Journal of Electronic and Optical Communication

Volume No. 9

Issue No. 1

January - April 2025

ENRICHED PUBLICATIONS PVT.LTD

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

Journal of Electronic and Optical Communication

Aims and Scope

Journal of Electronic and Optical Communication is a journal that publishes original research papers in the fields of Electrical and Electronic Engineering and in related disciplines. Areas included (but not limited to) are electronics and communications engineering, electric energy, automation, control and instrumentation, computer and Advanced technology, and the electrical engineering aspects of building services and aerospace engineering, Journal publishes research articles and reviews within the whole field of electrical and electronic engineering, new teaching methods, curriculum design, assessment, validation and the impact of new technologies and it will continue to provide information on the latest trends and developments in this ever expanding subject.

Journal of Electronic and Optical Communication

Journal of Electronic and Optical Communication

(Volume No. 9, Issue No. 1, January - April 2025)

Contents

Amplification in Optical Fibers by Rare Earth Doping

Asad Ali Khan[1], V. K. Sharma[2], Anil Kumar[3*]

[1]Department of Physics,, Teerthanker Mahaveer University, Moradabad (U.P.)

[2] Department of Physics, K.G.K. College, Moradabad (U.P.)

[3]Department of Physics, Hindu College, Moradabad (U.P.)

A B S T R A C T

An overview of the fundamental physical process responsible for optical amplification in Raman fiber amplifiers and in rare earth doped (thulium-doped and erbium- doped) fiber amplifiers, is discussed. We formulate basic equations governing optical amplification for each of the two types of amplifiers and define the important parameters used for performance characterization of these amplifiers. This paper outlines the method used in doped fiber amplifiers.

Keywords: Raman amplifier, Fiber, Spectral variation, Rare earth doping.

1. INTRODUCTION

Raman amplification takes place by the process of stimulated Raman scattering (SRS) which involves frequency shifting of an incident optical beam because of interaction having higher frequency vibration modes of a material. In process of Raman scattering, a photon of frequency $v_q = v_p + \Omega$.

The photons shifted upward and downward are called Stokes and anti-Stokes photons respectively. Anti-Stokes scattering requires the molecule to be in the excited state; that is, it requires the presence of a phonon frequency Ω. The phonon population;

$$n\,\Omega = \frac{1}{e^{h\,\Omega/K_B T} - 1} \qquad (1.1)$$

Where k_B is the Boltzmann constant; h is Planck's constant and T is the absolute temperature in degree Kelvin. Therefore at room temperature; the probability of anti – Stokes emission is much lower than that of stokes emission. Another important aspect of Raman scattering is that since it involves optical phonons with frequencies close to the maxima in the dispersion curve, the momentum conservation condition gets automatically satisfied [1]. Therefore; unlike Brillouin scattering, Raman scattering is described in terms of energy levels where an incident photon at frequency v_p excites a molecule up to a virtual level (non-resonant state) and the molecule decays almost instantaneously (~ femtoseconds) to a lower vibrational/rotational energy level, emitting a photon at frequency $v_s = v_p - \Omega$.

The difference between energy of incident and stokes photons is dissipated by the molecular vibrations of the host material. The presence of signal at Stokes-shifted frequency stimulates the conversion of pump photons into Stokes photons, and the process is termed as stimulated Raman scattering (SRS). SRS is a coherent process and it leads to the amplification of the signal. Raman gain exists in every molecular medium and the vibrational energy levels of the material determine the frequency shift $*\Delta\Omega = v_p - v_s\ (\mathrm{Hz}) = \frac{1}{\lambda_p} - \frac{1}{\lambda_s}\ (\mathrm{m}^{-1})]$ and shape of the Raman gain curve. To achieve Raman amplification in optical fibers, a high power pump wave is co-launched with the signal (having frequency corresponding to Stokes shift), and energy transfer from the pump wave to the signal Stokes wave, through Raman scattering, amplifies the signal.

2. RAMAN AMPLIFIERS IN OPTICAL FIBER COMMUNICATION

Raman amplifiers can be typically used in two of configurations-distributed Raman amplifier, where the transmission fiber itself is used as a gain medium and discrete Raman amplifier, which employs specialty fiber (DCF or specially designed high Raman gain fiber) for amplification. The characteristics make DRAS more suitable for higher bit rates and solution transmissions.

Raman amplifiers are used in conjunction with EDFA (hybrid Raman-EDFA Configuration) to improve noise performance or to increase optical gain band width of EDFAS. A typical DAR link consists of around 100 km standard transmission fiber pumped by a total power of about 1 W. Raman gain spectrum is highly non-fiat, and the conventional technique to flatten by using multiple pumps (with proper wavelengths / power), so that the overall gain spectrum (a superposition of the gain spectrum corresponding to each of the pump) is flat. This is a tedious technique and requires rigorous numerical computation to find out the optimum distribution of pump. Figure 1 shows the spectrum for a DRA based on 50 km long G.652 fiber link carrying simultaneously launched 1 nm spaced signal channel (1520-1600 nm) with input power of - 3 dbm per channel and signal-pumped by 700 mW power at 1480 nm. Here, we have taken typical spectral change in background attenuation [6] for standard transmission fiber.

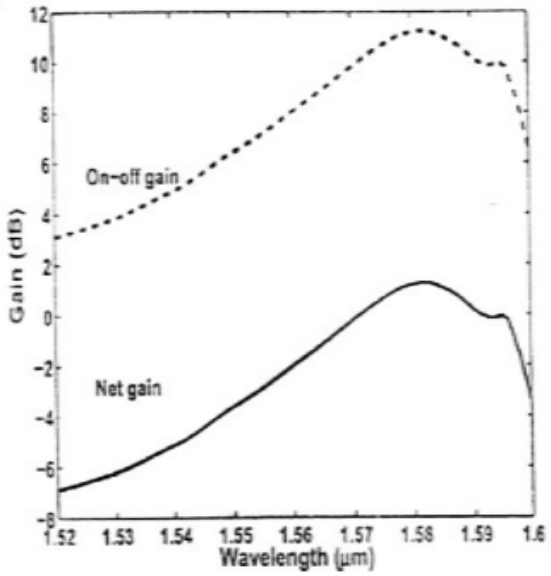


Fig. 1: Gain spectrum in a single pump DRA

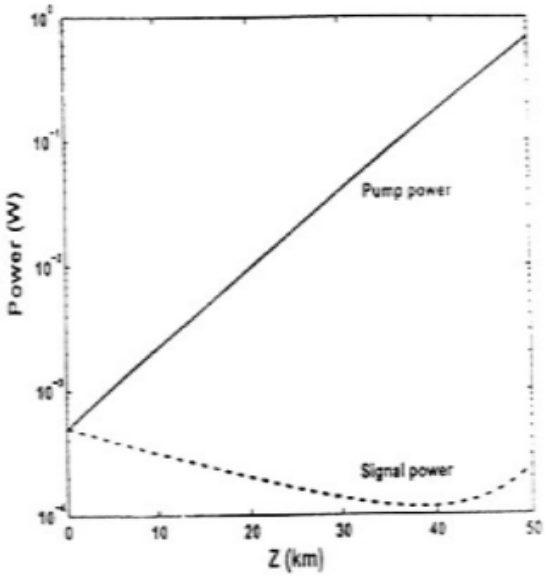


Fig. 2: Pump and signal power in a backward pumped DRA

Attenuation at pump wavelength is taken to be 0.3 dB/km\. Figure 2 shows the pump and signal evolution along the fiber length z, for 1550 nm signal wavelength. The OSNR for all wavelengths is found to be greater than 40 dB with negligible effect of DRS noise. The gain ripple in the presented case is about ±4 dB. It has been shown in literature [6] that for such a system a net gain of (0 ± 0.08) B can be obtained by 16 pumps at suitable wavelength and pump power. Here, one must note that the number of pump used is directly related to the gain flatness, and longer is the span length (i.e. more is the required on-off gain), lesser the flat- gain bandwidth, or equivalently, more is the number of pumps required for obtaining same gain – bandwidth [7]. We have verified the accuracy of our simulations by comparing the results with those in standard literature. The model is capable of handling bi-directional multiple pump, multiple signals, ASE and Rayleigh noise depending on the complexity of the problem, 5-20 iteration are generally required to obtain a convergent solution with an accuracy better than ±0.001db in signal gain.

3. ATOMIC RATE EQUATIONS FOR THREE LEVEL SYSTEM

The energy levels of the doped fiber amplification schemes-EDFA and L- band TDFA can be represented by a three level system. The various transitions in a three level system are shown in Fig. 3. R13 and R31 represent the stimulated absorption and stimulated emission rates for the pump between levels 1 and 3.

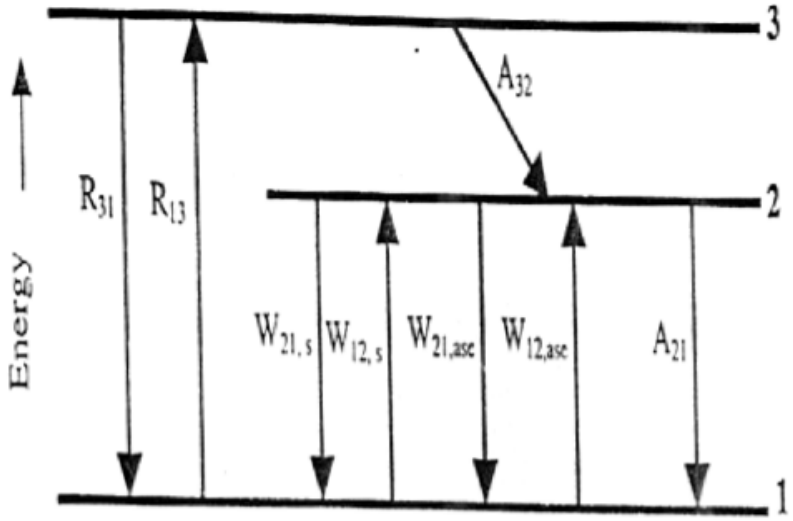


Fig. 3: Various transition processes in a three level system

In efficient amplification schemes, level 3 is usually characterized by a short lifetime (~ few micro-seconds), so the atoms rapidly decay (decay rate A32) to level 2 causing build up of a population inversion between levels 1 and 2. The stimulated emission and absorption rates between level 1 and 2 are denoted by W_{12i} and W_{21i} respectively where the subscript i = s, are stands for signal or ASE respectively. Spontaneous emission rate from level 2 to 1 is denoted by $A_{21} = 1/T$, where T is the fluorescence time interval of level of 2. Let pd be the total doped ion density and N_1,N_2 and N_3 are the population densities of level 1, 2 and 3 respectively, so that $pd = N_1 + N_2 + N_3$. The atomic rate equations for the three levels can them be written as:

$$\frac{dN_1}{dt} = -R_{13}N_1 + R_{31}N_3 - W_{12,S}N_1 + W_{21,S}N_2 + A_{21}N_2 - W_{12,ase}N_1 + W_{21,ase}N_2 \qquad (3.1)$$

$$\frac{dN_2}{dt} = W_{12,S}N_1 - W_{21,S}N_2 - A_{21}N_2 + A_{32}N_3 + W_{12,ase}N_1 - W_{21,ase}N_2 \qquad (3.2)$$

$$\frac{dN_3}{dt} = R_{13}N_1 - R_{31}N_3 - A_{32}N_3 \qquad (3.3)$$

In steady state, the populations of various levels are time independent, That is $dN_1/dt = 0$ (i=1,2,3) where it is assumed that the non-radiative decay rate A_{32} dominates over the pumping rates R_{13} and R_{31}, that is, $A_{32} >> R_{13,31}$, equations 3.1- 3.3 can be solved for N_1 and N_2, to yield:

$$N_1 = P_d \frac{W_{21,s} + A_{21} + W_{21,ase}}{R_{13} + W_{12,} + W_{12,ase} + A_{21} + W_{21,s} + W_{21,ase}} \qquad (3.4)$$

$$N_2 = P_d \frac{R_{13} + W_{12,} + W_{12,ase}}{R_{13} + W_{12,s} + W_{12,ase} + A_{21} + W_{21,s} + W_{21,ase}} \qquad (3.5)$$

If the pumping rate R13 is high enough such that N2>N1, then population inversion is said to be achieved and the gets amplified.

We have described the doped fiber in a polar cylindrical co-ordinate system (r, Ø, z). We denote the emission and absorption cross-section at frequency v_k by σ_{ek} and σ_{ak} respectively. The subscript k can take values s, p corresponding to the signal and pump respectively. The emission and absorption rates at signal frequency vs, at any point (r, Ø, z) in the fiber are proportional to the signal intensity Is (r, Ø, z) as follow:

$$W_{21,} = \frac{\sigma_{es}\, I_s}{h v_s} \quad \text{and} \quad W_{12,s} = \frac{\sigma_{es}\, I_s}{h v_s} \tag{3.6}$$

The pumping rate R_{13} at pump frequency v_p and intensity I_p (r, Ø, z) is given by:

$$R_{13} = \frac{\sigma_{ap}\, I_p}{h v_p} \tag{3.7}$$

The emission and absorption rates for the ASE are given by:

$$W_{12,ase} = \left[\int_0^{\infty} \frac{\sigma ak}{hvk} Sas(vk, z)\right] f_s^{lm}(r,\emptyset) \tag{3.8}$$

$$W_{21,ase} = \left[\int_0^{\infty} \frac{\sigma ak}{hvk} Sas(vk, z)\right] f_s^{lm}(r,\emptyset) \tag{3.9}$$

Where, S_{ase} (v_k,z) is the ASE spectral power density, since the ASE power in a unit frequency interval around frequency vk at position z. ASE power is generated over a continuum of frequencies spanning the entire gain spectrum and therefore the contribution to emission and absorption rates involve an integral over frequency. f_s^{lm} (r,Ø) represents the square of the transverse mode field profile in a fiber and has units of area -1; lm stands for the L P_{lm} mode in the fiber.

$$\int_0^{\infty}\int_0^{2\pi} f_k^{lm}(r,\emptyset)dr = 1 \tag{3.10}$$

The effective indices and mode field profile for any arbitrary refractive index profile have been obtained using matrix method.

4. PROPAGATION EQUATIONS

When a light beam of intensity I at frequency v_k traverses an amplifier of infinitesimal thickness dz, the change in the intensity is given by:

$$dI(z) = [\sigma_{ek}N_2 - \sigma_{ek}N_1]\, I\,(z)dz \tag{4.1}$$

We assume a homogeneously broadened amplifying medium where the ions are characterized by identical cross-sections at any point in the medium. The optical power P_k (z) at frequency v_k can be related to the intensity I_k through:

$$I_K(r,\emptyset,z) = p_k(z)\, f_k^{lm}(r, \emptyset) \tag{4.2}$$

Integrating Eqn. 4.2 over r and Ø, we obtain the rate of change of optical power with propagation distance z:

$$\frac{dp_{k\,z}}{dz} = p_k(z)\int_0^{\infty}\int_0^{2\pi}[\sigma_{ek} N_2 - \sigma_{ak}]f_k^{lm}(r, \emptyset)\, r\, dr\, d\emptyset \tag{4.3}$$

Here k = p, s refer to pump and signal respectively. This equation can be rewritten as:

$$\frac{dp_k}{dz} = [\gamma_e(vk, z) - \gamma_a(vk, z)_k(z) \tag{4.4}$$

$$\gamma_e(vk, z) = \sigma_{ek}\int_0^{b}\int_0^{2\pi} N_2\, f_k^{lm}(r, \emptyset)\, rdrd\emptyset \tag{4.5}$$

$$\gamma_a(vk, z) = \sigma_{ak}\int_0^{b}\int_0^{2\pi} N_1\, f_k^{lm}(r, \emptyset)\, rdrd\emptyset \tag{4.6}$$

with a and b being the inner and outer radii of the doped region. The rate equation governing propagation of forward and backward ASE is given by:

$$\frac{d\,S_{ase}^{\pm}}{dz} = \pm 2h\nu\Delta\nu\ \gamma_e\ (\nu,z) \pm [\quad (\nu k,z) - \gamma\ (\nu k,z)]S \qquad (\nu,z) \qquad (4.7)$$

where the first term on the RHS corresponds to the amplification of spontaneous noise equivalent to one fictitious input photon per mode in bandwidth Δν. The factor of 2 signifies generation of spontaneous noise in both polarization modes.

We have verified the validity of our simulations by comparing the result for a standard EDFA with those published in literature [8]. We consider a step-index fiber with numerical aperture of 0.2 and cutoff wavelength as 800 nm, doped with erbium ions (uniform concentration of 1.0 × 1024 m-3) in the core region. The absorption and emission scattering cross-sections refer to a Ge/Al/P-silica fiber. The radial variation of population density and erbium concentration as well as the transition rates and the modal intensities are considered at 40 points within the erbium-doping radium, and the spatial overlap integrals are solved numerically using these 40 points.

Figure 4 shows the variation of gain at 1532 and 1552 nm for different fiber lengths. A 50 mW pump at 980 nm wavelength and a single signal channel with 0.1 μW of power is considered to be co-directionally launched into the fiber.

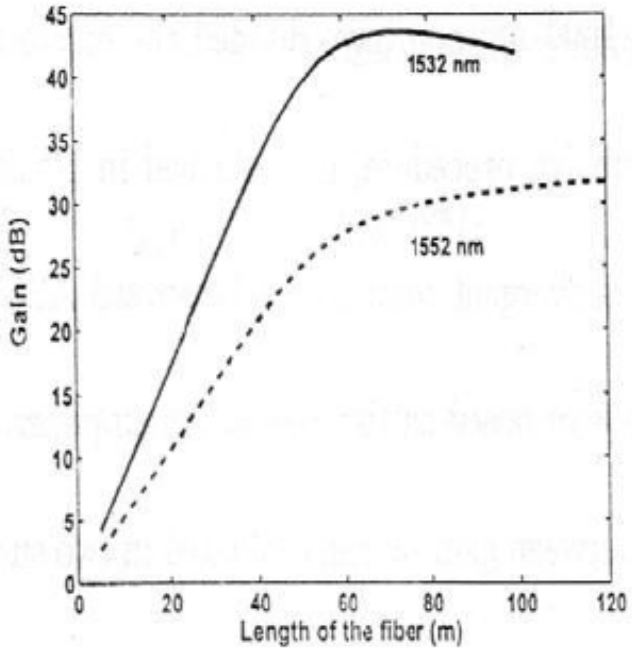


Fig. 4: Variation of EDFA gain

These results are in close matching with those published in literature [8] and thus verify our simulations. Figures 5 and 6 show the spectral variation of small signal gain and ASE spectral density for a 70 m long EDF pumped with 50 mW power at 980nm. simultaneously launched signal channels from 1520 to 1570 nm, with 0.1 μW of power per channel, have been considered in obtaining these spectra.

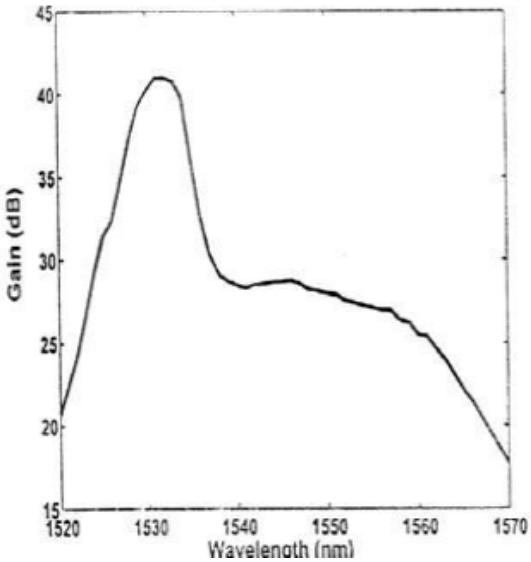


Fig. 5: Spectral variation of EDFA gain

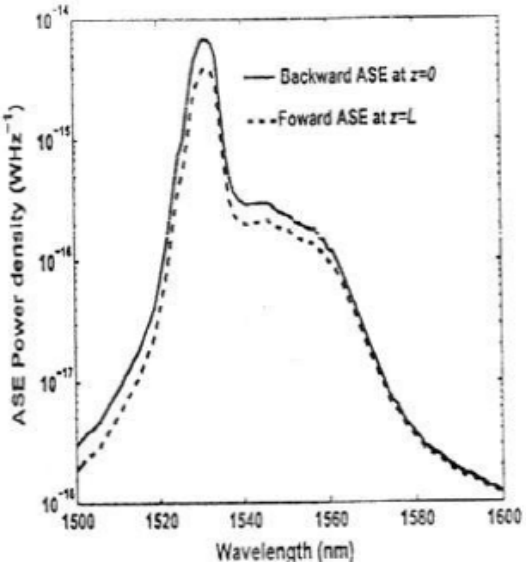


Fig. 6: Spectral variation of forward and backward ASE spectral density in an EDFA

The program has to undergo 18 forward-backward iterations to obtain the result.

5. CONCLUSION

In this paper, we have presented the theoretical background for Raman amplification and amplification by rare earth doping, in optical fibers. We have formulated the basic equations governing the evolution of pump, signal and noise power for both Raman fiber amplifiers and three-level system based doped fiber amplifiers. The analysis presented here forms the basis of modeling and designs of Raman Fiber Amplifiers and three-level system based on doped fiber amplifiers.

REFERENCES

[1] Yariv, A. (1967), Quantum Electronics, first edn, John Wiley.

[2] Rootwitt, K., Bromage, J., Stentz, A., Leng L., Lines, M. E. & Smith, H. (2003), 'Scaling of the Raman gain coefficient:applications to germanosilicate to fibers', Journal of Lightwave Technology 21, 1652-1662.

[3] Davey, S.T., Williams, D.L., Ainsile, B.J., ROTHWELL, W .J .M & Wakefield, B (1989), ' Optical gain spectrum of GeO2-SiO2 raman fiber amplifiers', IEE Proceedings 136, 301- 306.

[4] Kang, Y. (2002), Calculations and measurements of raman gain coefficient of different fiber types, M. s., Virginia Polytechnic Institute, Blackburg, Virginia. URL: http: // scholar.lib.vt.edu/theses/available/etd-01102003-020757/.

[5] Desurvire, E. (1994), Erbium-doped Fiber amplifiers: Principal and Applications, Wiley- interscience, New York.

[6+ Perlin, V. E. & Winful, H. G. (2002), 'On distributed Raman amplification for ultrrabroad- band long-haul WDM systems', Journal of Lightwave Technology 20, 409-416.

[7+ Liu, X. & Li, Y. (2003), 'Optimizing the bandwidth and noise performance of distributed multi-pump Raman amplifiers', Optics Communications 230, 425-431.

[8+ Pedersen, B. Bjarklev, A., Povlsen, J. H., Dybdal, K. & Larsen, C. C. (1991), 'The design of erbium-doped fiber amplifier', Journal of Lightwave Technology 9, 1105-1112.

Signed Mean E- Cordial Labeling

K. Ameenal Bibi [1] , T. Ranjani [2]

[1,2] P. G and Research Department of Mathematics,
D. K. M College for women (Autonomous), Vellore-632001.

ABSTRACT

Let G be a simple (p,q) graph and let $f : E(G) \to \{-1, +2, -3, \dots\}$ *e a mapping with the induced labeling* $f^*: V(G) \to \{0,1\}$ defined by $f^*(V) = \sum f(u+v)/(u+v \in E(G) (mod\ 2)$ *then f is called a Signed mean E- cordial labeling of a graph G if the number of vertices labeled with 0 and number of vertices labeled with 1 differ by atmost 1 and the number of edges labeled with alternative signed integers.*

A graph G which admits Signed mean E-cordial labeling is called a Signed mean E- cordial graph.

Here ,we have proved that wheel graph , circulant graph, Petersen graph and Gear graph admit Signed mean E- cordial labeling.

Mathematical subject classification: 05C78.

Keywords: Labeling, Mean labeling, Graceful labeling ,Cordial labeling, signed labeling, E-cordial labeling, Signed mean E- cordial labeling.

INTRODUCTION :

We begin with a graph $G = ((G), E(G))$ with p vertices and q edges we mean G to be simple, finite, connected and undirected graph .For any undefined notation and terminology ,we refer Gross and Yellen[8].

Definition 1.1:

A graph labeling is an assignment of integers to the vertices or edges or both subject to certain conditions.

In 1967,Rosa introduced the labeling on G ,called graceful labeling.

Definition 1.2:

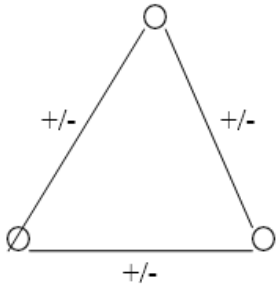
A function $f: (G) \to \{0,1 \dots | E(G) |\}$ is called a graceful labeling of a graph G if f is injective and the induced function $f^*(e = uv) = | f(u) - f(v) |$ is bijective. A graph which admits graceful labeling is called a graceful graph.

Definition 1.3:

A binary vertex labeling of a graph G with induced edge labeling $f^*: (G) \to \{0,1\}$ definedby $f^*(e = uv) = | f(u) - f(v) |$ is called a cordial labeling if $|v_f(0) - v_f(1)| \leq 1$ and $| e_f(0) - e_f(1) | \leq 1$. A graph G is a cordial graph if G admits a cordial labeling.

The concept of cordial labeling was introduced by Ebrahim Cahit(Turkey) as a Weaker version of graceful and harmonious labelings. He also investigated several results on this newly defined concept.

Definition 1.4:
In graph theory, Signed graph is a graph in which each edge or each vertex or both have a positive or negative sign.



The concept on Signed graph appeared first in 1953 by Frank Harary , at the center for Group Dynamics at the university of Michigan.

Definition 1.5:

Let G be a graph with vertex set V(G) and edge set E(G) and let $f: E(G) \to \{0,1\}$. Define a mapping f^* on V(G) by $f^*(V) = \sum f(uv)/(uv \in E(G)(mod\ 2)$. The function f is called an E-cordial labeling of G if $|v_f(0) - v_f(1)| \leq 1$ and $|e_f(0) - e_f(1)| \leq 1$. A graph G is called E cordial graph if it admits an E-cordial labeling.

In 1997, Yilmaz and Cahit [12] introduced E- cordial labeling as a weaker version of edge- graceful labeling and with the blend of cordial labeling.

Definition 1.6:
A graph G with p vertices and q edges is a mean graph if there is an injective function f from the vertices of G to {0,1,2, … .q} such that when each edge uv is labeled with

$\frac{(u)+f(v)}{2}$ if $f(u) + f(v)$ is even and $\frac{f^{(u)+f(v)+1}}{2}$ if $f(u) + f(v)$ is odd then the resulting edges are distinctly labeled.

Definition 1.7:

The Wheel graph W_n is defined to be the join $K_1 + C$. The vertex corresponding to K_1 is known as apex vertex and vertices corresponding to the cycle C_n are known as rim edges.

Definition 1.8:
The Gear graph G_n is obtained from the Wheel by subdividing each of its rim edges .

Main Results:

Theorem 2.1:
The Circulant graph Cn(n = 6) admits Signed mean E- cordial labeling with generating set (1,2).

Proof:

Let $G = C_n(1,2)$ be the 4- regular graph with n=6.

Let $V(G) = \{^{V}_{i} = 0,1,2..n-1\}$

We define a mapping $f: (G) \to \{-1,-2,-3,-4,-5,-6\}$

We have assigned the inner edges with positive integers.

Define the function (V_iV_{i+1}) = -i-1 for i=1,2,3,4,5.

$$(V_iV_{i+2}) = \begin{cases} i+7 \text{ for } i=0,5 \\ 3i+7 \text{ for } i=1 \\ i+6 \text{ for } i=2 \\ i+8 \text{ for } i=3 \\ i+5 \text{ for } i=4 \end{cases}$$

then apply $f^*(V) = \sum f(u+v)/(u+v \in E(G)(mod\ 2)$, then we get the induced function $f^*: V(G) \to \{0,1\}$.

Thus using the above labeling pattern , We found that C_n admits Signed mean E- cordial labeling.

Illustration 1.1:

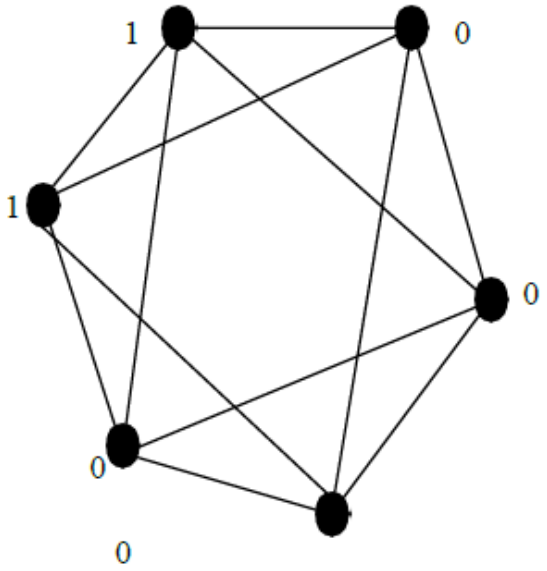


Figure 1: Signed mean E- cordial labeling of Circulant graph C.

Theorem 2.2:
The Gear graph G_n admits Signed mean E- cordial labeling.

Proof:

Let W_n be a Wheel graph with apex vertex v and rim vertices $v_1v_2 \ldots v$.

To obtain the Gear graph G , sub divide each of the rim edges of the Wheel graph by the vertices $u_1u_2 \ldots u_n$.

We define a mapping $f: (G) \to \{-1, +2, -3, +4 \ldots . +12\}$

We have assigned the inner edges with positive integers .

then apply $f^*(V) = \sum f(u+v)/(u+v \in E(G)(mod\ 2)$ then we get the induced function $f^*: V(G) \to \{0,1\}$.

Thus using the above labeling pattern , We found that G_n admits Signed mean E- cordial labeling.

Illustration 1.2:

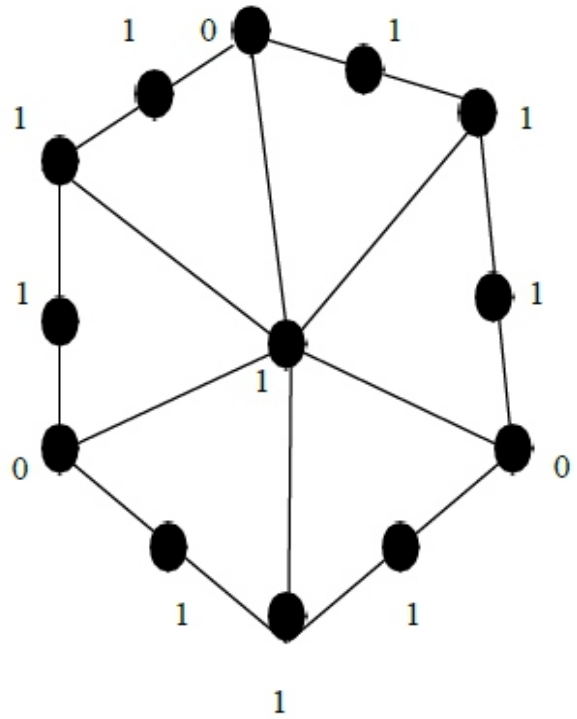


Figure 2: Signed mean E- cordial labeling of the Gear graph G7

Theorem 2.3:
Petersen graph admits Signed mean E- cordial labeling.

Proof:
Petersen graph is a 3-regular graph with 10 vertices and 15 edges.

Let $u_0, u_1 \ldots u_{14}$ be the edges and

Let $v_0, v_1 \ldots v_9$ be the vertices of Petersen graph.

Let $e_{1,2}, e_3, e_4, e_5$ be the inner edges.

We define the labeling function for the inner edges of the Petersen graph as follows:

$$f: (G) \to \{-1, -2, -3, -4, -5\}$$

Let the remaining outer edges be the positive integers.

Let $f: (G) \to \{6,7,8 \ldots 15\}$

then apply $f^*(V) = \sum f(u+v)/(u+v \in E(G)(mod\ 2)$ then we get the induced function $f^*: V(G) \to \{0,1\}$.

Thus using the above labeling pattern , We found that Petersen graph admits Signed mean E- cordial labeling.

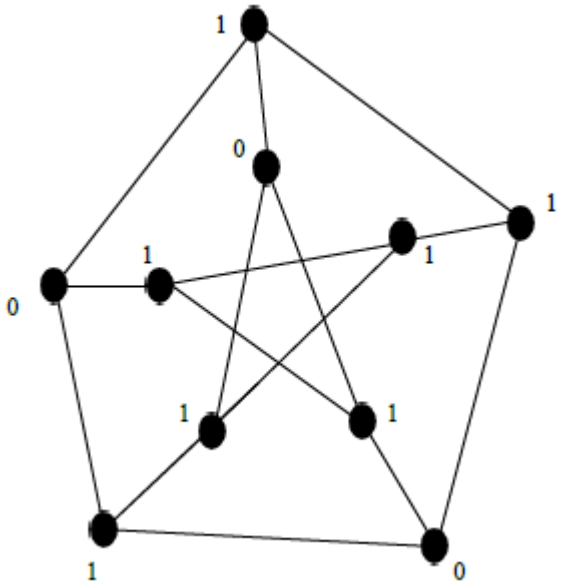


Figure 3: Signed mean E- cordial labeling G(10,15).

Theorem 2.4:

Let W_n be a wheel graph of order n=6 then W_n admits Signed mean E – cordial labeling.

Proof:

Let $W_n = (v_1 v_2 \ldots v)$ be a Wheel of order n=6.

We define a mapping $f: (G) \rightarrow \{-1, -2, -3, -4, -5\}$

We have assigned the inner edges with positive integers.

then apply $f^*(V) = \sum f(u+v)/(u+v \in E(G)(mod\ 2)$ then we get the induced function

$f^*: (G) \rightarrow \{0,1\}$.

Thus using the above labeling pattern , We found that W_6 admits Signed mean E- cordial labeling.

Illustration 1.4:

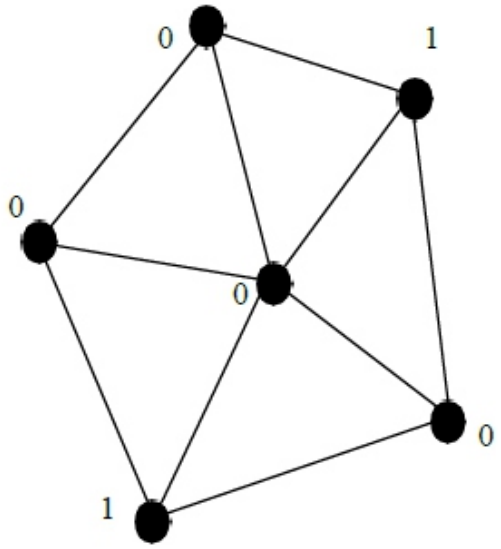


Figure 4: Signed mean E- cordial labeling of W_6

CONCLUSION :

In this paper, We have obtained Signed mean E-cordial labeling for the Circulant graph *C,* Petersen graph, Wheel graph and the Gear graph of finite order. We further, motivated to verify the above labeling process, for some more special classes of graphs.

REFERENCES:

1. *K. Ameenal Bibi and T. Ranjani, Total bi-magic circulant graphs with generating sets(1, 2, 3, 4) and (1, 2, 3, 4, 5), Global Journal of Pure and Applied Mathematics, 13, 3789–3799.*
2. *K.Ameenal Bibi , P.Rekha and T.Ranjani Cordial double – staircase graphs, "Global Journal Of Pure And Applied Mathematics". ISSN 0973-1768 Volume 13, pp3395-3401.*
3. *K.Ameenal Bibi and T.Ranjani , Edge – Even Graceful labeling on Circulant Graphs with different generating sets, "Global Journal Of Pure And Applied Mathematics".ISSN 0973-1768 Vol.13, N0.9(2017),pp 4555-4567.*
4. *K.Ameenal Bibi and T.Ranjani "Cordial labeling on Aztec Diamond Graph"- Communicated.*
5. *K.Ameenal Bibi and T.Ranjani "Fibonacci Mean Anti – Magic Labeling Of Some Graphs".*
6. *J.Baskar Babujee and L.Shobana. Prime cordial labeling "International Review of Pure and Applied Mathematics 5(2)(2009),277-282.*
7. *Gallian J.A. A Dynamic Survey of Graph Labeling, The Electronic Journal of Combinatorics,16,#Ds6(2013).*
8. *J.Gross and J.Yellen "Graph Theory and its Applications" CRC Press 1999.*
9. *S.K.Vaidya and N.B.Vyas "Some result on E- cordial labeling "International journal of Mathematics and Scientific Computing ISSN:2231-5330.Vol.2 No.1 – 2012.*
10. *S.K.Vaidya and Lekha Bijukumar, "Some New Results on E- cordial graphs". Int. Journal of Information Science and Computer Mathematics Vol 3,PP.21-29 2011.*
11. *S.K.Vaidya and N.B.Vyas E- Cordial Labeling of Some Mirror Graphs, Int.Journal of Contemporary Advanced Mathematics,Vol.2.PP 22-27. 2011.*
12. *R.Yilmaz and I.Cahit E- Cordial graphs Ars Combin. Vol.46. PP 251-266.1997.*

Security Vulnerability on Multi- Protocol Label Switching in Virtual Private Network

EZE, M. N.[1], OGBU, M. N. C.[2], ARINZE, S. N.[3]
Department of Electrical and Electronic Engineering Enugu State University of Science and Technology (ESUT) Enugu State Nigeria

ABSTRACT

Presently, Multi-Protocol Label Switching (MPLS) is the global data transmission technology used for delivery of voice and multimedia applications in Virtual Private Network (VPN). The main purpose of security is to protect the network assets. However, insecurity issues on the cloud of MPLS-VPN system remain the major challenges for the network designers. This paper discusses the security vulnerability on an MPLS-VPN with different enhancement techniques that have been implemented in the network in order to enhance it. Security vulnerabilities such as policy flaws, malicious software, protocol weaknesses and software / hardware vulnerabilities in MPLS-VPN need to be mitigated.

Keywords: Network Security, MPLS, VPN, Security Vulnerability, Enhancement Techniques.

1. INTRODUCTION

Multi- Protocol Label switching (MPLS) is an efficient and effective data transmission technology that forwards the packet across the network using short fixed-length known as label. MPLS is the latest technology developed by Internet Engineering Task Force (IETF) in 1999. This technology support many services such as Traffic Engineering (TE), creation of Virtual Private Network (VPN), and Quality of Services (QoS). VPN is an enterprise network that transmits data over the Internet by allowing users to securely enter into internal public infrastructure via unsecured network. According to Qureshu (2014) the main two functions performed by MPLS in VPN are packet forwarding and route distribution. During data transmission, there is no security of the VPN data traffic in MPLS networks. Thus there are number of insecurity issues associated with MPLS-VPN technology. The term security simple means protection against malicious attack by outsider/insider VPN users. Hackers gain illegitimate access to a MPLS-VPN network resources or the cloud. Security in a cloud based MPLS-VPN can be viewed from two different perspective namely from service provider or from the user. For the user, the attack is against intrusions from outside of the VPN customer into his or her domain while for the provider the attack is really available at the core side of MPLS network. Mende, D. et.al (2011) stated that MPLS does not provide protection against core, VPN customer security and Confidentiality, Authentication and Integrity (CAI) triad security requirement. There is need to provide an appropriate measure to mitigate those attack against cloud based MPLS-VPN.

Arora et al (2012) carried a study about the performance of different security techniques on a cloud network. The objective of the paper was to find quantitative terms such as Speed- up Ratio which help in implementation of security algorithms used to protect large traffic. The results showed that those security techniques when implemented on cloud based network like MPLS-VPN are more efficient than using them on single system. Usman, S. H. (2013) looked at the responsibilities of Internet Service Providers (ISP) to provide more security for their VPN customers. It was observed that people use internet as an avenue for illegal activities such as breaking into other people networks, stealing data and blocking legitimate users from services they subscribed. Veni, S., and Kadhar-Nwaz, G.M., (2012); demonstrated a new approach known as a new (k, n) Threshold Secret Sharing (TSS) scheme for

security enhancement in MPLS in the VPN customers. The MPLS security issues like confidentiality, integrity, modification and fabrication of packet were stated. Okafor, et al (2013) formulated a security model called Self-Monitoring Analysis and Reporting Technology Intrusion Detection System (SMART-IDS). In the model, a site-to- site VPN scheme for LAN and wireless supports were provided. The developed model improved the backbone of MPLS-VPN for proper security implementation. The result of the model gave high throughput with an improved QoSmetrics.

Sidhu, A. and Mahajam, R. (2014) explained that security in the cloud service architecture is always a big issue for the vendor as well as users. Different security models and algorithms that have been applied have failed to solve most of the security threats especially in cloud domain. Most of the security techniques were used for securing ordinary file but not for the transfer of communication messages. The proposed model by the authors was a hybrid approach of various algorithms like Advanced Encryption Standard (AES) and Message Digest 5 Hash function (MD5- which is a cryptographic Hash function) and these will handle the security issues. The results obtained with the hybrid algorithms were implemented in JAVA language. This prevented the inside attack in the cloud MPLS-VPN. However the authors recommended the use of other encryption technique such as Rivest Cipher, Data Encryption Standard (DES) etc. for better security concern of the network cloud. It was also recommended that future research work on comparison of security features under various attack in the cloud services should be carried out. Jakimoski, K. (2016) evaluated the security techniques for data protection in cloud computing. These security techniques were classified into four sections namely: confidentiality, access control, authentication and authorization. Secure Socket Layer (SSL) was used to overcome attacks like man-in-the-middle attack or Distributed Denial of Service (DDOS) attack.

2. THEORETICAL BACKGROUND OF MPLS-VPN

Multi-Protocol label Switching is a technology proposed by Internet Engineering Task Force (IETF) in order to overcome the limitation of traditional IP network. This technology is used by Internet Service Providers (ISP) especially in the core side of the network to give assure Quality of Service (QoS).Many telecommunications operators and ISP currently use services based on MPLS to create Virtual Private Networks (MPLS-VPN). This MPLS-VPN network is the technological method used to transport and route several types of network traffics using an MPLS backbone. There are three types of MPLS-VPN deployed in networks today, namely: Point-to-Point, Layer 2 and Layer 3 MPLS-VPN. Point-to-Point MPLS-VPN used virtual leased lines like E1/T1 Ethernet and ATM to provide point-to-point connectivity between two sites. Layer 2 MPLS-VPN also known as Virtual Private LAN Service (VPLS) can offer what is called switch in the cloud service between LAN sites. Layer 3 MPLS-VPN utilizes layer Virtual Routing and Forwarding (VRF) to segment routing tables for each VPN customers.

MPLS-VPN can be implemented in two different methods: Overlay and Peer-to-Peer method. In overlay implementation method, the ISP gives the customer a dedicated circuit for the service delivery, while in peer-to-peer, ISP peers with the customer via Provider Edge (PE) routers. The PE routers have VRF instance to keep all the customers routes separate from other customer.

The elements of the MPLS-VPN are the customer network (VPN site), Customer Edge (CE) router, Provider network in the core (MPLS cloud), Provider Edge (PE) router, and Provider (P) router. These are shown in architectural diagram of a cloud based MPLS- VPN which is depicted in the figure below

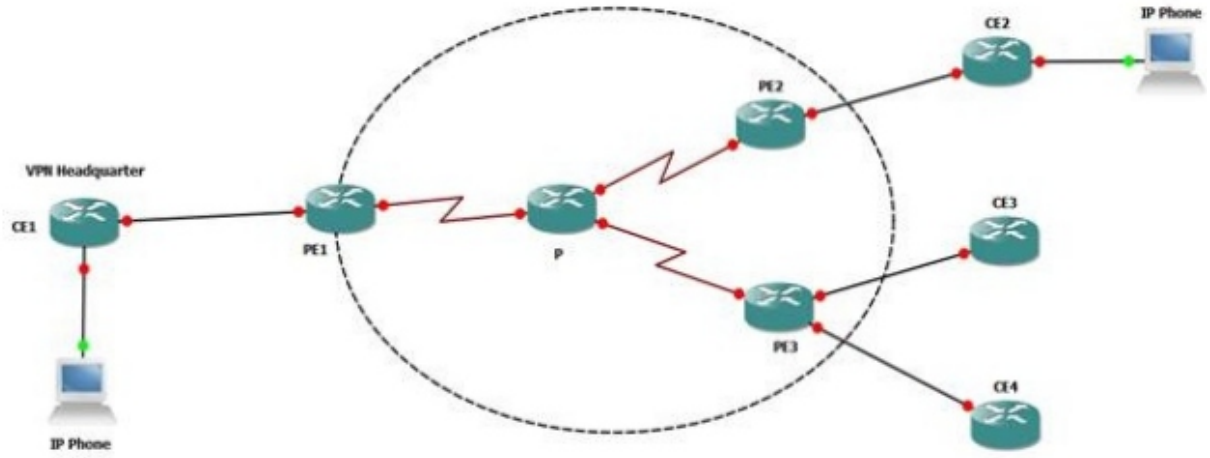


Fig 1 Architecture of MPLS-VPN

The core network of the MPLS consists of PE and P routers and PE routers are used to provide VPN services to the customers. Customer routers (CEs) are connected to the PEs. In MPLS-VPN technology packets can be transferred and processed in three different planes namely control, data and management planes. Each of these planes handle different functions in an enabled MPLS network. Exchanging, processing and establishing of routing information are done in a control plane, while data plane handle the implementation of those VPN data. Management plane is where the entire equipment configuration is managed. All these planes in an MPLS-VPN experience different security threats which need to be addressed.

3. BASIC PROPERTIES OF SECURITY IN MPLS-VPN

When considering security in an MPLS network, emphasis must be made by ensuring the whole network is secure. This will make none of the nodes to be vulnerable to attack. There are various basic properties of security in MPLS-VPN that need to be considered. They are confidentiality, integrity, authentication, and availability. They are the actual goal of any MPLS enabled network security.

- Confidentiality makes the data traffic on the network to remain private. Examples of attack methods are eavesdropping, hacking, IP spoofing and Denial of Service.
- Integrity property ensures that the message has not be modified in transit. Examples of the attack are viruses, worms, DoS and Trojans
- Authentication as a property ensures that the users of the MPLS network are who they say they are.
- Availability property gives the users easy access to the network and make all the nodes available at any point in time.

For any MPLS-VPN enterprise businesses to achieve its potential mission and vision, these properties of security must be addresses and all network must be protected for threats and vulnerabilities. Security objectives (properties) can be realize with the four A's notations (AAAA) meaning Authentication, Authorization, Auditing and Action.

4. MPLS-VPN SECURITY ANALYSIS

MPLS-VPN security requirement are as follows: VPN address and traffic separation, protective model against IP-spoofing, hiding of the MPLS core structure and robustness against attacks. The key security

requirement for the users is that their traffic is kept separate from other users and from the core side. In MPLS-VPN architecture, the address space is separated between users because only the PE routers know the IP-address of the user and their routes. Any VPN must use the same address space as any other VPN or as the MPLS core. Traffic routing between any two VPN or between any VPN and the core must be independent. It is important for the internal IP address of the core MPLS to remain hidden to the outside world. This will enable it to avoid attacks like Man-in-the-Middle or DoS.

5. SECURITY VULNERABILITY IN MPLS-VPN

Vulnerability comes from Latin word "Vulnus" which means wound and it is the state of being open or exposed to a threat. Vulnerability in MPLS-VPN means weaknesses in the MPLS technology, configurations, security policy, or in those inherent VPN devices such as routers, switches, servers and firewalls. Security vulnerability is referred to a cyber- security flaw in a network which makes the system open for attack. There are different types of security vulnerabilities such as policy flaws, malicious software, protocol weaknesses, and hardware and software vulnerabilities.

Policy flaws are the security policy weaknesses that create unforeseen threats when VPN users do not follow the policy thereby imposing risk to the system. Lack of continuity and lack of written policy are the examples of policy flaws in MPLS networks. Protocol weaknesses are those TCP/IP weaknesses that inherently made HTTP, FTP and ICMP unsecured in an MPLS-VPN. Simple Network Management Protocol (SNMP) and Simple Mail Transfer Protocol (SMTP) are the examples of TCP/IP protocol that when they are weak, threats will take advantage of them to attacks the network. Various types of network equipment such as routers, firewall, switches constitute the hardware vulnerability. The hardware vulnerabilities that could be observed in an MPLS-VPN network are as follows: password protection, lack of authentication, routing protocol and firewall holes. Network devices, computer hardware and mobile devices have software as a common thing among them. This software is the main source of security problems. In an MPLS-VPN, software such as router software, web browsers, web servers, Linux/ windows operating system can be exploited by an attacker due to bad software executed over the network. Software vulnerabilities can be seen as either design, implementation or configurations flaws. Examples of typical software vulnerabilities are buffer overflow, code or design defect, and web problem in SQL injection.

Security vulnerability threats of MPLS-VPN occur in three different plane levels viz control, data and management levels. In the control plane , VPN routing information that passes through P and PE routers have various attacks such as alteration of the routing information and Denial of service, while in data plane level , the attack normally occurs as IP source address spoofing, protocol session hijacking, Trojans and replay of legitimate MPLS packet etc. This attack usually occurs between the VPN Customer Edge (CE) and Provider Edge routers. The security threats of the management plane are the attack to network devices via the administrative interface.

6. SECURITY ENHANCEMENT TECHNIQUES

Network security is one of the important issues that organizations need guarantee for. Many techniques have been proposed for the enhancement of security vulnerability of MPLS-VPN. Techniques are Intrusion Detection System, Secure Socket Layer Encryption, Cryptographic Hashing Algorithm -- (Message Digest 5 (MD5) and Security Hash Algorithm), Advanced Encryption Standard, Rivest-Shamir-Adlehman (RSA), Diffie- Hellman and IP Security.

Encryption technique is the fundamental technique used for the protection of data in any network. This technique is normally used for the purpose of confidentiality. Encryption technique can be categorized into symmetric (private) and Asymmetric (public) key. Only one key is used to encrypt and decrypt data traffic in symmetric encryption technique while two keys are used in asymmetric type. There are four types of this technique commonly used in MPLS network, namely Data Encryption Standard (DES), Triple Data Encryption Standard (3DES), Advanced Encryption Standard (AES), Rivest- Shamir-Adlehman (RSA). DES is an algorithm that is used for parity check to verify the integrity of the data traffic in a network. RSA is a public key scheme used for encrypting message, exchanging keys and creating digital signatures. This technique is based on exponentiation that uses modular arithmetic to secure data during transmission. This technique is commonly used to directly encrypt user data transmission which takes to time to decrypt. Transport Layer Security formerly known as Secure Socket Layer technique is used to protect a layer 3 and 4 application such as HTTP by adding encryption and authentication to a layer 2 and 3 protocol.

IPSecurity (IPSec) technique is usually run with encryption like Encapsulating Security Protocol (ESP) and Authentication Header (AH) on the customer edge router or over the MPLS cloud. Diffie-Hellman technique is the key that exchange key between two users by generating a shared private key across an unsecure domain. This technique was named after Whitfield Diffie and Martin Hellman. Intrusion Detection System is another technique that logically combines with one or more firewalls to protect networks. The four main types of IDS are as follows:

- Network intrusion detection system
- Host-based intrusion detection system
- Perimeter intrusion detection system
- Virtual machine based intrusion detection system

IDS technique is used to strengthen the system security thereby increasing the resistance to core and outside MPLS cloud attacks.

7. CONCLUSION

This paper proposed a study of security vulnerability on Multi-Protocol Label Switching in Virtual Private Network. Basic security properties and requirement were explained. Different techniques that had been used to enhance security on MPLS network were stated. As a future work the paper is proposing the use of Software Defined Algorithm as a new security approach for a Cloud Based MPLS-VPN.

REFERENCES

1. *Afolabi, A. O., and Atanda, O. G. (2016). "Comparative Analysis of some Selected Cryptographic Algorithms". Computing Information Systems, Development Informatics and Allied Research Journal. Vol. 7, No. 2, pp. 41 -52.*
2. *Arora, P., Singh, A. and Tiyagi, H. (2012).Evaluation and Comparison of Security Issues on Cloud Computing Environment. World of Computer Science and Information Technology Journal (WCSIT), Vol. 2 No. 5, pp. 179 - 183.*
3. *Jakimoski, K. (2016). "Security Techniques for Data Protection in Cloud Computing". International Journal of Grid and Distributed Computing. Vol. 9, No. 1, pp. 49 -56.*
4. *Mende, D., Rey. E. and Schmidt, H. (2011).Practical Attacks against MPLS or Carrier Ethernet Networks. Enno Rey Netzwerke (ERNW) providing Security. Version 9.*
5. *Okafor, K.C., Okezie, C.C., Udeze, C.C. and Okwuelu, N. (2013). "SMART-IDS: An Enhanced Network Security Model in IP- MPLS based VPN". African Journal of Computing and ICT Reference format, Vol. 6, No. 3, pp. 135-146.*

6. *Qureshi, K.N, Abdullah, A.H, Hassan, A.N, Sheet, D.K and Anwar, R.W, 2014. Mechanism of Multi-ProtocolLabel Switching for forwarding packets and performance in Virtual Private Network.Middle-East Journal of Scientific Research.Vol. 20, No. 12, pp 2117-2127.*
7. *Sidhu, A., and Mahajam, R. (2014).“Enhancing Security in Cloud Computing Structure by Hybrid Encryption”.International Journal of Recent Scientific Research.Vol. 5, No.1, pp. 128 -132.*
8. *Usman, S. H. (2013). “A Review of Responsibilities of Internet Service Providers toward their customers network Security”.Journal of Theoretical and Applied Information Technology.Vol.49, No.1, pp. 70 -78.*
9. *Veni, S. and Kadhar-Nwaz, G. M. (2012). “A new Approach to Enhance Security in MPLS network”.Advanced Computing: An International Journal, Vol.3, No.3, pp. 75 – 80.*

Introduction To Wireless Sensor Network and its Applications

Anju Devi
Department of Computer Science and IT GNG College,
Santpura, Yamuna Nagar

A B S T R A C T

Sensor networks are expected to play an essential role in the upcoming age of pervasive computing.WSN stands for Wireless Sensor Network. Wireless Sensor Network consists of thousands of self organizing, low-power, low cost wireless nodes and is used in variety of fields which includes military, healthcare, environmental, biological, home and other commercial applications. In this paper, different types of wireless sensor network topologies described in details. The characteristic of this is to divide WSN into network based on Topologies i.e. Bus, Tree, Star, Ring, Mesh. Information of the position of nodes, and those nodes are organized within the network by the Topological way.

Wireless Sensor Networks (WSN), which is composed of several thousands of sensor nodes which are capable of sensing, actuating, and relaying the collected information. This paper presents an overview of the various wireless sensor network types and their applications, operations, topologies and advantages etc.

Keywords: wireless sensor network, applications, topologies, types

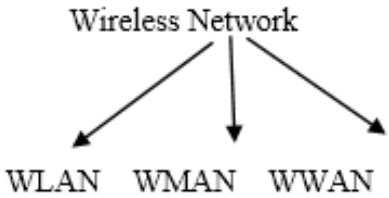
INTRODUCTION

Wireless sensor network refers to a group of spatially dispersed and dedicated sensors for monitoring and recording the physical conditions of the environment and organizing the collected data. Recently, this technology becomes more popular because of its application and cost. The wireless sensor networks are built of several hundred or thousands of nodes, where each node is connected to one or several sensor. It measures the environmental conditions like temperature, pollution, wind, sound and etc. The development of wireless sensor networks was motivated by military applications like battlefield surveillance, today this type of network also used in industrial applications like this industrial process monitoring and controlling, machine monitoring etc.

Wireless sensor network is dynamic which can consist of various types of sensor nodes. The environment is heterogeneous or dissimilar type in terms of both hardware as well as software. The sensor node construction focuses to reduce cost, increase flexibility, Improve conserve energy. The structure of sensor node consists of sensing unit (sensor and analog to digital converter), processing unit (processor and storage), communication unit (transceiver), and power supply unit.

Wireless Network

Wireless networks are not connected to cable. Wireless telecommunications networks are generally implemented and using a transmission system called radio waves. AM radio, FM radio, satellite radio, satellite TV, satellite Internet access and broadcast TV are wireless networks. Wireless technology is very convenient. Wireless networks have many uses. A common is the portable office. People on the road want to use their portable electronic equipment to send and receive telephone calls, faxes, and electronic mail, read remote files, login on remote machines. Computers there can send messages, keep records, and so on. It is a kind of computer network. Wireless communication is the transfer of information between two or more devices that are not connected through cable. The most common wireless technology is use radio communication. There are various types of wireless networks:-

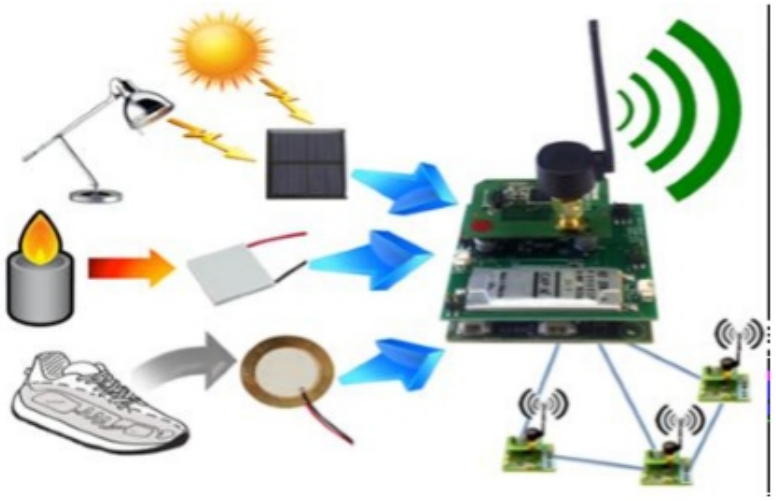


Wireless local area network (WLAN), it covers a very little area to communicate the networks with each others. Wireless metropolitan area network (WMAN), communicates with the device over a city, town etc. Wireless wide area networks (WWAN), information are shared over all the world.

Wireless Sensor Network:

A sensor network is a group of tiny, generally battery powered device and wireless infrastructure that monitor and record conditions in any number of environment.

WSN monitors are parameters which are temperature, direction of wind and speed, pressure, intensity of vibrations, pollution, humidity etc.



A wireless sensor network is a kind of wireless network. These networks covers a large number of distributed, battery operated, embedded devices that are network to collect, process and transfer data to the operators. The sensor node is a multi-functional, efficient wireless device. A collection of sensor nodes collects the data from the surrounding to achieve specific application.

Types of WSNs

There are various types of sensor networks which are given below:

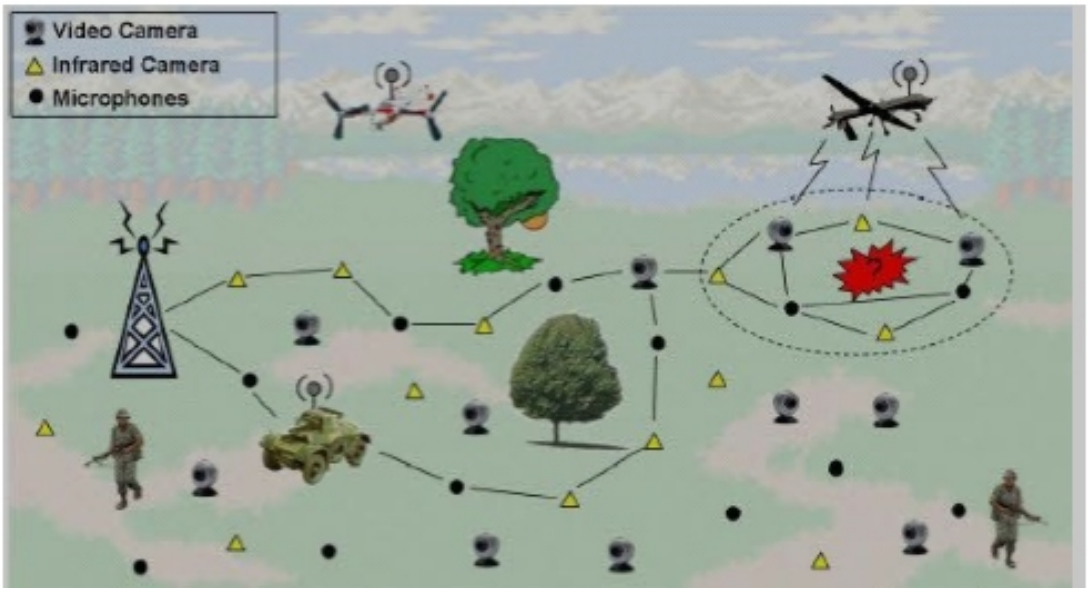
1. Terrestrial WSNs
2. Multimedia WSNs
3. Underground WSNs
4. Underwater WSNs
5. Mobile WSNs

1. Terrestrial WSNs

Terrestrial WSNs are capable of communicating base stations, and consist of hundreds to thousands of wireless sensor nodes deployed either in unstructured or structured manner. In an unstructured mode, the sensor nodes are randomly distributed within the target area that is dropped from a fixed plane. The structured mode considers optimal placement, 2D, 3D placement models. In this wireless sensor network limited battery power.

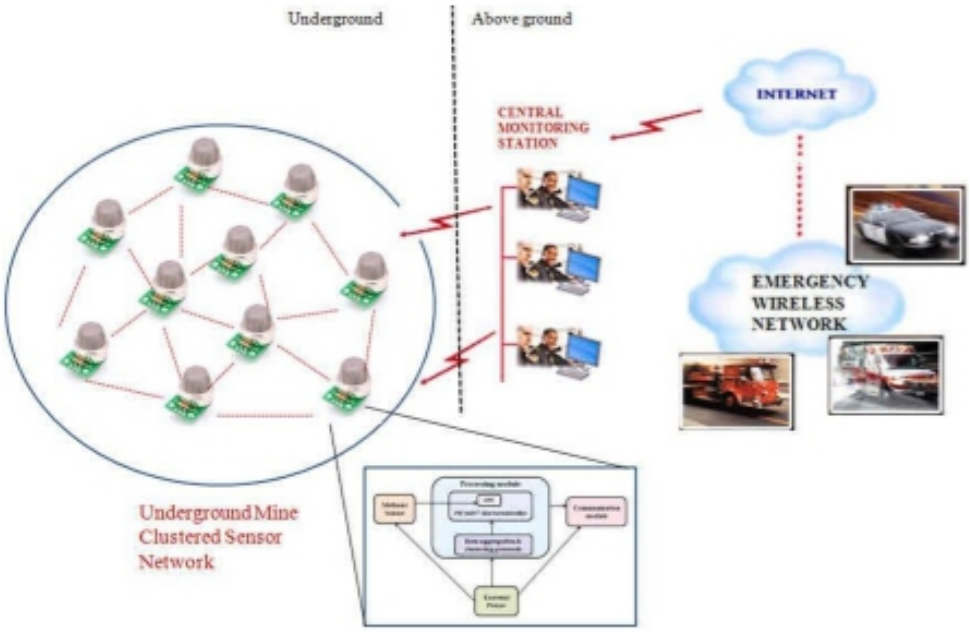
2. Multimedia WSNs

Multimedia wireless sensor networks to enable monitoring and tracking in the form of multimedia: images, audio and video. These networks consists of low cost sensor nodes equipped with cameras and microphones. The challenges with the multimedia wireless sensor networks include high energy consumption, data processing techniques and high bandwidth requirements



3. Underground WSNs

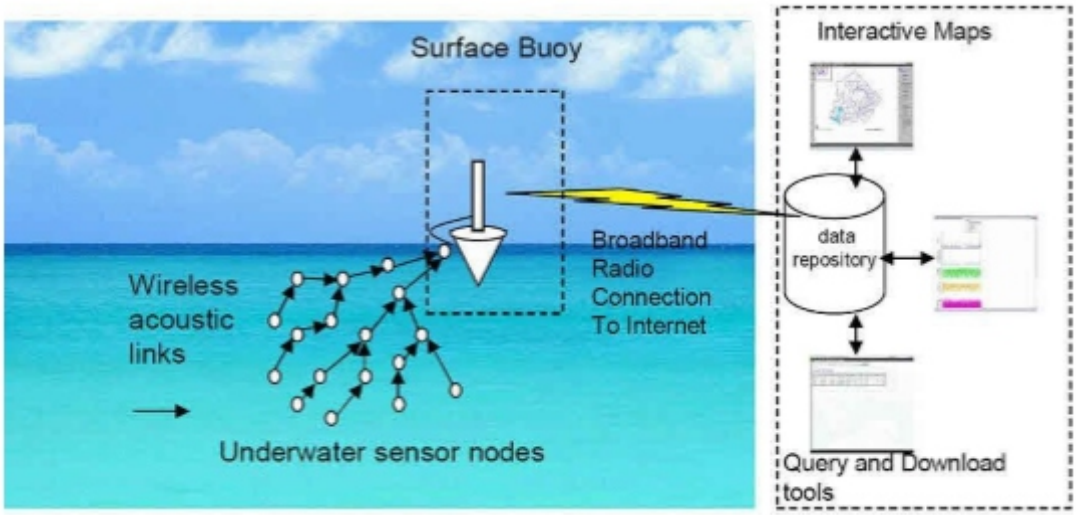
The underground wireless sensor networks are more expensive than the terrestrial wireless sensor networks in terms of deploy, maintenance, cost considerations and planning etc. The WSNs networks consist of a number of sensor nodes that are hidden in the ground to monitor underground conditions. To relay information from the sensor nodes to the base station, additional sink nodes are located above the ground.



The underground wireless sensor networks deployed into the ground are difficult to recharge. The sensor battery nodes equipped with a limited battery power.

4. Under Water WSNs

More than 70% of the earth is occupied with water. These networks consist of a number of sensor nodes and vehicles deployed under water. Autonomous underwater vehicles are used for gathering data from these sensor nodes. A challenge of underwater communication is a long propagation delay, bandwidth and sensor failures.



Under water WSNs are equipped with a limited battery that cannot be recharged or replaced. The issue of energy conservation for under water WSNs involves the development of underwater communication and networking techniques.

5. MOBILE WSNS

These networks consists of a collection of sensor nodes that can be moved on their own and can be interacted with the physical environment. The mobile nodes have the ability to sense and communicate. It is more versatile than the static sensor networks. The advantage of this WSNs are better energy, channel capacity good and improved coverage etc.

Operation of wireless sensor network

In wireless sensor network, wireless transmission consists of three major operations:

1. Convert data into radio wave.
2. Amplifying radio waves until reaching the receiving sensor.
3. Receiving sensor receives the data.

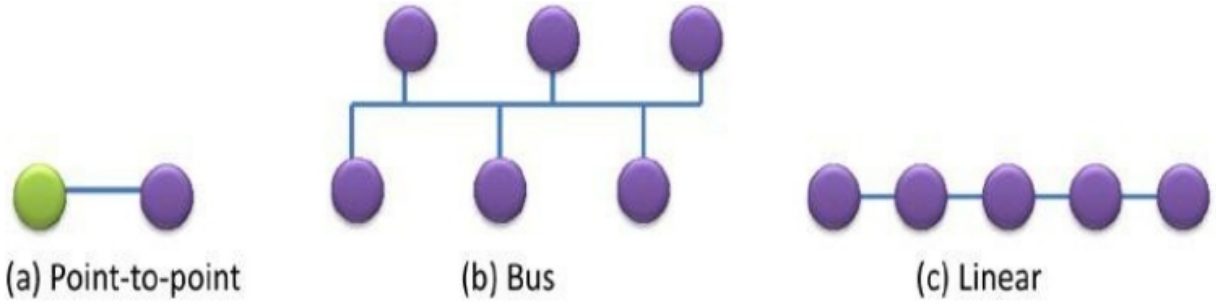
WSN Topology

For radio communication networks, the structure of a WSN includes different types of topologies like: star, mesh, tree, ring.

Bus Topology

In this topology, there is a node send message to another node on the network sends a broadcast message onto the network but only the intended recipient actually accepts and processes the message. Bus topology is easy to install. However, bus networks work best with a limited number of nodes. If more than a few dozen nodes are added to a network bus, performance problems will likely result.

In this paper presents a framework for real-time bus priority control system. The proposed system architecture integrated active and passive strategies and adding a priority classification level, can provide efficient bus priority control and minimize overall effects to motor vehicle movements under different traffic condition.



Star Topologies

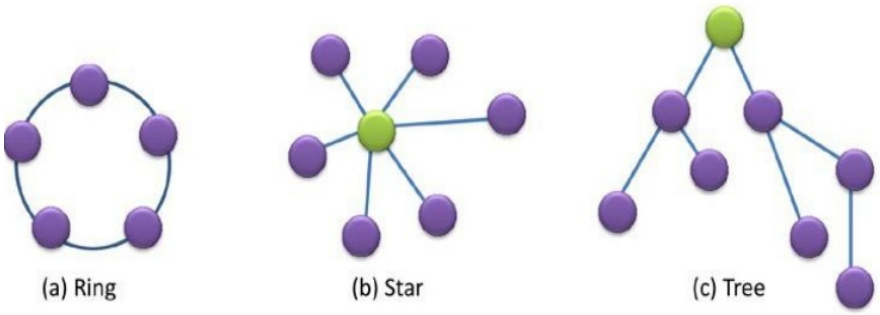
Star topology consists of a single ―central node,‖ such as a hub or a switch that every node in the network connects to it. This topology is easy to design, implement, and extend. All data traffic flows through the central node. Failure of this node will result in failure of the entire network. The star network topology is one of the most common sensor network topologies. A wireless personal area network (WPAN), consists of a smart phone connected to several wireless sensors, is a common example of this topology.

Due to its dependency on a single node to manage the network, the gateway must be within the radio transmission range of all the individual nodes. The advantage includes the ability to keep the remote nodes' power consumption to a minimum and simply under control. The size of the network depends on the number of connections made to the hub.

Tree Topologies

Tree topology is a hierarchy of nodes in which the highest level of the hierarchy is a ―root node,‖ and this node is connected to one or many nodes in the level. A tree topology can contain many levels of nodes. The processing and power in nodes increase as the data moves from the branches of the tree toward the root node, allowing data to be processed close to where it is generated. This topology is scalable and the simple structure makes it easy to identify and isolate faults. Tree networks become increasingly difficult to manage as they get larger.

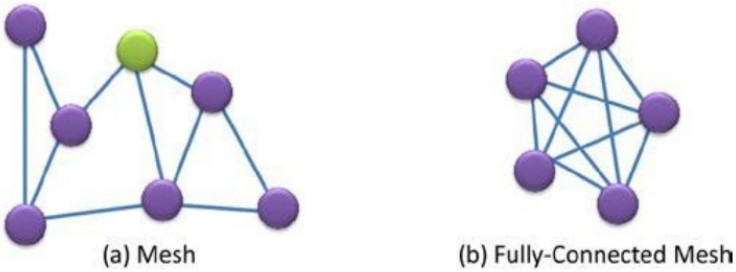
Tree topology is also called as cascaded star topology. The main advantage of the tree topology is that the expansion of a network can be easily possible, and also error detection becomes easy. The disadvantage with this network is that it relies heavily on the bus cable; if it breaks, all the network will collapse.



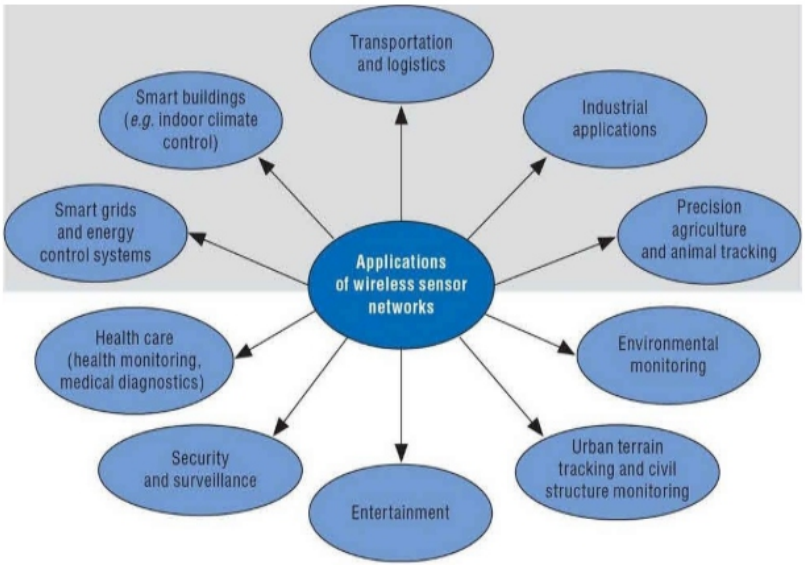
Mesh Topologies

The Mesh topologies allow transmission of data from one node to another, which is within its radio transmission range. There are two forms of mesh topology: a partially connected mesh, in which some nodes are connected to more than one other node; and a fully connected mesh, in which every node is connected to every other node in the mesh. Mesh networks are self-healing, as data can be routed along a different path if a node fails. Mesh topologies are most commonly found in wireless networking Sensor networks can also be described by their logical topology—the method they use to move data around the network. This logical topology is used in bus, star, or hybrid physical topology networks, due to their shared data bus or shared node.

The advantage with this mesh topology includes easy isolation and detection of faults in the network. The disadvantage is that the network is large and requires huge investment.



Wireless Sensor Networks applications



- These sensor networks are used in environments applications such as:animal tracking, flood detection, weather prediction and also in commercial applications activities prediction and monitoring.
- Health applications are also used this type of network such as: tracking and monitoring of doctors and patients.
- Wireless sensor networks can be an integral part of military command, control, communications, computing, intelligence, surveillance, reconnaissance and targeting systems.
- Area monitoring is a common application of WSNs. In area monitoring, the WSN is deployed over a region where some phenomenon is to be monitored. A civilian example is the geo-fencing of gas or oil pipelines.
- The most of the applications used in the field of transport systems such as monitoring of traffic etc.

Advantages of sensor network

1. Sensor nodes can be added or removed easily.
2. Execution pricing is inexpensive.
3. It can be opened by using a centralized monitoring.
4. Can be configured into different network technologies: star, tree, mesh etc.
5. Node location can be changed without rewiring.

Limitations of Wireless Sensor Network

1. It consumes a lot of power because it works in short communication range.
2. Very little storage capacity.
3. It has a limited life time of batteries
4. This network is not secure as compared to wired networks. Hackers can easily hack the network.
5. Communication speed is low as compared to wired network.
6. Wireless sensor network keep distraction by other wireless devices.

CONCLUSION

The wireless sensor network (WSN) technology is one such a new technology and has been attracting significant attention. In this paper, we have presented the introduction, topologies and characteristics of the wireless sensor network which will help the researchers and industry to design a functional WSN with maximum throughput using minimum resources with a low cost. There are different types of topologies of wireless sensor networks each topologies have different performance. The application of wireless sensor network in the area of healthcare, military, environmental, industrial etc. These applications are possible flexibility, fault tolerance, low cost. Though wireless sensor networks are constrained by scalability, cost, topology change and power consumption, new technologies are being devised to overcome these and to make sensor networks an integral part of our lives. The future prospects of wireless sensor network applications are highly promising to revolutionize our everyday lives.

REFERENCES

[1] http://en.wikipedia.org/wiki/Sensor_Networks

[2] Kazem Sohraby, Danielminoli, Taieb Znati,— WIRELESS SENSOR NETWORKS: Technology, Protocols, and Applications‖, published by John Wiley & Sons, Inc., Hoboken ew Jersey, 2007.s

[3] http://www.google.com/sensor- networks topologies

[4] E. Amir, S. McCanne, and R. Katz. An active service framework and its application to real- time multimedia transcoding. In SIGCOMM '98: Proceedings of the ACM SIGCOMM '98 conference on Applications, technologies, architectures, and protocols for computer communication, pages 178–189. ACM Press, 1998.

[5] A. Flemmini, P. Ferrari, D. Marioli, E. Sisinni, and A. Taroni, ―Wired and wireless sensor networks for industrial applications,‖ Microelectronics Journal, vol. 40, pp. 1322-1336, September 2009.

[6] F. Salvadori, M. D. Campos, P. S. Sausen, R. F. D. Camargo, C. Gehrke, C. Rech, M. A. Spohn, and A. C. Oliveira, ―Monitoring in industrial systems using wireless sensor network with dynamic power management,‖ IEEE Trans. on Instrumentation and Measurement, vol. 58, no. 9, pp. 3104-3111, September 2009.

[7] Culler, D.; Estrin, D.; Srivastava, M. Overview of sensor networks. IEEE Comput. Mag. 2004,37, 41–49.

[8] H. Karl, A, Willing, ―Protocols and Architectures for Wireless Sensor Networks‖. New York: Wiley, 2005. 314−340, 2005.

[9] http://www.sensornetworks.net.au/applic_health.html http://en.wikipedia.org wiki / Sensor _ Networks

Quantum and Electrochemical Studies of Ecofriendly and Green Corrosion Inhibitor Lonic Liquid for Metal Surface in 0.5 M Sulfuric Acid

Bhaskaran[*a], Gurmeet Kaur[b] , Raj Kishore Sharmaa and Gurmeet Singh[*a]

[a]Department of Chemistry, University of Delhi, Delhi-110 007

[b]SGTB Khalsa College, University of Delhi, Delhi-110007

*(gurmeet123@yahoo.com), *(bhaskaryadav7@gmail.com)

ABSTRACT

An ionic liquid-like imidazolium was synthesized and characterized by 1H, 13C, and I.R spectroscopy. Anticorrosion impacts of the1-Butyl-3-Ethyl imidazolium bromide ionic liquid were studied. The analysis was observed by Tafel plot and Electrochemical Impedance Spectroscopy which show high mitigation efficiency in 0.5 M H2SO4 solution. Electrochemical studies revealed that the investigated compound is a mixed-type of inhibitor and Langmuir adsorption isotherm is observed. The mitigation efficiency was increased with an increase in concentration. The corrosion mitigation influence of 1-Butyl-3-Ethyl imidazolium bromide is observed due to the adsorptive interaction with the surface of mild steel which formed a protective layer against corrosion. The quantum chemical calculations supplement the results of polarization studies.

INTRODUCTION:

To achieve the optimum performance of industrial equipment and machinery, scale and oxide are isolated from the metallic surface to reduce the corrosive product formation. During the pickling procedure, acidic solutions are generally employed [1-3]. Carbon steel products are mostly treated with solutions of HCl and H2SO4. The exceedingly corrosive nature of these solutions, in turn, affect the physicochemical properties of the carbon steel materials. As a consequence of this, the corrosion inhibitors method is used for the protection of metallic materials against corrosion loss is employed. From the most recent years several organic compounds of nitrogen, such as pyridines, imidazolines [4-5], and azoles, have revealed high action for the inhibition ofcorrosion. In spite, of this, the toxicity of these compounds is endangering the environment.

Researchers have diverted *Corresponding Authors their interest in ionic liquids as corrosion inhibitors because of their green nature towards the environment. Ionic liquids (ILs) are a captivating collection of solvents possessing a distinctive mixture of physicochemical properties, encountering extremely low vapor pressure at room temperature, low melting point, chemical, and thermal stability. They also hold the wide liquid range with the capability to dissolve both polar and non-polar inorganic and organic compounds. For this reason, in various chemical processes ionic liquids [6-8] can replace many volatile organic solvents, together with synthesis, extraction, catalysis, and separation. The cationic and anionic parts of ionic liquids are the deciding factor for the overall physical and chemical properties of a given ionic liquid. The variation of cationic and anionic part invariably affect the various physical properties of ionic liquid such as miscibility, solvation, viscosity, hydrophilicity. Ionic liquids can be categorized as "customized solvents" because they can be modified and adapted according to conditions.

In the current investigation, 1-Butyl-3-Ethyl Imidazolium Bromide Ionic Liquid [BEIM]Br has been read as corrosion mitigators for Mild steel (MS) in 0.5 M H2SO4. Electrochemical strategies including tafel plot and electrochemical impedance spectroscopy have been executed to find out corrosion

inhibition properties of MS in presence of 0.5 M H2SO4. This IL examined has indicated anticorrosive properties. The hindrance efficiencies were affirmed by the electrochemical tests, which were additionally enhanced by quantum studies.

Galvanostatic Polarization Studies:-

The polarization parameters Ecorr, Icorr, βa, βc are listed in Table 1. Tafel bends for MS in 0.5 M H2SO4 solution at various concentrations of [BEIM]Br have appeared in Fig.1. Through this examination, it is seen that the presence of [BEIM]Br IL caused a conspicuous decline in the consumption rate. Table 1. shows that the corrosion current thickness diminishes with anexpansion in the convergence of the inhibitor and [BEIM]Br while the relief productivity diminishes with the increment in temperature of the system [9-12].

Electrochemical Impedance Spectroscopy:-

Electrochemical impedance studies show that with an increase in the concentration of [BEIM]Br, charge transfer resistance (Rct) increases which gives a clear indication that there is a formation of a protective layer between metal-solution interface. Moreover, Cdl value (Table 2) also decreases with an increase in the concentration of inhibitor which provides information that the thickness of the electric double layer has considerably increased thereby giving better corrosion inhibition. Nevertheless, the sizes of the capacitive loops are increased [13-14].

Thermodynamic Studies

Thermodynamic datas were determined to clarify the adsorption behavior of inhibitor on the metal surface. The Datas as given in Table 3 demonstrate that the adsorption cycle is for the most part by chemisorption[15,16]. which is ascribed to ΔG˚ads valve - 82.35 kJ mol-1. The estimation of R2 i.e regression coefficient of the adsorption process shows that the Langmuir adsorption model is trailed by inhibitor. so Mitigation effectiveness turns into the capacity of the electrode surface secured by the inhibitor molecules [17,18]. The free vitality of adsorption can be determined from Kads utilizing Eq. (1).

$$K_{ads} = \frac{1}{55.5} exp\left[\frac{-\Delta Gad}{RT}\right] \quad (1)$$

The following equation (2) represents the adsorption isotherm relationship for Langmuir Adsorption Isotherm

$$\frac{C}{\theta} = \frac{1}{K_{ads.}} + C \quad (2)$$

Quantum Chemical Studies:-

The streamlined structure of ILs, energies of HOMO and LUMO, absolute charge density, complete current potential, 3D isosurface of all out charge thickness on the inhibitors per unit area are given in Fig. 3 and the various quantum studied data are recorded in Table 4.

The distinction between EHOMO and ELUMO (the energy gap, ΔE) is a significant boundary in choosing the alleviation strength of the inhibitor particles. The lower the distinction in ELUMO and EHOMO, the higher will be the relief proficiency which is because of the simplicity of adsorption on the metal surface. (19,20).

CONCLUSION:-

(1) [BEIM]Br principally adsorbs on the MS surface through the emphatically charged N-heterocyclic particle in the imidazole ring, and it complies with the Langmuir isotherm dynamic model.

(2) [BEIM]Br displays a decent inhibitive exhibition because of the strong electron-donating effect of the alkyl group.

(3) Activation Energy(Eact) values are higher in the presence when contrasted with without inhibitors, showing that disintegration of MS is slow within [BEIM]Br .

Affirmation:-

The Authors appreciatively recognize University of Delhi for Research and Development grant and the Director of USIC for doing phantom investigations.

REFERENCES

1. Q.B. Zhang, Y.X. Hua, Electrochim. Acta 54 (2009) 1881–1887.

2. A. Subramania, N.T. Kalyama Sundaram, R. Sathiya Priya, K. Saminathan, V.S.Muralidharan, T. Vasudevan, J. Appl. Electrochem. 34 (2004) 693–696.

3. D. Kuang, P. Wang, S. Ito, M. Zakeeruddin, M. Gratzel, J. Am. Chem. Soc. 128 (2006) 7732–7733.

4. D. Zhao, Z. Fei, T.J. Geldbach, R. Scopelliti, P.J. Dyson, J. Am. Chem. Soc. 126 (2004) 15876–15882.

5. K. M. Manamela, L. C. Murulana, M. M. Kabanda, E. E. Ebenso, Int. J. Electrochem. Sci. 9 (2014) 3029-3046.

6. O. Olivares-Xometl, C. Lopez-Aguilar, P. Herrastí-Gonzalez, N. V. Likhanova, I. Lijanova, R. Martinez-Palou, J. Antonio Rivera-Marquez, Ind. Eng. Chem. Res. 53 (2014) 9534−9543.

7. X. Zheng, S. Zhang, M. Gong, W. Li, Ind. Eng. Chem. Res. 53 (2014) 16349−16358.

8. D. Guzm_an-Lucero, O. Olivares-Xometl, R. Martinez-alou, N. V. Likhanova, M. A. Dominguez-Aguilar, V. Garibay-Febles, Ind. Eng. Chem. Res. 50 (2011) 7129–7140.

9. L. C. Murulana, A. K. Singh, S. K. Shukla, M. M. Kabanda, E. E. Ebenso, Ind. Eng. Chem. Res. 51 (2012) 13282–99.

10. M. H. Wahdan, A. A. Hermas, M. S. Morad, Mater. Chem. Phys. 76(2) (2002) 111-118.

11. L. B. Tang, G. H. Liu, Mater. Chem. Phys. 95 (2006) 29–38.

12. Q. B. Zhang, Y. X. Hua, Electrochim Acta. 54 (2009) 1881-1887.

13. S. M. Tawfik, J. Mol. Liq. 207 (2015) 185-194.

14. H. Vashisht, I. Bahadur, S. Kumar, M. S. Goyal, G. Kaur, G. Singh, L. Katata-Seru, E. E. Ebenso, J. Mol. Liq. 224 (2016) 19-29.

15. J. H. Ha, J. H. Cho, J. H. Kim, B. W. Cho, S. H. Oh, J. Power Sources 355 (2017) 90-97.

16. P. Huanga, J. A. Lathama, D. R. MacFarlaneb, P. C. Howletta, M. Forsyth, Electrochimica. Acta. 110 (2013) 501– 510.

17. P. Kannan, J. Karthikeyan, P. Murugan, T. S. Rao, N. Rajendran, J. Mol. Liq. 221 (2016) 368–380.

18. A. A. Olajire, J. Mol. Liq. 248 (2017) 775–808.

19. E. Heakal, A. S. Fouda, M. S. Radwan, Mater. Chem. Phys. 125 (2011) 26–36

20. L. C. Murulana, A. K. Singh, S. K. Shukla, M. M. Kabanda, E. E. Ebenso, Ind. Eng. Chem. Res. 51 (2012) 13282−13299.

21. G. Gece, Corros. Sci. 50 (2008) 2981–2992.

22. N.O. Obi-Egbedi, I. B. Obot, Corros. Sci. 53 (2011) 263–275

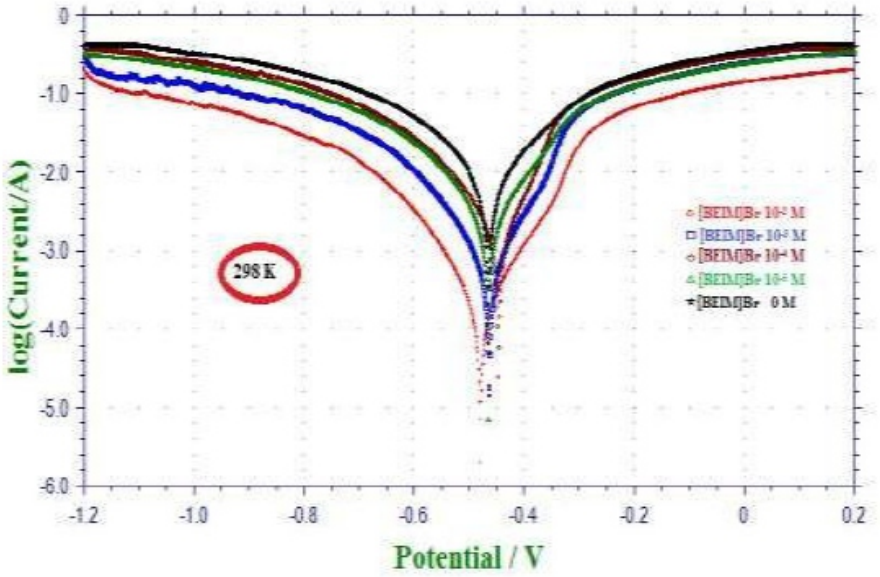


Fig.1. Tafel Polarization Values for the Corrosion of MS in 0.5 M H2SO4 with [BEIM]Br at 298 K

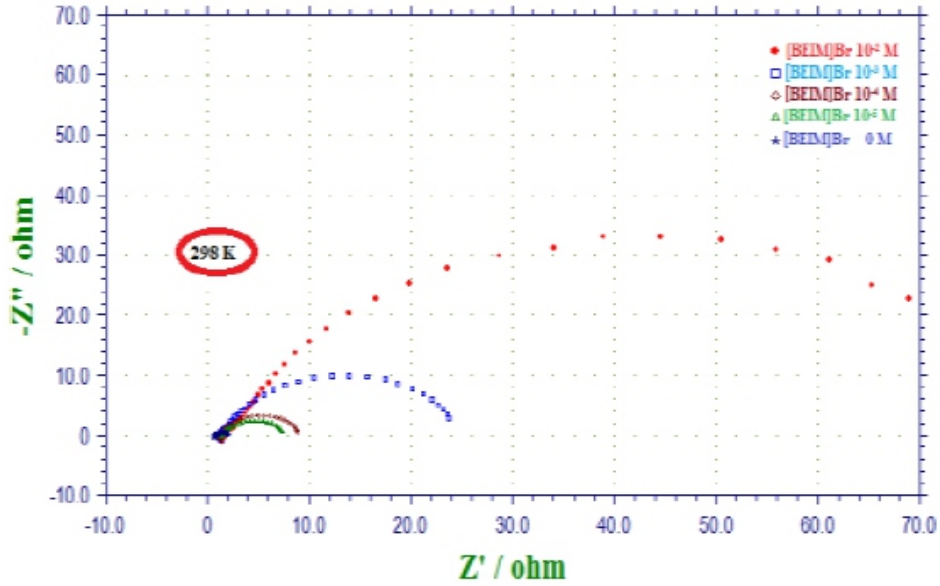


Fig.2. The nyquist curve for the Corrosion mitigation of MS in 0.5 M H2SO4 in the Presence and Absence of [BEIM]Br at 298 K

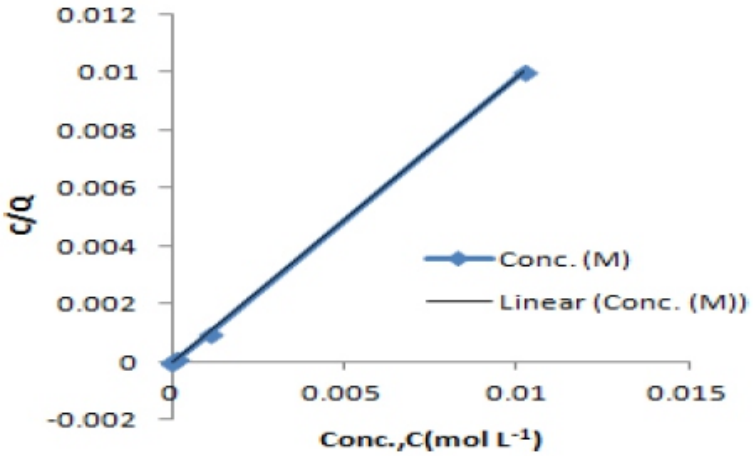


Fig.3. Adsorption behavior of [BEIM]Br on the mild steel surface in 0.5 M H2SO4

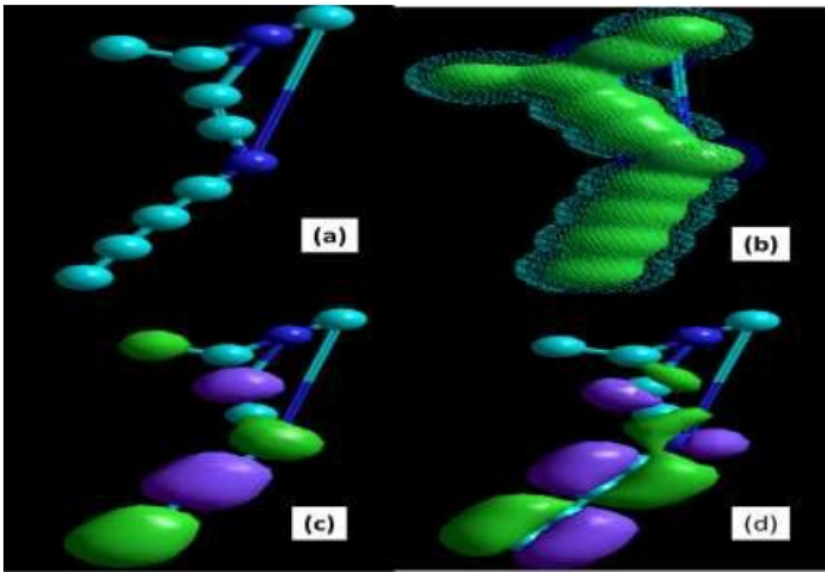


Fig. 4. (a) Structure of [BEIM]Br (b) Total Charge Density of [BEIM]Br (c) HOMO of [BEIM]Br (d) LUMO of [BEIM]Br

Table 1: Tafel polarization datas for the consumption of Metal surface in 0.5 M H2SO4 with presence and nonappearance of [BEIM]Br at 298 K

Temp. (K)	Conc. (mol/L)	I_{corr} (mA/cm^2)	$-E_{corr}$ (mV)	b_a (mV/dec.)	b_c (mV/dec.)	IE%
298	*Blank*	9.679	465	70.59	60.89	-
	10^{-5}	2.800	465	108.28	137.21	68.19
	10^{-4}	1.545	447	63.19	129.29	82.45
	10^{-3}	0.653	463	77.74	114.62	92.57
	10^{-2}	0.199	478	92.62	103.46	97.74

Table 2: Impedance boundaries for the consumption of Metal surface in 0.5 M H2SO4 with presence and nonappearance of [BEIM]Br at 298 K

Solutions	Conc. (M)	R_{ct}	F_{max}	C_{dl}	I.E
H_2SO_4	0.5	1.65	21.23	4.54×10^{-3}	-
[BEIM]Br	10^{-5}	5.97	2.10	1.26×10^{-2}	72.36
	10^{-4}	7.63	14.36	1.45×10^{-3}	78.37
	10^{-3}	22.60	8.07	8.72×10^{-4}	92.70
	10^{-2}	67.35	3.09	7.65×10^{-4}	97.55

Table 3: Thermodynamic parameters for the mitigation of Metal surface in 0.5 M H2SO4 with presence and nonappearance of [BEIM]Br at 298 K

Inhibitor	Temperature (K)	Log K_{ads}	R^2	$-\Delta G^{\circ}_{ads}$ (kJ mol^{-1})
[BEIM]Br	298	10.41	0.9984	82.35

Table 4: Quantum Chemical parameters for [BEIM]Br

Quantum	Para Meters
Binding Energy (kcal/mol)	-35723
Heat of Formation (kcal/mol)	450.78
Dipole Moment (Debye)	1.54
E_{HOMO} (eV)	-9.581
E_{LUMO} (eV)	-2.925
E_{HOMO}- E_{LUMO} (eV)	-6.656

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.

Note