Sharma," Application of WSN in Rural Development, Agriculture Water Management", International Journal of Soft Computing and Engineering (IJSCE), Volume-2, Issue-5, PP.65-72 (Nov. 2012).*
3) *http://agrophysics.in/Published/2012/4-GS-Tagore.pdf*
4) *http://geospatialworldforum.org/2011/proceeding/pdf/AbhishekFullPaper.pdf*
5) *http://photonicsforenergy.spiedigitallibrary.org/article.aspx?articleid=1182520*
6) *http://samples.ccafs.cgiar.org/measurement-methods/chapter-8-yield-estimation-of-food-and- non-food-crops-in-smallholder-production-systems/*
7) *http://www.tropecol.com/pdf/open/PDF_43_1/43106.pdf*
8) *http://www.unulrt.is/static/fellows/document/taimi.pdf*
9) *http://www.vineandtreefruitinnovations.com/niagarairrigation.cfm*
10) *http://www.wamis.org/agm/pubs/agm8/Paper-14.pdf*

"implications of Network Neutrality in the Light of Make in India Digital Drive"

Ms. Ankita Jain, Ms. Vandana Gablani
Assistant Professor, Delhi School of Professional Studies & Research, New Delhi
Assistant Professor, Delhi School of Professional Studies & Research,New Delhi

ABSTRACT

Internet is everywhere, without it no organization can think of business in this fast moving world where survival of the fittest in the world market finds itsnichewith the delivery of not only right information to right person at right time and place but also the dissemination of information over the internet should be impartial i.e. Network Neutrality or Net Neutrality. [1]

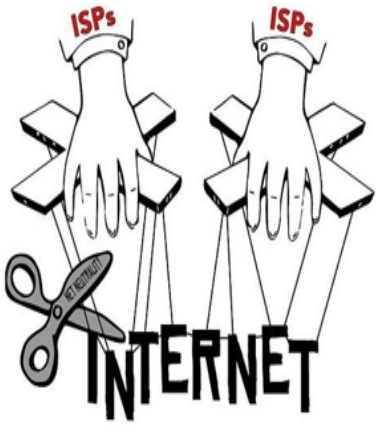
Network neutrality is the principle that all Internet traffic should be treated equally.[2] *According to Columbia Law School professor Tim Wu, the best way to explain network neutrality is as when designing a network: "that a public information network will end up being most useful if all content, sites, and platforms are treated equally."* [3]

This paper discusses about the implications of the network neutrality in the light of the Make in India digital drive. In other words, the objective is to discuss whether the dream of making India, truly a digital India as part of Make in India project will be successful if all the internet service providers in India give their customers equal access to all lawful websites and services on the Internet, without giving priority to any website over another.

Keywords: Digital India, Net Neutrality, Make in India, Internet for all, Save the Internet

INTRODUCTION

Should the Net Be Neutral?



This very hot debate took its very first flight when a survey of operator practices in US was conducted in 2002.[4] In that year, evidence of a discrimination problem became clear from several sources, including consumer complaints about operators who ban classes of applications or equipment, like servers, Virtual Private Networks, or Wi-Fi devices[5],and in filings at the Federal Communications Commission by application developers.[6] The survey advised that operators indeed had implemented significant contractual and architectural limits on certain classes of applications.

Operators showed an unfortunate tendency to ban new or emerging applications or network attachments, like Wi-Fi devices or Virtual Private Networks, perhaps out of suspicion or an (often futile) interest in price discrimination. On the whole the evidence suggested that the operators were often pursuing legitimate goals, such as price discrimination and bandwidth management. The problem was the use of methods, like bans on certain forms of applications, which were likely to distort the market and the future of application development.[7]

Global Threats to Net Neutrality

In the light of the foregoing facts and the possible threat to the Internet with regards to its unbiased use globally, many rules were made and adopted but the latest rules adopted by the Federal Communications Commission[8] on February 26, 2015 – the FCC's Open Internet rule gave strongest ground as far as legal foundations are concerned. The new rules will protect no matter how they access the internet-over mobile or desktop computer.

Few of the glimpses of above said rules[9]

No Blocking:

Broadband providers may not block access to legal content, applications, services, or non-harmful devices.

No Throttling:

Broadband providers may not impair or degrade lawful Internet traffic on the basis of content, applications, services, or non-harmful devices.

No Paid Prioritization:

Broadband providers may not favor some lawful Internet traffic over other lawful traffic in exchange for consideration of any kind—in other words, no "fast lanes." This rule also bans ISPs from prioritizing content and services of their affiliates.

To ensure an open Internet now and in the future, the Open Internet rules also establish a legal standard for other broadband provider practices to ensure that they do not unreasonably interfere with or disadvantage consumers' access to the Internet. The rules build upon existing, strong transparency requirements. They ensure that broadband providers maintain the ability to manage the technical and engineering aspects of their networks. The legal framework used to support these rules also positions the Commission for the first time to be able to address issues that may arise in the exchange of traffic between mass-market broadband providers and other networks and services.

But policy makers in other regions of the world like Europe and India are on the track of making new rules that could threat the net neutrality. Few months back, the European Council, which is made up of the 28 national governments of European Union members, adopted a proposal that would allow telecom companies to charge Internet businesses like Google fees to deliver their content to the users faster as compared to smaller companies that could not afford to pay that preferential payment.

Net Neutrality: The Indian Ambience

The topic of "net neutrality" came to spotlight in India in December 2014 when Airtel, a mobile telephony service provider announced the additional charges for making voice calls from its network using apps like Watsapp, Facebook, Skype etc[10] . However, the issue of net neutrality started creeping in 2006 itself when TRAI published a paper on it by inviting options from stakeholders whether regulatory inventions are required or left to market force.[11] Bharti Airtel's Director of Network Services, Jagbir Singh in July 2012, recommended that large Internet companies like Facebook and Google should contribute a part of their revenues to telecom companies. According to him, Internet companies were enjoying huge profits from small investments, whereas the telecom companies were actually investing in building networks. This move of Airtel faced harsh criticism on social networking sites due to which later on 29 December 2014, Airtel announced that it would not be implementing planned changes, pointing out that TRAI would be soon releasing a consultation paper on the issue.[12] On 27 March 2015, TRAI released a consultation paper on over-the-top services (OTT) and net neutrality for public feedback.[13][14] The last date for submission of comments was 24 April 2015 and TRAI received over a million emails.[15]Another scheme that violates net neutrality is launching of Internet.org in India with Reliance Communications by Facebook in February 2015 that aims to provide free access to 38 websites through an app.[16] To add to this listin April 2015, Airtel announced "Airtel zero" scheme under which if an app sign contract with them then Airtel will provide that app free of cost to it's customer.[17] Flipkart decided to join the scheme but again due to negative response from the public and being criticized for its action it pull out its hand from this scheme. All these schemes time and again has breached the net neutrality in India.

LITERATURE REVIEW

Bruce M. Owen has enlightened in his paper on "The Net Neutrality Debate" [18] that regulator and regulations have time and again been obstacle in the path of technological innovation as it gives power to the present producers by preventing entry of new competitors, which in turn reduces incumbent's own enticement to innovate. According to him, sad history of failure of attempts to regulate old AT&T under traditional utility regulation principle should be an eye opener for us that the "net neutrality" remedy is a cure far worse than the feared disease.

Robin S. Lee and Tim Wu in their paper on "Subsidizing Creativity through Network Design: Zero-Pricing and Net Neutrality"[19] emphasized on the theory of two-sided market which suggests the de-facto ban on termination fees on the content providers by the Internet service Providers and hence supports the zero- pricing aspect of net neutrality. The theory of two-sided markets provides bedrock for the skyscraper building of new content and spurs innovation while avoiding crumbling of the Internet.

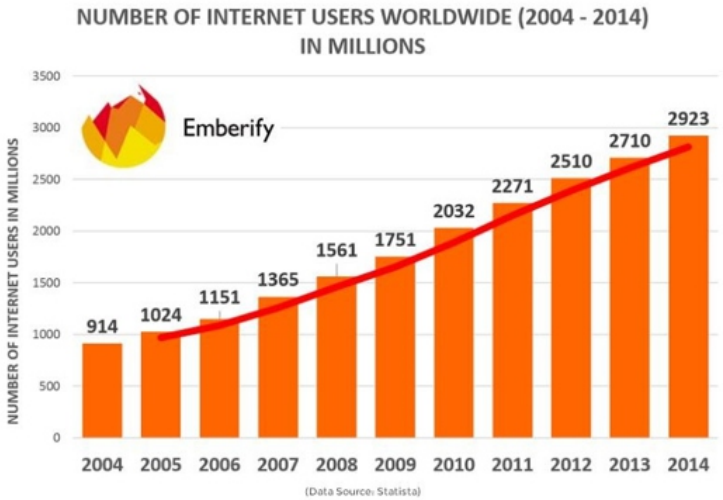
H.Kenneth Cheng, Hong Guop and Subhajyoti in the paper "The Debate on Net Neutrality: A Policy Perspective"[20] found that if the net neutrality concept is removed the broadband service providers will be on gaining side because they will be able to extract preferential fees rom the content providers. Also, incentive to expand infrastructure capacity for broadband service provider under the umbrella of net neutrality are higher than the no neutrality regime as under net neutrality broadband service provider always invest in broadband infrastructure at socially optimum level but either under-or –over invests in infrastructure in absence of it.

Not much research has been conducted in this so far because it is one of the latest issue that has come into limelight, thus having a great scope of further studies with the suggestions of its implementation and its impact over the Indian Economy.

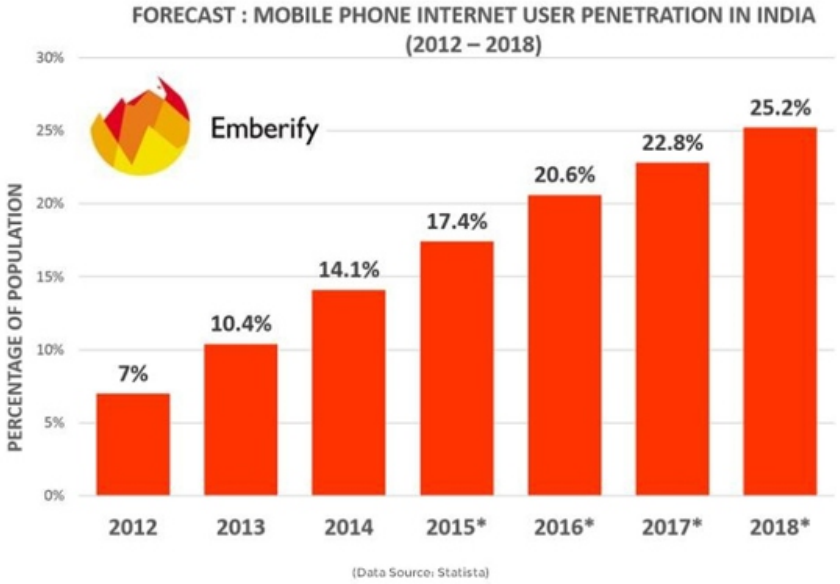
NET NEUTRALITY: THE REAL STAKEHOLDERS

A threat to the Start-up Ecosystem

Startups are taking India by storm and galvanizing the picture of India in global market. All this is because of the vast customer that they can pitch through the internet. Beauty of internet is that anyone with a computer and an internet connection can start his own business and reach the new heights in Business world. Firstly, the number of Internet users in the world is on a steady rise. If we look at the statistics from 2004 up to 2014, we see that the number of users has been growing at a tremendous pace. As of 2014, the number of Internet users worldwide stood at 2.92 billion people, up from 2.71 billion in 2013. [21]



Shifting the focus to India now, where the topic of net neutrality is still trending, there's been a rise in the mobile phone Internet user penetration share. From a statistic of 7% in 2012, a figure of 14.1% was attained in just two years. It is projected that in 2015, 17.4% of the total population in India will use mobile Internet, and this number will grow to about 25.2% by 2018.[21]



To sum it up, we can see that world is embracing internet like never before, which signifies its importance for the small business and start-ups to make their online presence vital. Without net neutrality all the innovation will take back seat and ideas will no longer be turned into reality resulting into crushed ambitions of millions of young entrepreneurs. Net Neutrality is of the utmost importance for small business owners, startups and entrepreneurs, who can simply launch their businesses online, advertise the products and sell them openly, without any discrimination on the basis of cost or speed. As India's vibrant entrepreneurial ecosystem is emerging, it would do well to understand the role of startups and create support for them to succeed with first and foremost requirement of providing them a fair playing field which is possible only through net neutrality.

A threat to Digital Marketing

Digital marketing is so powerful because the Internet has removed the middle man. Earlier, with traditional marketing medium; the evil media company was in the middle of the business owner and the customers. Business owners had to pay the media companies an advertising fee to reach the audience. The medias – TV, Radio, Newspaper and Magazines had access to the audience and they guarded it well. The Internet enabled the business owner to reach the customer directly for free using content marketing or at a very low cost using Marketing. Now the middle man wants to come back. This time it is not the media companies but the ISPs who control access to the audience. They are going to set the rules. With such an ecosystem only the people who already have the money will be able to have the reach they want. A group of 3-4 people wanting to innovate from a small room in Bangalore cannot

compete with the big giants. The playing field will not be level again. Without innovation from small timers, there is no competition. Without competition, there is no innovation in big companies. In the end, we will end up paying more for mediocre products and services and disruptive innovation which has been improving our lives will come to a grinding halt.

A threat to Digital India plan

Honorable Prime Minister Mr. Narendra Modi spoke extensively of his vision for Digital India, a program to transform India into digital empowered society and knowledge economy It would ensure that government services are available to citizens electronically. It would also bring in public accountability through directive delivery of government's services electronically. This will be for preparing the India for the knowledge based transformation and delivering good governance to citizens by synchronized engagement with both Central Government and State Government. Digital India's main objective is to provide an equal platform of opportunities and bringing citizens to same level by digitally connecting them and creating a digitally empowered society which can be possible only through unbiased internet.

The main ongoing highlights of Digital India campaign are: [22]

1. The programme aims to widespread the use of internet to each nook and corner of India by providing the coverage to 2.5 lakh Gram panchayats by the end of December 2016 and by turning 1.5 lakh post offices into multi-service centers. At the same time, it will be ensured that 2.5 lakh schools get facilitated with the free wifi services and there are web-based platforms to encourage "2-way communication" between government and public.
2. Mobile coverage is being provided for 42,300 remote villages of India for supporting the ongoing effort of increasing network coverage in the country and to fill the gaps.
3. The era of "e-governance" is being introduced with this campaign by implementing methods like "online applications and tracking", "use of online repositories", "use of Payment gateway platforms" and using IT to automate different government processes and reduce paper work.
4. Other small projects under this campaign which are being run are wi-fi in universities, free wi-fi spots at tourist centers and in cities with population greater than 1 million,etc.

The question arises, is all this possible without net neutrality???

As we can see that for all these objectives of "Digital India" campaign internet is the prime requirement. And internet without net neutrality is handicapped in fulfilling the above goals. The net neutrality can only ensure the success of "Digital India" drive. If all the 2.5 lakh Gram panchayats have the internet provision but they have to pay the price for accessing websites on it then what's the use of such facility

made available to them??? We have to ensure net neutrality so that each and everyone should be able to get benefitted from the internet services and be able to freely explore the world of internet for his use. Almost all of the above have net neutrality as their backbone. Digital India campaign depends on "high-speed" internet for its success as it is the core utility with which National Telecom Policy 2012 envision providing affordable and reliable broadband on demand by 2015 and 175 million broadband connections by 2017. A web economy that will enhances affordability and increased access and delivery of multiple services at reduce cost is not possible without a neutral internet.

CONCLUSION

Technology, in both its evolutionary form and in its revolutionary form, has changed our lives drastically. India is on the path of development wherein with the campaign like Digital India its image is being projected as one of the emerging superpower country in the world. Today there is much excitement and expectation about the advent of Digital India—a major initiative of the government to transform the country into a digitally empowered society—which is centered on three key areas of digital infrastructure as a utility to every citizen, governance and services on demand, and digital empowerment of citizens. However, where are we today? Voice connectivity is only about 60% and data penetration far lower at about 20%. Digital India is closely connected to Net Neutrality. Net neutrality can only ensure the fulfillment of the dream of Digital India which aims taking India forward on the path of development. Net neutrality framework promotes and protects the innovation. In recent times, some of the products and services that have transformed the way we live, such as Tablets, smart phones, the Internet, social media etc., have been a result of revolutionary innovation. Innovation is the backbone of start-ups and they are in turn one of the major role player in the development of Indian Economy. Net neutrality will facilitate Digital India plan.

REFERENCES

[1] The term coined by Columbia University media law professor Tim Wu in 2003, as an extension of the longstanding concept of a common carrier.

[2] Honan, Matthew (12 February 2008). "Inside Net Neutrality: Is your ISP filtering content?"

[3] Wu, Tim. "Network Neutrality FAQ"

[4] Wu, Tim (23 April 2005). "Network Neutrality, Broadband Discrimination"

[5] Complaints about restrictions on broadband applications like filesharing applications or VPNs are common on discussion forums like DSL Reports. See, e.g., BROADBAND REPORTS, at http://www.dslreports.com/forum/remark,3775421;mode=flat;root=sware (July, 2002)- Retrieved June 07, 2015.

[6] See Comments of the High Tech Broadband Coalition, In re: Inquiry Concerning High-Speed Access to the Internet Over Cable and Other Facilities (filed June 18, 2002), available at http://www.itic.org/policy/fcc_020618.pdf; see also FCC Ex Parte Letter, Aug. 22 2003, available at http://faculty.virginia.edu/timwu/wu_lessig_fcc.pdf.

[7] Wu, Tim (23 April 2005). "Network Neutrality, Broadband Discrimination"

[8] An independent U.S. government agency overseen by Congress, the commission is the United States' primary authority for communications law, regulation and technological innovation.

[9] https://www.fcc.gov/openinternet Retrieved on June 08, 2015

[10] "What Net Neutrality?". NDTV. 24 December 2014. Retrieved 24 December 2014.

[11] "What is net neutrality and why it is important". The Times of India. 20 January 2014. Retrieved29 September 2014.
[12] "Airtel drops plans to charge extra for internet voice calls". The Hindu. 29 December 2014. Retrieved1 January 2015.
[13] "TRAI seeks views on net-neutrality". The Hindu. 27 March 2015. Retrieved 27 March 2015. [14]"Consultation Paper On Regulatory Framework for Over - the - top (OTT) services" (PDF). Telecom Regulatory Authority of India. 27 March 2015. Retrieved 27 March2015.
[15] "Trai publishes email IDs of netizens, site hacked". Deccan Chronicle. 28 April 2015. Retrieved4 May 2015.
[16] "Union minister Ravi Prasad tweets about net neutrality, says committee to look into matter". DNA India. 8 April 2015. Retrieved 8 April 2015.
[17] "Airtel Zero: Another blow to net is net neutrality is only for airtel users..?/?neutrality". The Times of India. 6 April 2015. Retrieved 6 April 2015.
[18]The Net Neutrality Debate: Twenty Five Years after United States v. AT&T and 120 Years after the Act to Regulate Commerce Bruce M. Owen
[19]Subsidizing Creativity through Network Design: Zero-Pricing and Net Neutrality Journal of Economic Perspectives—Volume 23, Number 3—Summer 2009—Pages 61–76
[20] The Debate on Net Neutrality: A Policy Perspective Department of Decision and Information Sciences Warrington College of Business Administration University of Florida Gainesville, FL 32611-7169 U.S.A.
[21]Net Neutrality and its Impact on Startups | Emberify Blog
[22] http://www.youthkiawaaz.com/

Time Slice Protocol to Detect Node Replication Attack in Wireless Sensor Networks

A U Surya[1],Chinnaswamy C N[2],Kumar Swamy H S[3],Dr T H Sreenivas[4]

[1]B-E IV year, Department of Information Science and Engineering, The National Institute of Engineering, Mysore, Karnataka

[2]Associate Professor, Department of Information Science & Engineering, The National Institute of Engineering, Mysore, Karnataka

[3]B-E IV year, Department of Information Science and Engineering, The National Institute of Engineering, Mysore, Karnataka

[4]Professor, Department of Information Science and Engineering, The National Institute of Engineering, Mysore, Karnataka

ABSTRACT

The low-cost unshielded hardware components in unshielded sensor-networks nodes leave them vulnerable to certain security attacks. With the little effort, an attacker or adversary may capture a node's information, analyze and replicate them, insert these at strategic locations to further repeat the attack. The consequences of attacks allow network to corrupt the data and can make system crash. Previous node replication detection schemes include centralized detection which has single point failure drawback, or neighborhood voting protocols that fail to detect distributed replications. Also there are many location-based detection schemes which detect accurately except in the case of attacker strategizing a replicated node to be kept in the same location of the original node. To address these issues we have proposed a new protocol that is non- topological, time-slice based to distinguish the replicated nodes from the original ones. The protocol is also lightweight protocol which consumes sufficient power from the nodes.

Key Words:Lightweight, Replication, Same location, Time-slice,

1. INTRODUCTION

Wireless sensor nodes are useful in wide range of applications. They are deployed in various domains such as temperature and humidity sensing, battle surveillance, etc. Sensor nodes can easily scale to large configurations, since administrators can simply drop new sensors into the desired locations in the existing network. To join the network, new nodes neither require administrator intervention nor interaction with base station; instead, they initiate simple neighbor discovery by broadcasting their pre-stored credentials.

Unfortunately, sensor nodes are equipped with low-cost hardware components unprotected by physical shielding that could preclude access to sensor's memory, processing, sensing and communication components. Deploying unshielded nodes in a hostile environment may lead to arbitrary attacks by

adversaries to capture, replicate and insert duplicate nodes at chosen network location effortlessly. Thus if, adversaries even capture a single node, they can replicate it indefinitely, spreading influence throughout the network. If left undetected there may be various dangerous attacks possible. With the help of already replicated nodes adversaries can further subvert the data aggregation by injecting false data or suppressing legitimate data. Further the replicated nodes can trigger the disconnection of legitimate nodes by calling the node-revocation protocols indefinitely.

We discuss, compare the protocols existing system and its limitations which should be rectified and implemented newly in the proposed protocol, in subsequent sections. We also provide a detailed explanation about the supporting existent protocols needed for cluster head selection, which we use to implement in our system.

2. EXISTING SYSTEM

There are numerous centralized and distributed protocols to detect node replication in sensor nodes. Here, in this section we discuss them with working and its listed limitations.

2.1. Centralized Detection:

The most straightforward detection scheme is centralized approach [1]. Each sensor node sends a list of its neighbors and its location claims to the base station. The base station can then assess and examine the sent claims of every node to find the replicated entries of claims. If it discovers the replicas, then it will revoke the replicated nodes by flooding the network with an authenticated revocation message.

While conceptually simple, this approach suffers from severe drawbacks inherent in a centralized system. First the base station becomes single point of failure. Any compromise of the base station will render the protocol useless. Second, the routing load will be more on the nodes in vicinity of base station, thus these become attraction of adversaries for the attack.

2.2. Nodes-to-Network Broadcasting

One approach to distributed system utilizes a simple broadcast protocol. [2][4] Each node in the network uses an authenticated broadcast message to flood the network with its location information for its neighbors and if it receives a conflicting claim, revokes the offending node. This protocol ensures 100% detection of all duplicate location claims under the assumption that broadcasted message always reaches every node. However when adversaries somehow manage to jam the key areas of message delivery, this protocol fails. Nodes could employ redundant messages or authenticated acknowledgment techniques to thwart such attacks.

2.3. Deterministic multicast

Previous protocols send claims to all of the nodes in the network .However this protocol describes an improved method to detect replicated nodes. Instead of sending broadcasting claims to every node, the claims are only sent to limited subset of "witness" nodes. When a node broadcasts its claim, its neighbors forward the location claims to subset of nodes called witness nodes. The witness nodes are chosen as a function of the node's ID. If the adversary replicates a node, the witness will receive two different location claims for the same node ID. The conflicting location claims become evidence for the trigger of node- revocation protocol. The disadvantage of deploying the protocol is that the selections of witness nodes are not random. Hence if the adversary can guess the same and could jam the broadcasted claims [2], then the protocol fails.

2.4. Randomized multicast

To improve the resiliency of the deterministic multicast protocol discussed in section 2.3, a new protocol that randomizes the witnesses of a given node's location claim [3], so that the adversary cannot replicate their identities. When a node announces its location, each of its neighbors sends a copy of the location claim to a set of randomly selected witness nodes. If the adversary replicates a node, then two sets of witness nodes will be selected. In a network of n nodes, if each location produces $\sqrt{n}$ witnesses, then the birthday paradox predicts at least one collision with high probability, i.e., at least one witness will receive a pair of conflicting location claims which is sufficient to initiate node- revocation protocol.

2.5. Line-selected Multicast

Communication overhead is the main drawback of previous multicast protocols. To overcome, [1] Bryan Parno came up with a different scheme to detect conflicting claims. We note that nodes in sensor network are both sensing units and routers. For a location claim to travel from node A to node B, it must pass through several intermediate nodes as well. If these intermediate nodes also store location claims, then we have effectively drawn a line across the network. If a conflicting claim ever crosses the line, then the node at the intersection will detect the conflict and initiate a revocation broadcast.

3. PROPOSED SYSTEM

In our proposed system, in this section we primarily describe how the clusters are selected out of field of sensor units by explaining specific protocol for cluster-head selection and then we concentrate on explaining our protocol for detection of replicated nodes. We also examine the advantages and limitations of the same. Below in this section we list the section/phases of our system.

The phases of detecting a node replication are:

1) Cluster-head selection
2) Node authentication
3) Node Replication Detection

3.1. Cluster-head selection

The cluster-head selection is significant process where energy ought to be balanced in order to prevent draining out of power by cluster head nodes. Hence the replication protocol gets backed by sufficient power.

Recent protocols for cluster head selection are based on probabilistic model so that there are very fair chances of every node in network becoming cluster-heads in its lifetime. One such protocol is LEACH [7] (Low-Energy Adaptive Cluster Head selection) which below we adapt its improved version called LEACH-TLCH [7],[8] protocol which is more energy-balanced protocol. Below here, we intend to explain in brief the LEACH and its improved LEACH-TLCH protocols.

3.1.1. LEACH

Low-energy adaptive cluster head selection protocol is energy efficient. LEACH protocol uses round as unit, each round is made up of cluster set-up stage and steady-state stage, for the purpose of reducing unnecessary energy costs, the steady state stage must be much longer than the set-up stage. The process of it is shown in following figure.

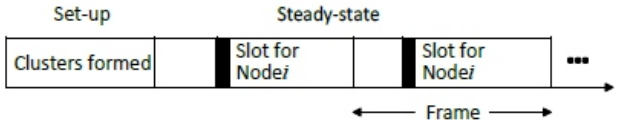


Fig.1 LEACH Protocol process.

At the stage of cluster forming, a node randomly picks a number between 0 to 1, compared this number to the threshold values t (n), if the number is less than t (n), then it becomes cluster head in this round, else it become common node. Threshold t (n) is determined by function expressed below

$$t\,n = \begin{cases} \dfrac{p}{1 - p * r \bmod \frac{1}{p}} & if\ n \in G \\ 0 & if\ n \notin G \end{cases}$$

Where p is the percentage of the cluster head nodes in all nodes, r is the number of the round; G is the collections of the nodes that have not yet been head nodes in the first 1/P rounds. Using this threshold, all nodes will be able to be head nodes after 1/P round s. The analysis is as follows: Each node becomes a cluster head with probability p when the round begins, the nodes which have been head nodes in this

round will not be head nodes in the next 1/P rounds, because the number of the nodes which is capable of head node will gradually reduce, so, for these remain nodes, the probability of being head nodes must be increase d. After 1/P-1 round, all nodes which have not been head nodes will be selected as head nodes with probability 1, when 1/P rounds finished, all nodes will return to the same starting line.

When clusters have formed, the nodes start to transmit the inspection data. Cluster heads receive data sent from the other nodes, the received data was sent to the gateway after fused. This is a frame data transmission. In order to reduce unnecessary energy cost, steady stage is composed of multiple frames and the steady stage is much longer than the set-up stage.

3.1.2. LEACH-TLCH (Improved LEACH)

Although the LEACH seems balanced, it does not account a node's energy to consideration. Hence, if a low energy node has a probability of being cluster head same as the node which has very high energy then there might be fast drain of remnant energy in the CH and affects network performance. Improved version of this, LEACH-TLCH considers two factors to balance energy in the network. There would be a selection of secondary CH. Now the data aggregation, data fusion functions are assigned to the secondary CH. The only work of primary CH is to transfer the data to BS.

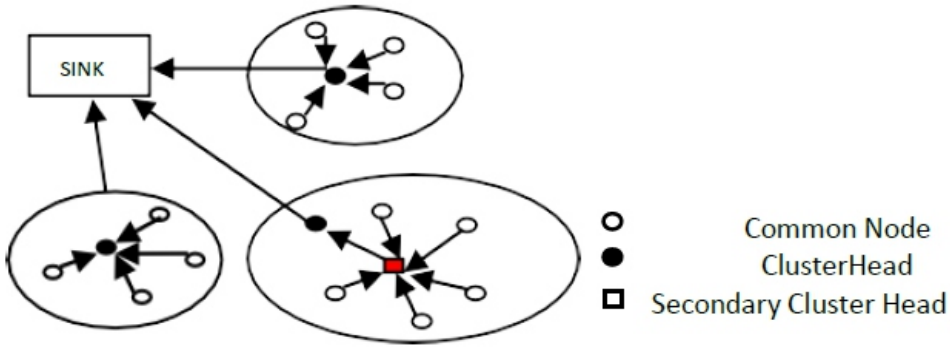


Fig.2 Push Mechanism

However the secondary CH is not chosen for every cluster. The basis for selection is,

1) If in the cluster the current energy E_{cur}<E_{avg}, the average energy of all nodes in the cluster, then secondary CH is chosen.
2) If in the cluster the distance of CH from BS, d >d , the average distance of all the nodes in the cluster to BS, then secondary CH is chosen.

3.2. Node Authentication

Since this protocol is making use of energy based LEACH(3.1.2) the cluster head will be keep on changing and the cluster will have to be reformed every time. This might cause a serious trouble, the

attacker may attack the network at the time of cluster formation and capture a node and replicate it. So to avoid this we use node authentication.

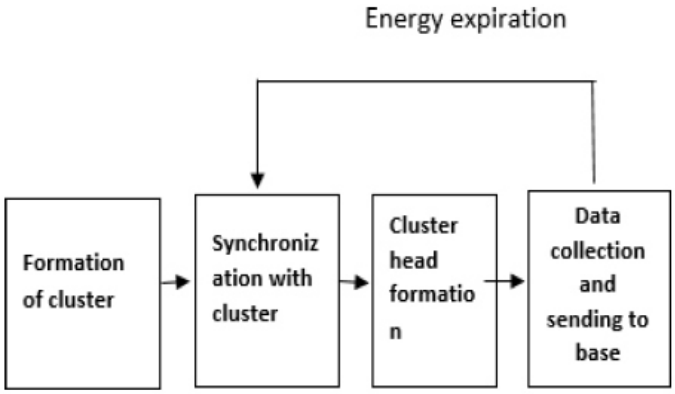


FIG 3 Network operation of cluster sensor network

FIG 4 Three steps of secure cluster formation

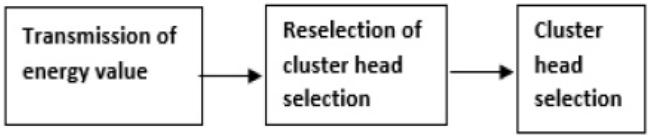


FIG 5 Three steps of secure CH selection

Node authentication works as shown in FIG 3, first the cluster will be formed, then the synchronization of each cluster node will take place, third step would be the selection of cluster head, and final step is collecting the data from each node and sending it to the base station. This will continue until the energy level of CH comes down to the level of average energy level of the cluster. Once this happens the CH will be re-elected and the same procedure continues [6].

3.3. Node Replication Detection

3.3.1. The Algorithm

The Detection phase consists of our protocol which works in the case when the adversary puts the replicated protocol in the same place of original node. Here below we describe the data flow when the detection phase starts.

Assumptions:

Node Deployment: The node deployment actually is application dependent. But here we assume that the nodes are deployed deterministically where the sensors are manually placed and data is routed through pre-determined paths.

Data Reporting Model: Data sensing and reporting in sensor networks is dependent on the application and time criticality of the data reporting. We consider that data reporting here is time driven assuming the application requires periodic data monitoring.

Working:

Initially all nodes of each cluster are time synchronized and the order in which the nodes should send the data is stored in cluster head for verification. The nodes of each cluster get ready to send data according to the order established. The first node sends data to cluster head for a specific time interval and if it doesn't have data it just sends the acknowledgement containing the node ID and cryptographic keys and waits for the interval to complete. During the time when data is pushed by node to cluster head the cluster head checks if the node id is matching the specific node ID present in the order. If there is any mismatch in the Id present in the order queue stored, that particular node will be blacklisted and reported to base station.

A new order is established by cluster head after elimination of the blacklisted nodes which could have been replicated. For understanding purpose let's assume that the next node in the order will occupy the position of the replicated node in the order. Then the next node pushes and the entire procedure is repeated periodically. When the cluster head's power is down to minimum level, the leach protocol [7] selects a new cluster head and the order is copied to the new head.

The protocol works because for any adversary to replicate a node in the sensor network, it takes a lot of time which is enough to detect the replicated node.

Node replication Schemes: The following example shows the various scenarios as in which our protocol detects a replication.

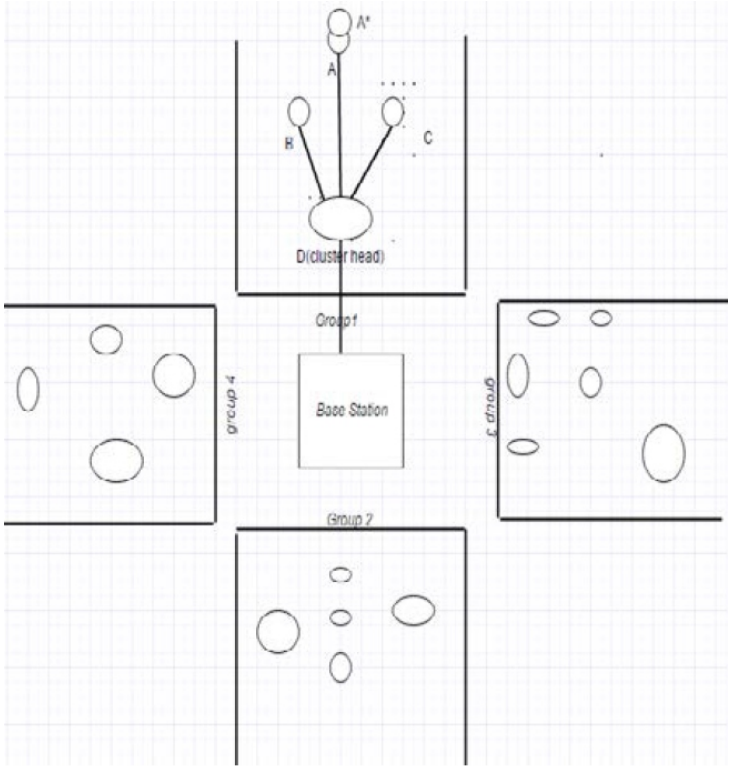


Fig.6 Sample Node Environment

Data sending order established in cluster head of Group 1 is (B-A-C).The replicated node of A is A* which is kept by adversary at the same location of node A. Each node sends data for 5minutes. (Time Slice).

The safe case when there is no replicated node detected is when each of nodes sends data for 5minutes according to the order.

B (0-5) A (5-10) C (10-15)

Replication detection cases:

In the following cases the node is revoked and blacklisted:

1. B (0-5) A(5-10) A(10-12)

After 10 minutes A again sends the data hence it is blacklisted because at that time it's C's turn to send the data.

2. B (0-5) A(5-10) C(10-15) A

After 15minutes node B should send the data instead A is sending. Hence A is blacklisted because originally B should have sent the data.

3. B (0-3) A(4)

Node A should have started sending data after 5th minute. But it started sending at 4th minute.

4. B (0-5) C(10-15)

Node A is not available from 5- 10th minute so it is either down or been compromised for replication hence it is blacklisted.

One of the advantages of the protocol includes no need of time synchronization frequently. By selecting the cluster head there is a decrease in a communication overhead. Since push mechanism is followed by the nodes cluster head power consumption is decreased.

The random selection of node by adversary may lead to the selection of cluster head though the probability is less. This protocol fails when the location of the replicated node is kept somewhere else than the original place in which case any of the previously mentioned protocols can be used to detect the replicated node.

4. CONCLUSION

By the end we look to conclude with the detection algorithm, advantages and limitations of the protocol. Certainly the advantage is that the protocol is a lightweight one and also the attacker cannot hide replicated node at the same location of the original node. But the cost of clock synchronization of nodes requires sufficient energy from nodes. Also the time- slice must be optimum such that no attacker sneaks to replicate between the set-up phases. The protocol is feasible when there are large numbers of sensor nodes which cannot be monitored by simple, location based ones.

5. REFERENCES

[1] B. Parno, A. Perrig, and V. Gligor, "Distributed detection of node replication attacks in sensor networks," in Proceedings of the IEEE Symposium on Security and Privacy (IEEE S and P '05), pp. 49–63, May 2005.

[2] M. Conti, R. D. Pietro, and L. V. Mancini, "A Randomized, Efficient, and Distributed Protocol for the Detection of Node Replication Attacks in Wireless Sensor Networks," In Proc. of ACM MobiHoc, September 2007.

[3] Suvarna Game, Mr. ChandrashekharRaut –" Protocols for Detection of Node Replication Attack", IOSR Journal of Computer Engineering (IOSR-JCE) e-ISSN: 2278-0661, p- ISSN: 2278-8727Volume 16, Issue 1, Ver. II (Jan. 2014), PP 01-11

[4] MoirangthemMarjit Singh, Ankita Singh and Jyotsna Kumar Mandal – "Towards Techniques of Detecting Node Replication Attack in Static Wireless Sensor Networks ", International Journal of Information and Computation Technology. ISSN 0974-2239 Volume 4, Number 2 (2014), pp. 153-164

[5] Yu-Shen Ho, Ruay-Lien Ma, Cheng-En Sung, I-Chen Tsai, Li-Wei Kang, Chia-Mu Yu – "Deterministic Detection of Node Replication Attacks in Sensor Networks",2015 International Conference on Consumer Electronics-Taiwan (ICCE-TW).

[6] K.Ramesh and Dr. K.Somasundaram – "A ComparitiveStudy ofClusterhead Selection Algorithms In Wireless Sensor Networks",International Journal of Computer Science & Engineering Survey (IJCSES) Vol.2, No.4, November 2011.

[7] Chunyao FU, Zhifang JIANG, Wei WEI and Ang WEI, -"An Energy Balanced Algorithm of LEACH Protocol in WSN", IJCSI International Journal of Computer Science Issues, Vol. 10, Issue 1, No 1, January 2013 ISSN (Print): 1694-0784 | ISSN (Online): 1694-0814

[8] LalitaYadav, Ch. Sunitha – "Low Energy Adaptive Clustering Hierarchy in Wireless Sensor Network (LEACH) ",LalitaYadav et al, / (IJCSIT) International Journal of Computer Science and Information Technologies, Vol. 5 (3) , 2014, 4661-4664.

Instructions for Authors

Essentials for Publishing in this Journal

1 Submitted articles should not have been previously published or be currently under consideration for publication elsewhere.

2 Conference papers may only be submitted if the paper has been completely re-written (taken to mean more than 50%) and the author has cleared any necessary permission with the copyright owner if it has been previously copyrighted.

3 All our articles are refereed through a double-blind process.

4 All authors must declare they have read and agreed to the content of the submitted article and must sign a declaration correspond to the originality of the article.

Submission Process

All articles for this journal must be submitted using our online submissions system. http://enrichedpub.com/ . Please use the Submit Your Article link in the Author Service area.

-

Manuscript Guidelines

The instructions to authors about the article preparation for publication in the Manuscripts are submitted online, through the e-Ur (Electronic editing) system, developed by **Enriched Publications Pvt. Ltd**. The article should contain the abstract with keywords, introduction, body, conclusion, references and the summary in English language (without heading and subheading enumeration). The article length should not exceed 16 pages of A4 paper format.

Title

The title should be informative. It is in both Journal's and author's best interest to use terms suitable. For indexing and word search. If there are no such terms in the title, the author is strongly advised to add a subtitle. The title should be given in English as well. The titles precede the abstract and the summary in an appropriate language.

Letterhead Title

The letterhead title is given at a top of each page for easier identification of article copies in an Electronic form in particular. It contains the author's surname and first name initial .article title, journal title and collation (year, volume, and issue, first and last page). The journal and article titles can be given in a shortened form.

Author's Name

Full name(s) of author(s) should be used. It is advisable to give the middle initial. Names are given in their original form.

Contact Details

The postal address or the e-mail address of the author (usually of the first one if there are more Authors) is given in the footnote at the bottom of the first page.

Type of Articles

Classification of articles is a duty of the editorial staff and is of special importance. Referees and the members of the editorial staff, or section editors, can propose a category, but the editor-in-chief has the sole responsibility for their classification. Journal articles are classified as follows:

Scientific articles:

1. Original scientific paper (giving the previously unpublished results of the author's own research based on management methods).

2. Survey paper (giving an original, detailed and critical view of a research problem or an area to which the author has made a contribution visible through his self-citation);

3. Short or preliminary communication (original management paper of full format but of a smaller extent or of a preliminary character);

4. Scientific critique or forum (discussion on a particular scientific topic, based exclusively on management argumentation) and commentaries. Exceptionally, in particular areas, a scientific paper in the Journal can be in a form of a monograph or a critical edition of scientific data (historical, archival, lexicographic, bibliographic, data survey, etc.) which were unknown or hardly accessible for scientific research.

Professional articles:

1. Professional paper (contribution offering experience useful for improvement of professional practice but not necessarily based on scientific methods);
2. Informative contribution (editorial, commentary, etc.);
3. Review (of a book, software, case study, scientific event, etc.)

Language

The article should be in English. The grammar and style of the article should be of good quality. The systematized text should be without abbreviations (except standard ones). All measurements must be in SI units. The sequence of formulae is denoted in Arabic numerals in parentheses on the right-hand side.

Abstract and Summary

An abstract is a concise informative presentation of the article content for fast and accurate Evaluation of its relevance. It is both in the Editorial Office's and the author's best interest for an abstract to contain terms often used for indexing and article search. The abstract describes the purpose of the study and the methods, outlines the findings and state the conclusions. A 100- to 250-Word abstract should be placed between the title and the keywords with the body text to follow. Besides an abstract are advised to have a summary in English, at the end of the article, after the Reference list. The summary should be structured and long up to 1/10 of the article length (it is more extensive than the abstract).

Keywords

Keywords are terms or phrases showing adequately the article content for indexing and search purposes. They should be allocated heaving in mind widely accepted international sources (index, dictionary or thesaurus), such as the Web of Science keyword list for science in general. The higher their usage frequency is the better. Up to 10 keywords immediately follow the abstract and the summary, in respective languages.

Acknowledgements

The name and the number of the project or programmed within which the article was realized is given in a separate note at the bottom of the first page together with the name of the institution which financially supported the project or programmed.

Tables and Illustrations

All the captions should be in the original language as well as in English, together with the texts in illustrations if possible. Tables are typed in the same style as the text and are denoted by numerals at the top. Photographs and drawings, placed appropriately in the text, should be clear, precise and suitable for reproduction. Drawings should be created in Word or Corel.

Citation in the Text

Citation in the text must be uniform. When citing references in the text, use the reference number set in square brackets from the Reference list at the end of the article.

Footnotes

Footnotes are given at the bottom of the page with the text they refer to. They can contain less relevant details, additional explanations or used sources (e.g. scientific material, manuals). They cannot replace the cited literature.
The article should be accompanied with a cover letter with the information about the author(s): surname, middle initial, first name, and citizen personal number, rank, title, e-mail address, and affiliation address, home address including municipality, phone number in the office and at home (or a mobile phone number). The cover letter should state the type of the article and tell which illustrations are original and which are not.

Global Journal of Networks and Applications

SUBSCRIPTION FORM

SUBSCRIPTION PRICES

India	Institutional	Individual
Print	3000 INR ☐	2000 INR ☐
Print + Online	3000 INR ☐	3000 INR ☐
Online	1500 INR ☐	800 INR ☐

Rest of the world	Institutional	Individual
Print	300 USD ☐	200 USD ☐
Print + Online	400 USD ☐	300 USD ☐
Online	200 USD ☐	150 USD ☐

Contact Person : _____

Designation: _____

Institution Name:_____

Address :_____

_____

City : _____ Pin : _____State :_____

Tel : _____Fax : _____ Email :_____

PAYMENT OPTIONS

☐ Cheque / DD is enclosed in favour of **" Apex Subscription Pvt. Ltd."** Payable at Mumbai.

Amount : _____

Cheque / DD No : _____ Dated : _____ Drawn on Bank

_____

☐ **NEFT / RTGS :**

Beneficiary Name : Apex Subscription Pvt. Ltd.

Bank Name : HDFC Bank Ltd, BRANCH : Goregaon (East),

Bank A/C No : 02122320004035, IFSC Code: HDFC0000212

Note : For more subscription detail follow the link www.apexsubs.com

Editorial Office
Enriched Publications Pvt. Ltd
S-9, IInd Floor Above Federal Bank,
Plot No-5, Sector-5, Dwarka, New Delhi- 110075,
Phone: - + (91)-(11)-47026006
Email : info@enrichedpublications.com
Website : www.enrichedpub.com

Subscription Manager
APEX SUBSCRIPTION PVT LTD.
304, De-Elmas, Sonawala Cross Road 2,
Goregaon (East) Mumbai - 400063.
Tel : +91-022-26853114/5 Fax : 022-26853116
Email : enquiry@apexsubs.com
Website : www.apexsubs.com