Online ISSN : 0975-4172
Print ISSN : 0975-4350

Global Journal

of Computer Science and Technology: E

Network, Web & Security

Highlights

Wireless Sensor Networks

Text Partition Algorithm

Ant Colony Optimization

Secure Routing Protocol

Discovering Thoughts, Inventing Future

VOLUME 13 ISSUE 4 VERSION 1.0

Global Journal of Computer Science and Technology: E
Network, Web & Security

Global Journal of Computer Science and Technology: E
Network, Web & Security

Volume 13 Issue 4 (Ver. 1.0)

Open Association of Research Society

Incorporation No.: 0423089
License No.: 42125/022010/1186
Registration No.: 430374
Import-Export Code: 1109007027
Employer Identification Number (EIN):
USA Tax ID: 98-0673427

Global Journals Inc.

(A Delaware USA Incorporation with "Good Standing"; Reg. Number: 0423089)

Sponsors: *Open Association of Research Society*
Open Scientific Standards

Publisher's Headquarters office

Global Journals Inc., Headquarters Corporate Office, Cambridge Office Center, II Canal Park, Floor No. 5th, ***Cambridge (Massachusetts)***, Pin: MA 02141
United States
USA Toll Free: +001-888-839-7392
USA Toll Free Fax: +001-888-839-7392

Offset Typesetting

Global Association of Research, Marsh Road, Rainham, Essex, London RM13 8EU
United Kingdom.

Packaging & Continental Dispatching

Global Journals, India

Find a correspondence nodal officer near you

To find nodal officer of your country, please email us at *local@globaljournals.org*

eContacts

Press Inquiries: *press@globaljournals.org*
Investor Inquiries: *investers@globaljournals.org*
Technical Support: *technology@globaljournals.org*
Media & Releases: *media@globaljournals.org*

Pricing (Including by Air Parcel Charges):

For Authors:

22 USD (B/W) & 50 USD (Color)

Yearly Subscription (Personal & Institutional):

200 USD (B/W) & 250 USD (Color)

Editorial Board Members (HON.)

Dr. Bart Lambrecht
Director of Research in Accounting and FinanceProfessor of Finance
Lancaster University Management School
BA (Antwerp); MPhil, MA, PhD (Cambridge)

Dr. Carlos García Pont
Associate Professor of Marketing
IESE Business School, University of Navarra
Doctor of Philosophy (Management), Massachusetts Institute of Technology (MIT)
Master in Business Administration, IESE, University of Navarra
Degree in Industrial Engineering, Universitat Politècnica de Catalunya

Dr. Fotini Labropulu
Mathematics - Luther College
University of ReginaPh.D., M.Sc. in Mathematics
B.A. (Honors) in Mathematics
University of Windso

Dr. Lynn Lim
Reader in Business and Marketing
Roehampton University, London
BCom, PGDip, MBA (Distinction), PhD, FHEA

Dr. Mihaly Mezei
ASSOCIATE PROFESSOR
Department of Structural and Chemical Biology, Mount Sinai School of Medical Center
Ph.D., Etvs Lornd University
Postdoctoral Training,
New York University

Dr. Söhnke M. Bartram
Department of Accounting and FinanceLancaster University Management SchoolPh.D. (WHU Koblenz)
MBA/BBA (University of Saarbrücken)

Dr. Miguel Angel Ariño
Professor of Decision Sciences
IESE Business School
Barcelona, Spain (Universidad de Navarra)
CEIBS (China Europe International Business School).
Beijing, Shanghai and Shenzhen
Ph.D. in Mathematics
University of Barcelona
BA in Mathematics (Licenciatura)
University of Barcelona

Philip G. Moscoso
Technology and Operations Management
IESE Business School, University of Navarra
Ph.D in Industrial Engineering and Management, ETH Zurich
M.Sc. in Chemical Engineering, ETH Zurich

Dr. Sanjay Dixit, M.D.
Director, EP Laboratories, Philadelphia VA Medical Center
Cardiovascular Medicine - Cardiac Arrhythmia
Univ of Penn School of Medicine

Dr. Han-Xiang Deng
MD., Ph.D
Associate Professor and Research Department Division of Neuromuscular Medicine
Davee Department of Neurology and Clinical NeuroscienceNorthwestern University
Feinberg School of Medicine

Contents of the Volume

Global Journal of Computer Science and Technology
Network, Web & Security
Volume 13 Issue 4 Version 1.0 Year 2013
Type: Double Blind Peer Reviewed International Research Journal
Publisher: Global Journals Inc. (USA)
Online ISSN: 0975-4172 & Print ISSN: 0975-4350

Overlapped Text Partition Algorithm for Pattern Matching on Hypercube Networked Model

By Prof. KSMV Kumar, Prof. S. Viswanadha Raju & Prof. A. Govardhan
Jawaharlal Nehru Technological University

Abstract - The web has been continuously growing and getting hourglass shape. The indexed web is measured to contain at least 30 billion pages. It is no surprise that searching data poses serious challenges in terms of quality and speed. Another important subtask of the pattern discovery process is sting matching, where in which the pattern occurrence is already known and we need determine how often and where it is occurs in given text. The target of current research challenges and identified the new trends i.e distributed environment where in which the given text file is divided into subparts and distributed to N no. of processors organized in hypercube networked fashion .To improve the search speed and reduce the time complexity we need to run the string matching algorithms in parallel distributed environment called as hypercube networked model using RMI method. we considered both KV-KMP and KV-boyer-moore string matching algorithms for pattern matching in large text data bases using three data sets and graph's drawn for different patterns.

Keywords : indexed web, pattern, text, distributed, hypercube network, RMI method and string matching.

GJCST-E Classification : C.2.5

OVERLAPPED TEXT PARTITION ALGORITHM FOR PATTERN MATCHING ON HYPERCUBE NETWORKED MODEL

Strictly as per the compliance and regulations of:

Overlapped Text Partition Algorithm for Pattern Matching on Hypercube Networked Model

Prof. KSMV Kumar [α], Prof. S. Viswanadha Raju [σ] & Prof. A. Govardhan [ρ]

Abstract - The web has been continuously growing and getting hourglass shape. The indexed web is measured to contain at least 30 billion pages. It is no surprise that searching data poses serious challenges in terms of quality and speed. Another important subtask of the pattern discovery process is sting matching, where in which the pattern occurrence is already known and we need determine how often and where it is occurs in given text. The target of current research challenges and identified the new trends i.e distributed environment where in which the given text file is divided into subparts and distributed to N no. of processors organized in hypercube networked fashion .To improve the search speed and reduce the time complexity we need to run the string matching algorithms in parallel distributed environment called as hypercube networked model using RMI method. we considered both KV-KMP and KV-boyer-moore string matching algorithms for pattern matching in large text data bases using three data sets and graph's drawn for different patterns.

Keywords : indexed web, pattern, text, distributed, hypercube network, RMI method and string matching.

I. Introduction

String matching diversely used in many areas of computer sciences. It has been one of the prominent issues of information retrieval system. Some standard algorithms have been used for processing text files against patterns, for example in manipulation of text, text compression, network analysis and also in data retrieval systems. The algorithms studied in the present character forms the basic components in its software implementation and also serve as a model in fields of computer science like system design purposes, web search engines, computer virus signature matching and networking [1]. Rapid growth of abundant information makes necessary to have efficient methods for information retrieval. Coping with the growth of the web and query traffic requires scalable information retrieval systems. Today commercial search engines are fully automatic and their web index on a few data centers [2]. It is tedious task to come up with scalable indexing and query processing techniques for next generation IRS in the coming future.

The web comprises wide variety of content in the form of structured Meta data, databases, maps, images, videos and textual documents etc. [1]. The main challenge of present IRS may be scalability. A recent trends envisions that the number of servers required by a search engines to keep up with the load in 2010 may be in the order of millions as such the text size is increasing to tens of billions of pages [1,2]. Hence it is very urgent to design a truly distributed large scale systems that enables fast and accurate search over very large amount of content [15]. In this paper we mainly focus on pattern matching on distributed environment called as hypercube network model using RMI method [14]. Given a pattern may be more common or more specific, we wish to count how many times it occurs in the text and to point out its occurrence positions. For pattern matching we used Kumar Viswanadha-KMP and Kumar Viswanadha- Boyer Moore string matching algorithms for different text files against different pattern files [2, 3]. Basically Boyer -Moore algorithm is works based on two heuristics: bad character heuristics and good suffix heuristics. The text files is partitioned and processed in two ways, one is non-overlapping and second is overlapping text partitioned processing [2]. In both the cases KV-KMP and KV-BM are applied for string matching (pattern matching) and the remote server will be invoked using JAVA RMI method on hypercube networked model to reduce the search time.

The paper is organized as follows section II deals with literature survey of string matching in parallel environment, section III deals with text processing techniques called as overlapping and non-overlapping text partitioned in divide and conquer paradigm. Section IV explains about the hypercube model networked systems. Section V presents experimental setup. Result analysis and discussions were discussed in section VI and VII is conclusion. Section VIII gives the references.

II. Literaure Survey

Large amounts of data and textual information has been continuously increasing in many fields of information systems. Rapid growth of abundant information makes necessary to have efficient methods for information retrieval [1]. This chapter will give an idea how far the algorithms have helped in achieving the desired information along with its time complexities. String matching scan be accomplished by designing algorithms in two categories namely, *exact string*

Author α : KSMV KUMAR, Association Prof in CSE Dept. SIET, IBP, AP, India-501506. E-mail : ksmvkumar@yahoo.co.in
Author σ : S. Viswanadha Raju, Professor in CSE Dept. JNTUH, Jagityal, AP, India-500000. E-mail : svihere@here.com
Author ρ : A. Govardhan professor in CSE Dept. JNTUH, kukatpally, HYD. AP, India - 500085. E-mail : agovarancse@yahoo.com

Global Journal of Computer Science and Technology (E) Volume XIII Issue IV Version I Year 2013

matching algorithms that locates exact match of the pattern in the text string or source string and *approximate string matching* algorithms that finds closest possible match of pattern in the text with some mismatches. Exact string matching problem can be addressed in two ways *software based approach* or *hardware based approach*. Software based algorithms are slow on comparison with hardware based [22]. Hardware based solutions to string matching provides efficient data storage and fast matching [12]. String matching application in network intrusion detection systems require that the matching shall be accomplished at wire speed , software based solutions could not afford this, due to which hardware based algorithms are chosen mostly over software grounded algorithms. The algorithms discussed below addresses mostly exact string matching. Text represents an important form of data involving a lot of operations [6]. Pattern matching is one of the problems encountered in text manipulation. It is about searching and locating substring within a sequence of characters in a raw text.

a) Software Based String Matching Algorithms

In 1972, Cook exhibited string matching using two way push down auto meta and solved pattern matching in O(m+n) time in worst case where m and n are the lengths of text and pattern respectively[19]. However in 1977 Rivest determined that every string matching algorithm must go through at least n-m+1 comparison at worst. This shows there is no solution of obtaining a sub linear n worst time in solving the issue. It means the time needed to run an algorithm must be a function of its input size. The next algorithm discussed makes an attempt to achieve a sub-linear matching time.

Donald Knuth-Voughan Pratt-James H. Morrris (1977) basing on modifications of Cook's theorem came up with a new string matching algorithm popularly known as KMP Algorithm, briefly discussed below [3]. It is the first linear pattern matching algorithm discovered with a run time of O(m+n).

i. *Knuth-Morris-Pratt Algorithm*

Knuth Morris Pratt's string matching algorithm employs exact string matching technique with linear time complexity [3]. It involves pattern preprocessing .It scans the text string from left to right for pattern matching, while scanning the text it stores the information about the matched characters and whenever a mismatch occurs it uses this information to avoid unnecessary comparisons by sometimes shifting more than one position. It thus avoids backtracking and reduces the number of comparisons unlike naïve approach which wastes the scan information. The present algorithm uses a sliding window which slides over text string and makes shifts as per mismatches. It smartly shifts the pattern over text than the brute-force approach. Window shift uses a KMP formulated prefix function obtained by preprocessing pattern to reduce unnecessary comparisons. The algorithm uses this function to decide about the number of characters to be skipped while shifting the window whenever a mismatch takes place.

ii. *Aho-Corasick Algorithm*

Unix fgrep command implementation is based on Aho-Corasick algorithm which locates finite and fixed set of strings in a file and outputs the lines containing at least one of the strings [8]. Consider a dictionary (X) containing a fixed set of strings and a text denoted by Y. Let k be the number of strings present in X. Suppose if we wish to find all the occurrences of all the strings of a dictionary. The simple solution would be to repeatedly implement few string matching algorithms on each string .The time complexity of this operation will be O(m+n*k), where m is the sum of the lengths of the k strings of dictionary X and n is the length of the text Y. This indicates the inefficiency of this approach as the text has to be read for k times. This problem is addressed by Aho-Corasick algorithm discussed below, it undergoes sequential read of the text and run time would be O(m+n).The present algorithm extends the weaker versions of Knuth-Morris-Pratt algorithm and also fastly matches a number of patterns at one time against a single text [3].

This algorithm locates all the occurrences of finite number of keywords in a string of text. It involves construction of a finite state pattern matching machine, an automaton and then uses the machine for text processing in a single. A keyword is a finite set of strings denoted by K= $y_1, y_2,\ldots y_n$ and let X be an arbitrary text string. Pattern matching machine employs three functions namely, goto function *g*, failure function *f*, and output function *output*.

iii. *Boyer Moore Algorithm*

*B*ob Boyer and J. Strother Moore discovered this algorithm in the year 1977 which is known as one of the most efficient algorithms and also stands as a benchmark for string matching process [6]. The algorithm compares pattern string within a sliding window over a text string, employing right to left scan of characters inside the window where as the window slides from left to right over the text. The aim of this algorithm is to avoid certain fragments of text that are not eligible for comparison. This decision is taken by placing the window in left alignment with text. The algorithm starts comparing the pattern characters with the text characters in the order of right to left. If 'm' being the length of pattern (x), the algorithm compares $x_m=y_m$, where 'y' symbolizes text. On true result of this comparison the procedure continues with $x_{m-1}=y_{m-1}$ and on the occurrence of false, the algorithm makes two ways out. One is named as bad character shift or occurrence shift and the other is called as good suffix shift or better factor shift or sometimes matching shift.

On grounds of these two measures the window makes shifts and locates the pattern. These measures are explained in the following paragraphs with an example demonstration.

iv. *Horspool Algorithm*

Boyer Moore algorithm uses two gauges to know shift distance. Good suffix shift is quite complicate to implement so there was a need of a simplified algorithm using bad character measure [7]. This algorithm is a simplification of Boyer –Moore algorithm based on bad character shift. It has been produced by Nigel Horspool in the year 1980.The reason for this simplification is pattern is not always periodic. The concept used is when a bad character, reason for a mismatch is encountered; the shift decision is made by analyzing the characters towards the right of the text window.

a. *Working Principle*

The process starts by a window on text string of size equal to pattern. The scan of elements goes through right to left inside the window whereas the window slides from left to right over the text.

When a mismatch is countered for some wt[i] != wp[j], $0 \leq (i, j) < m$, wt→ text window character and wp → pattern window character. Then the match of the right most character of the text window is looked in the pattern so that wt [m-1] = wt[i], where $0 \leq i < m-1$, when both found the characters are therefore aligned causing a window shift.

Case I: Suppose the bad character does not exist in the pattern then shift the whole window of size pattern.

Case II: There exists two matches of the bad character in the pattern then the rightmost character is preferred.

b) Hardware Based String Matching Algorithms

i. *Mishina Algorithm*

Mishina produced a string matching algorithm for vector processors in the year 1993.This algorithm is used by Hitachi's pipelined vector processor and Integrated vector processor. A vector processor also known as an array processor is a CPU which executes instructions in a single dimensional array of data items [20]. Meaning it can perform parallel computations on the elements of array. The current algorithm works in two phases: *cutout* and *check.* In the first phase, that is in cutout segment the text string is divided into autonomous serviceable substrings so that each substring can be tested for equality with respective pattern strings in a pipeline using array processors. In the next phase, as the name indicates check phase, a string matching algorithm is employed to perform pattern matching. Here Aho-Corasick algorithm is applied to all substrings drawn from the cutout part. This way of applying string matching is ten times faster than the scalar string matching using Aho-Corasick algorithm.

ii. *Sidhu's Algorithm for String Matching using Hardware Technology*

The algorithm is grounded on non-deterministic finite state machine (NFSM) for regular expression matching. In the field of computing, regular expression gives a concise meaning to "match" [21]. The pattern can match one or more text strings. A non-deterministic finite state machine or automaton is a state machine resembles a directed graph that exhibits different states represented by nodes and edges designate character or empty string. The algorithm works by generating regular expressions for every string and NFSM examines the input at a speed of one byte at a time. This approach needs a time of O(m), m symbolize pattern length. NFSMs are tough to implement and requires rebuilding every time a string is added making it complicated.

c) String Matching Based on FM-Index

Despite of many algorithms presented on string matching, the present attempt to solve string matching problem uses FM-index technique that concatenates the attributes of suffix array and Burrows-Wheeler transformation [22]. To understand the working of this architecture the above concepts has to be acknowledged. The next segment of this section presents a detailed discussion of it.

i. *2D-LARPBS*

It represents two-dimensional LARPBS. The model has the system's buses arranged in a two-dimensional set up that makes communication among buses more effective [23]. It can be use for the design of both exact and approximate string matching. The construction of these algorithms is based on Hamming distance.

ii. *Hamming Distance*

Hamming distance measures the amount of inequality between two strings. It can be applied for error detection and correction. For any two strings it gives the number of the corresponding characters that are dissimilar. Using this measure the knowledge of closeness of two strings can be known and thus gives an idea about the operations to be done to obtain one string from another.

a. *Formal Definition of Hamming Distance*

For strings A and B with same length k, the Hamming distance H (A, B) is given by

H (A, B) = no. of positions where A[i]!=B[i] and $0 < i < k$.

III. Text Processing Techniques

Making text ready to be scanned for string search so that it helps yield reduced search time is text processing. In the previous chapter's literature it was determined that to improve time complexities of string matching approaches parallelization has to be adopted. The root lead towards this starts with divide and conquers procedure and dynamic partition techniques intended for parallel processing, and are presented in the current chapter.

a) Divide and Conquer Paradigm

i. *Introduction*

Decomposing a complex problem into two or more smaller sub-problems until a simple portion is obtained for easy solvability is dividing and conquer paradigm as the name suggests [2]. If the problem is easy it can be solved directly but if a complicated problem persists then breaking into its small instances and solving each instance independently resembles divide and conquer strategy. The solutions to the smaller versions of main problem are clubbed up to attain actual solution to the original instance. It adopts the recursive division while undergoing the breaking up of a problem. The goodness of using divide and conquer strategy lies in the point that it stands as a powerful tool in solving conceptually tough problems [12]. The algorithms implementing divide and conquer paradigm are often found to be efficient. It is also considered an apt algorithm to be executed in multi-processing environment as distinct sub-parts of a problem can be executed in parallel on different machines. The general stages of this strategy would be divide, conquer (solve) and unite.

b) Generic Divide and Conquer Algorithm

Input: Problem P and n = Size (P)

Output: S = Solution (P)

Begin

Step 1: If n is small Solve (P)

Step 2: Else divide P into sub-problems p1 and p2 of lengths n1 and n2 respectively such that

$$n1 \approx n2 \approx n/2$$

Step 3: Conquer

$$S1 \leftarrow \text{solve } (p1, n1)$$
$$S2 \leftarrow \text{solve } (p2, n2)$$

Step 4: Unite solutions to obtain actual solution

$$S \leftarrow \text{unite } (s1, s2)$$

End

IV. Hypercube Network Topology

A hypercube is a geometrical figure in four or more dimensions similar to a cube in three dimensions with all its edges having equidistant from their respective nodes. For an n-dimensional hypercube, there are 2^n vertices and $n*2^{n-1}$ number of edges. In a network, a node is a connection point or a redistribution point, more formally in a physical network it is an electronic device that can send, receive or forward information over the communication channel to other nodes in the network where as edges provides access to the network and also involves in transmitting information in a network over the nodes [24]. A router is an example of an edge device in a network.

In computer science, a hypercube network is a configuration of multiple parallel processors having distributed memory such that the locations of the processors are analogous to the vertices of a mathematical hypercube and the links correspond to the edges. For an n-dimensional hypercube, as mentioned above, it has 2^n processing nodes and $n*2^{n-1}$ edges coupled in an n-dimensional cube network. The 2^n nodes are designated by binary numbers from 0 to 2^n-1. The nodes are connected by links responsible for intercommunication. The two nodes are connected if the binary numbers assigned to it stand apart by exactly one bit position.

a) Message Transmission in Hypercube Network

Every node in the network has the ability to send, receive and transmit data to other nodes. The information that is passed is in the form of packets. Every node is represented by a unique id that is presented in the binary form. For n-dimensional hypercube, every node is represented in n-bits.

b) Algorithm to find the shortest path for transmitting message from source node to target node

Input: Source node $S_{n-1}S_{n-2}.....S_3S_2S_1S_0$, Target Node $T_{n-1}T_{n-2}.....T_3T_2T_1T_0$.

Output: Path of transmission.

Begin

Step 1: Equate each bits of the source node with target node beginning with the right-most bit that is from the LSB of Source node. Formally, compare S_0 with T_0.

Step 2: On encountering inequality, if S0!=T0 then complement the respective bit to get the next intermediate node for transmission. The next bit would be $S_{n-1}S_{n-2}.....S_3S_2S_1S_0{}^c$.

Step 3: Repeat steps 1 and 2 for each of all the bits preceding LSB exclusively till the target node is obtained.

End.

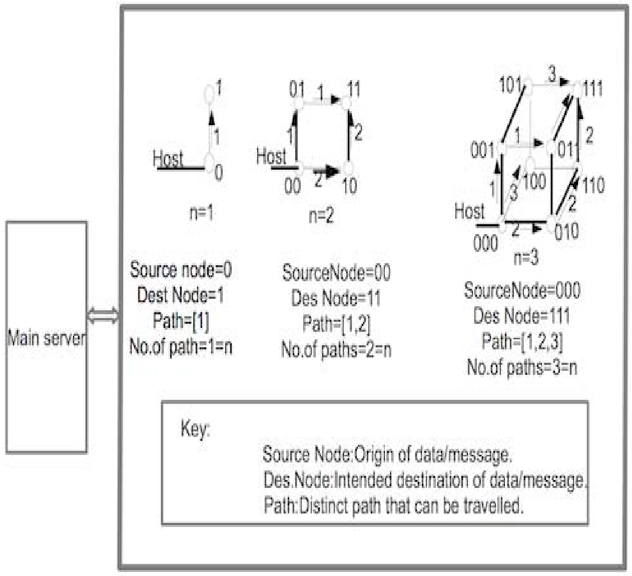


Figure 1 : Distinct Communication Patts.

In the above figure circles shows the node and arrow mark shows the path which connects the server/nodes. The main server which is connected from the outside the hypercube network servers, such that connection establishes from host node to destination node and path is established to broadcast the text files and pattern files with the help of hypercube program. Path direction along with the node numbers are shown in the above diagram for n=1 means two node H.C, n=2 means four node H.C and n= 3 means eight node H.C.

V. Experimental Setup

Experimental setup required for the above implementation is more processors P(at least four) connected with hypercube model on INTERNET of either similar systems (homogeneous) or dissimilar systems (heterogeneous). P processors where 0<P<5 and time, by taking K patterns where 0<K<4 as key factor, before conducting test [2].

a) *Parallel kumar viswanadha and Boyer Moore String Matching Employing Overlapped Text Partitions*

The algorithm implements Boyer Moore string matching algorithm in a parallel environment. The input text string is sliced into *'i'* subtexts such that each text partition holds (n/P)+m-1 text string characters with m-1 text characters overlapping in each partition, here P refers to the number of processors in the topology, m and n being the lengths of text and pattern string respectively [12] .The number of sub texts obtained after partitioning the text string using the above formula equals the number of processors allotted in the architecture, i.e., *i=P,* thereby representing the static allocation of the processors. The complete idea behind the working of this procedure can be well understood by the algorithm given below.

i. *Parallel kumar viswandha Boyer Moore Algorithm*

Begin

Step 1: Input on the user interface text file of size n, pattern file of size m and number of processors (P) available.

Step 2: Undergo text file division into ' *i* ' number of subtexts, each i contains (n/P)+m-1 text characters using m-1 overlapping text characters. The divided sub text files are stored in a directory.

Step 3: Broadcast these sub text files to each processor in the topology.

Step 4: Each Processor searches the pattern string in the given Sub text file using the Boyer Moore Algorithm and sends back the result.

Step 5: *Boyer Moore Algorithm*

Begin

Step 5.1: A window of size pattern slides over the text Scanning m elements of text string with the pattern string of length m from right to left.

Step 5.2: On a mismatch use the longest shift distance of the bad character heuristic and Good suffix heuristic. Window shifts are carried till n-m+1th position is attained on the text string.

Step 5.2.1: The bad Character heuristic states that the mismatching text character termed as bad character of the corresponding pattern character is searched for the rightmost occurrence in the left portion of the pattern window, if found the bad character is aligned with it. If occurs nowhere in the pattern then m characters of the text can be skipped.

Step 5.2.2: According to the good suffix heuristic, the suffix appending the bad character is searched in the left portion of the pattern and thus aligned if found else skip m characters of the text string.

Step 5.3: On a successful match of all the pattern characters with the text characters in the window, locate the pattern string and continue matching for the next occurrence skipping m characters of the text.

Step 5.4: Repeat steps 5.1 to 5.3 till n-m+1 position of the text string.

End

Step 6: Each processor stores the sub results and sends back to the main program to sum up the obtained results.

End.

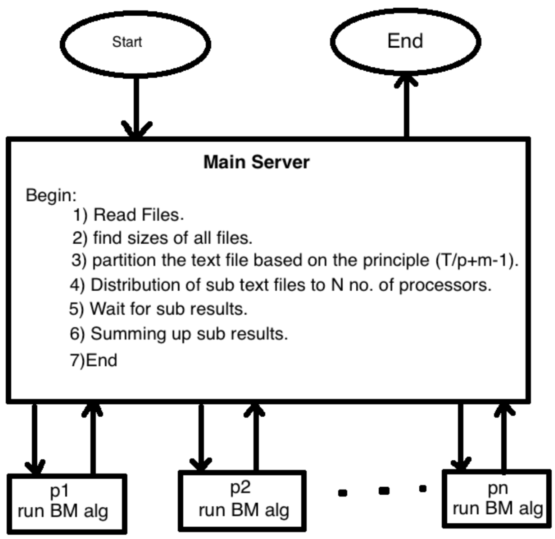


Figure 2 : Overlapped Partition Algorithm on Distributed Network

VI. Result Analysis and Discussions

We have considering three files for the implementation discussed in the previous chapter such as f_1 of size 1 Mb, f_2 of size 2 Mb, and f_3 of size 3 Mb from TREC- 05psn datasets and TREC-09ps micro biology datasets. The pattern files are p_1, p_2, p_3 with respect to those three files [2, 10, 12]. Here bytes mean number of characters. Time is measured in milli seconds $p_{i,j,}$ represents pattern i in file j.

Example : $p_{1,1}$ gives pattern 1 in file 1 (f_1),
$p_{1,2}$ gives pattern 1 in file 2 (f_2).

File 1 The pattern files that are searched in the text file f_1 are $p_{1,1}$ of size 3 bytes, $p_{2,1}$ of size 10 bytes, and $p_{3,1}$ of size 15 bytes has to be found using KV-Boyer moore Exact string matching algorithlm and as well as KMP Algorithms.

File 2 The pattern files that are searched in the text file f_2 are $p_{1,2}$ of size 8 bytes, $p_{2,2}$ of size 4 bytes, and $p_{3,2}$ of size 20 bytes has to be found usingKV- Boyer moore Exact string matching algorithm and as well as KMP Algorithms.

File 3 The pattern files that are searched in the text file f_3 are $p_{1,3}$ of size 3 bytes, $p_{2,3}$ of size 7 bytes, and $p_{3,3}$ of size 19 bytes has to be found using KV-Boyer moore Exact string matching algorithm. The test is conducted for three text files against three patterns of different sizes for Both the Boyer Moore and KMP and The results are shown in tables. The results of KMP algorithm are beyond the scope of this paper.

Results of KV-BM string Matching Algorithms are basically taken from output file and from instant graphs. The program was designed and implemented such that, it generates the instant graph (Bar chart) based on the No. of processors which are represented on X-axis and time on Y-axis in milliseconds along with no. of occurrences of pattern against each processors shown in the figures 3, 4, and 5. The Bar chart Graph uses the multi-colors to separate the each processors from the other, on the top of the bar No. of occurrences are mentioned with numeric number in braces. The program gives the output results in the form of text file along with the instant graphs. The output results text file gives the test parameters like start time ,end time and elapse time , along with the time taken for reading the text file and broad costing timings of sub text files . It also gives other kinds of output parameters called as position of the pattern occurrences and size. The figure.7 in tables we shown only the elapse time and average time of the processors involved in milliseconds, along with the no. of times the pattern is occurred . Actual test is conducted separately for single processor, two processors, three processors and four processors. Every time, while the test is conducted the program gives elapse time for each processor separately. Therefore the average time is calculated from output result based on the maximum time taken by the individual processor among the processors involved for the particular test. The table shows that for each pattern, as the No. of processors increases the time reduces and accuracy Increases. The graph's shows that the search time taken by single processor is more when compared with multiple processors . It is also observed that as the pattern size increases the search time decreases further. For bigger pattern sizes string matching is more easier for Boyer moore algorithm because of less number of mismatches.

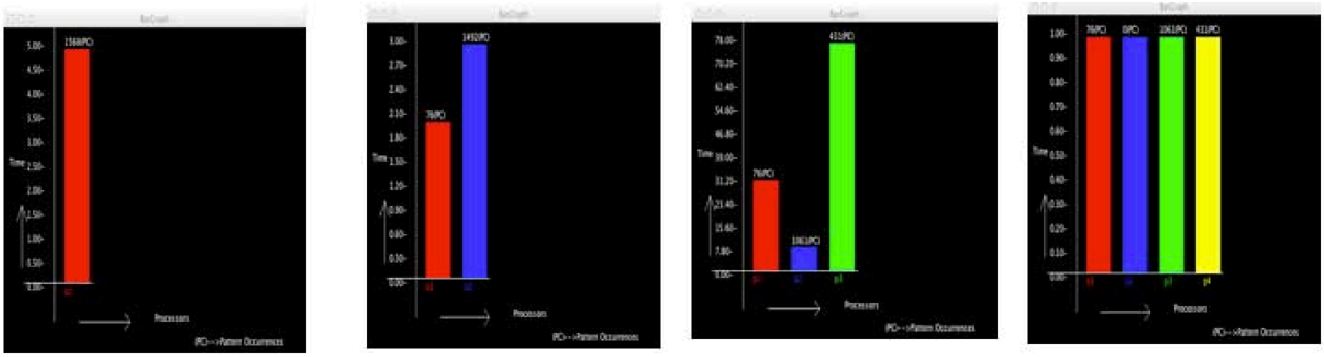


Figure.(3) :Instant graph for Pattern.1(gov) on (a) Single processor ,(b) Two Processors(c) Three processors (d) four processors

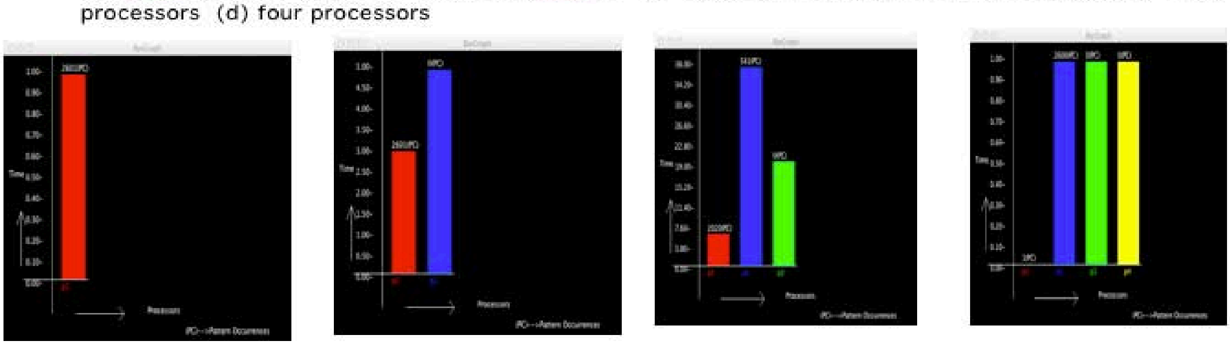


Figure.(4) :Instant graph for Pattern.2(graylabs) on (a) Single processor ,(b) Two Processors(c) Three processors (d) four processors

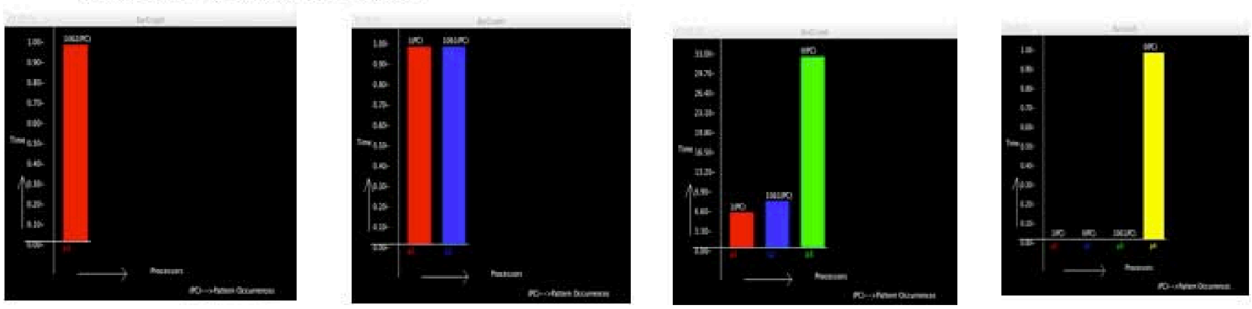


Figure.(5) :Instant graph for Pattern.3 (sis_gov_org)on (a) Single processor ,(b) Two Processors(c) Three processors (d) four processor

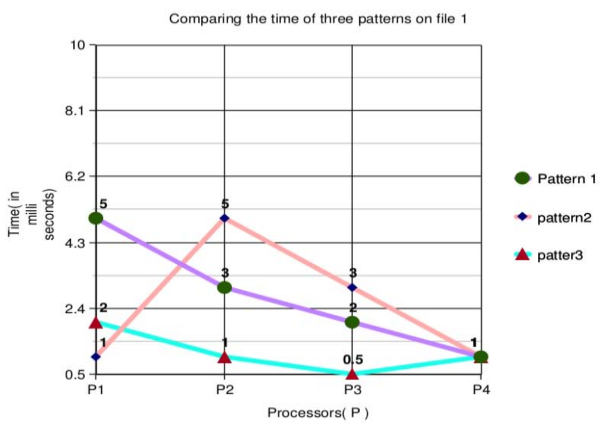
Table1: BM-SM Shows the variation of time among the processors for File 1

S.No	Pattern with size	Single processor		Two processors			Three Processors				Four Processors					No.of times pattern occurred
		Elapse Time of P1	Average time	Elapse Time of P1	Elapse Time of P2	Average time	Elapse Time of P1	Elapse Time of P2	Elapse Time of P3	Average time	Elapse Time of P1	Elapse Time of p2	Elapse Time of P3	Elapse Time of P4	Average time	
1	P1-(3bytes)	5	5	2.1	3	3	2	2	1	2	1	1	1	1	1	1568
2	P2-(7bytes)	10	10	3	5	5	2	3	2	3	1	1	1	1	1	2601
3	P3-(10bytes)	1	1	1	1	1	0.5	0.5	1	1	0	0	0	1	1	1026

Figure.(6) :Results are tabulated for elapse time along with number of occurrences

Figure 6 : KV-BM algorithms results are tabulated for four processor against three patrern files

Figure 7 : KV-BM algorithms results on line graph for comparison of three pattern files



This graph is constructed online by feeding the results from the above table. It is evident that the pattern 1 is of size 3 bytes and text file of size 1MB takes the 4.8 ms time to search the pattern but as the No. of processors increases it reduces to 0.5ms. In case of pattern 2 the size is 7bytes and it is also behaves similar to pattern 1 in case of more No. of processors but, for pattern 3 of size 10 bytes search time reduces drastically as the pattern size increases and as well as No. of processor increases .Hence our experimental results give excellent out puts and we also conducted more experiments but , results are not presented due space problem Theoretically discussed.

VII. Conclusion

In this paper we have compared string-matching on single processor with multi-processors in parallel environment on hypercube network. The total time taken by search pattern is going to reduces as the No. of processors increases in network. This application developed for text documents of size only MB. It may extend to any size i.e GB to TB also and any other format likes image and video files etc. There is lot of scope to develop new trends in this area by evolving modern methods and models for increasing search speed and accuracy. In near future we also produce new results by conducting more no. of experiments using the similar setups.

References Références Referencias

1. Roi Blanco, B.Barla cambazoglu "8th LSDS-IR'10 – ACMSIGIR Form, Vol 44 No. 2 Dec-2010.
2. S. Viswanadha Raju, K.S.M.V. kumar, "Implementation of String matching on Multiprocessors using divide and Conquer Technique" in 2011 3rd international Conference on Machine Learning and Computing (ICMLC) WWW.Elsevier.com, Dec 2011.
3. D. E. Knuth, J. Morris, and V. Pratt, "Fast Patern Matching in Strings," SIAM J. of Comput., Vol. 6, pp. 323-350, 1977.
4. http://www.worldwidewebsize.com
5. www.lsdsir.org-page-id=21
6. R.S. Boyer and J.S. Moore. A fast String Searching Algorithm Communications of the ACM, 20(10):762–772, 1977.
7. Awsan Abdulrahman Hasan and NurainiAbdul Rashid "Hash-Boyer Moore-Harspool string Matching Algorithm for Intrusion Detection Systems" INCNCS-2012, IPCSIT vol. 35 (2012), Singpore.
8. V. Aho and M. J. Corasick. Efficient String Matching: An Aid to Bibliographic Search. Communication of the ACM, 18(6): 333–340, 1975.
9. M Allen, B. Wilkinson, "Parallel Programming: Techniques and Applications using Networked Workstations and Parallel Computers", Prentice Hall, 1999.
10. S. Viswanadha Raju and A. Vinaya Babu, 2006, "Optimal Parallel Algorithm for String Matching on Mesh Network Structure", International Journal Applied Mathematical Sciences, 3 No.2, 167-175.
11. Snort. www.snort.org.
12. S. Viswanadha Raju, S.R. Mantena, A. Vinayababu and GVS Raju, 2006, "Efficient Parallel String Matching Using Partition Method", Proc PDCAT-2006, IEEE Computer Society, 281-284.
13. Herbert Scheldt's (Osborne) Java 2-Complete Reference, 5th edition-2008.
14. RMI:http://java.sun.com/products/jdk/rmi/, http://www.ece.vill.edu/~khenry/rmiapp/
15. Bi Kun, Gu Nai-jie, Tu Kun, Liu Xiao-Hu and Liu Gang "A Practical Distributed String matching Algorithm Architecture and Implementation WASET vol.19, pp.156-162, oct. 2005.
16. Zvi Galil, "A Constant-Time Optimal Parallel String-Matching Algorithm," Journal of the ACM, Vol. 42, pp. 908-918, July 1995.
17. Hiroki Arimura, Atsushi waraki Ryoichi Fujino and Stno Arikawa "A Fast Algorithm for Discovering optimal String Parrens in Large Text Databases".
18. Jin Hwan Park and K.M. George, "Parallel String Matching Algorithms Basedon Dataflow", Computer Science Department, Oklahoma State University, Stillwater, USA.
19. Cooks and Rivest "Two-way pushdown automata for string matching" journal of IEEE.1977.
20. Y. Mishina and K. Kojima string-matching algorithms for vector processing and its implementation in proceedings of 1993 IEEE international conference on computer design (ICCD'93) 1993.
21. R. Sidhu's V.K Prasarna "Fast regular Expression Matching using FPGA's" In IEEE symposium on FPCCM; Rohnert park, CA USA, April 2001.
22. Edward Frenandez, W Najjar and S Lonardi "String-matching in Hardware using the FM-Index". In IEEE 1998.

Global Journal of Computer Science and Technology
Network, Web & Security
Volume 13 Issue 4 Version 1.0 Year 2013
Type: Double Blind Peer Reviewed International Research Journal
Publisher: Global Journals Inc. (USA)
Online ISSN: 0975-4172 & Print ISSN: 0975-4350

Enhancing Network Lifetime in Wireless Sensor Networks Adopting Elephant Swarm Optimization

By Chandramouli.H, Dr. Somashekhar C Desai, K S Jagadeesh & Kashyap D Dhruve
JJT University, Jhunjhunu

Abstract - Enhancing the lifetime of wireless sensor networks had baffled researchers for quite some time now. The authors of this research manuscript draw inspiration from the behavior of large elephant swarms and incorporate their behavior into wireless sensor networks. The complex elephant swarm behavior is incorporated using a cross layer approach. The elephant optimization discussed in this paper enables optimized routing techniques, adaptive radio link optimization and balanced $TDMA\ MAC$ scheduling to achieve a cumulative enhanced network performance. The proposed elephant swarm optimization is compared with the popular $LEACH$ protocol. The experimental study presented proves that the Elephant Swarm Optimization technique enhances the network life time by about 73%.

Keywords : elephant swarm, optimization, network lifetime, cross-layer design, energy efficiency, resource allocation, sensor networks.

GJCST-E Classification : C.2.1

ENHANCING NETWORK LIFETIME IN WIRELESS SENSOR NETWORKS ADOPTING ELEPHANT SWARM OPTIMIZATION

Strictly as per the compliance and regulations of:

Enhancing Network Lifetime in Wireless Sensor Networks Adopting Elephant Swarm Optimization

Chandramouli.H [α], Dr. Somashekhar C Desai [σ], K S Jagadeesh [ρ] & Kashyap D Dhruve [ω]

Abstract - Enhancing the lifetime of wireless sensor networks had baffled researchers for quite some time now. The authors of this research manuscript draw inspiration from the behavior of large elephant swarms and incorporate their behavior into wireless sensor networks. The complex elephant swarm behavior is incorporated using a cross layer approach. The elephant optimization discussed in this paper enables optimized routing techniques, adaptive radio link optimization and balanced $TDMA\ MAC$ scheduling to achieve a cumulative enhanced network performance. The proposed elephant swarm optimization is compared with the popular $LEACH$ protocol. The experimental study presented proves that the Elephant Swarm Optimization technique enhances the network life time by about 73%.

Keywords : elephant swarm, optimization, network lifetime, cross-layer design, energy efficiency, resource allocation, sensor networks.

I. Introduction

Let us consider a topology of wireless sensor networks deployed over a specified geographical region. The sensor nodes are assumed to have homogenous energy properties and are battery operated which is the case most often than not. The sensor distribution over the geographical region is considered to be dense to achieve higher transmission data rates. Owing to dense deployments numerous links are established induce interference amongst the sensor nodes which needs to be minimized to achieve better network performance in terms of throughput. This paper introduces an Elephant Based Swarm Optimization model to enhance network life time. A cross layer approach is adopted to incorporate the elephant swarm optimization features.

Elephants are social animals [1] and exhibit advanced intelligence [2]. Elephants are often found to exist in a "fluid fission-fusion" social environment [3]. Elephants characterized by their good memory, their nature to coexist and survive within a "clan" [4] (a large swarm of more than 1000 elephants) socially formulated during testing times like migration and when the resources are scare. Elephants exhibit an unselfish behavior which enable them to grow and is the secret of their longevity. Keeping progress and survivability in mind the older elephants disassociate from the "clan". Elephants by nature are protective of their younger generation. Elephants communicate using varied advanced techniques which include acoustic communication, chemical communication, visual communication and tactile communication [5] [6]. Their memory empowers them with recognition, identification and problem solving scenarios [4]. All these features exhibited have influenced the authors to incorporate such behavior in wireless sensor networks to improve network performance.

The elephant swarm model is complex and to realize such behaviors in wireless sensor networks the authors have proposed to adopt a cross layer approach to incorporate the elephant swarm model. Optimizations need to be adopted at the Routing Layer, MAC Layer and the Radio Layer of the wireless sensor node. This paper introduces a cross layer approach to incorporate the elephant swarm optimization technique which is compared with the popular $LEACH$ protocol and its efficiency is proved in the latter section of this paper.

The remaining manuscript is organized as follows. Section two discusses a brief literature study conducted during the course of the research work presented here. The system modelling and the elephant swarm optimization technique using a cross layer approach is discussed in the third section of this paper. The experimental study conducted is described in the penultimate section of this paper. The conclusions drawn and the future work is presented in the last section of this paper.

II. Literature Review

The literature review discussed in this paper emphasizes the cross layer architectures proposed by researchers to overcome the drawbacks that exist in wireless sensor networks.

A research work [7] describes the fundamental concept of sensor networks which has been made viable by the convergence of micro electro-mechanical

Author α : Research Scholar, JJT University, Jhunjhunu, Rajasthan, India. E-mail : hcm123cool@rediffmail.com
Author σ : Professor, BLDEA College of Engineering, Bijapur, India. E-mail : desaisc07@gmail.com
Author ρ : Research Scholar, JJT University, Jhunjhunu, Rajasthan, India. E-mail : Ksj_20012002@yahoo.co.in
Author ω : Technical Director, Planet-I Technologies, Bangalore, India. E-mail : kashyapdhruve@hotmail.com

Global Journal of Computer Science and Technology (E) Volume XIII Issue IV Version I Year 2013

systems technology, wireless communications and digital electronics. In their work initially the potential sensor networks are explored and then the dominant factors influencing the system architecture of network is obtained and in the later stage the communication architecture was outlined and the algorithms were developed for different layers of the network for system optimization. As this proposal brought certain positive results but was lacking the optimized output and having a lot of vacuum for further development.

The researcher in [8] developed a recommender system, employing a particle swarm optimization (PSO) algorithm for learning the personal preferences of users and facilitates the tailored solutions. The system being used in this research was based on collaborative filtering approach, building up profiles of users and then using an algorithm to find profiles similar to the current user. To overcome the problem of sparse or implicated data they utilized stochastic and heuristic-based based models to speed up and improve the quality of profile matching and finally the PSO was used to optimize the results. That system was found to be outperforming Genetic Algorithm concept but the system could not play a vital role in higher data rate with cross layer architecture and especially for heterogeneous type of network.

In literature [9] a number of fundamental cross layered resource allocation techniques at MAC layer were considered for fading channel. This research work emphasizes on characterization of fundamental performance limits while considering the network layer, MAC layer quality and physical layer as performance.

Considering the dominant network parameters like deploy, energy consumption, expansibility, flexibility and error tolerance Jin, Lizhong et al [10] presented a research work that employs a cross layer MAC protocol for wireless network. This work employs the splitting of MAC layer and of course it performed well, but considering the higher data rate transmission this system was found to be ineffective even having more error prone.

In [11] investigated the cross layer survivable link mapping when the traffic layers are unambiguously desired and survivability is must. In this work a forbidden link matrix is identified the masking region of the network for implementing in such conditions where some physical links are reserved exclusively for a designated service, mainly for the context of providing multiple levels of differentiation on the network use. The masking upshot is then estimated on two metrics using two sensible approaches in a real-world network, depicting that both effectiveness and expediency can be obtained.

The literature [12] the researcher proposed a route discovery and congestion handling mechanism that employs a cross layer model including a potential role in congestion detection and its regularization. The limitation of the proposed technique was its confined data rate.

Hang Su [13] proposes the cross layer architecture based an opportunistic MAC protocol that integrates the spectrum sensing at PHY layer and packet scheduling at the MAC layer. In their proposal the secondary user is equipped with two transceivers where one is tuned for dedicated control channel while another one is designed particularly for cognitive radio that can effectively use the idle radio. They propose two shared channel spectrum-sensing approach, named as the random sensing policy and the negotiation-based sensing policy so as to assist the MAC protocols detect the availability of leftover channels. This technique has a great potential but the emphasis has been made on the efficient use of leftover frequency and thus the other QoS parameters are not being considered.

In literature [14] proposed a new cross layer-based MAC protocol stated as $CLMAC$. In this proposed cross layered MAC technique, the communications among MAC, Routing and Physical layers are fully exploited so as to minimize the energy consumption and multi-hop delay of the data delivery for wireless sensor networks. In precise, in that approach the carrier-sensing technology is applied at the layer so as to sense the traffic load and necessarily initiates the neighbor nodes in multi hops so that the data transmission can be realized over multi hop. Similarly, by implementing the routing layer information, the developed cross layered facilitates the receiver of the ascending hop on the path of routing that has to be effectively waken up and ultimately it results into the potential reduction in energy consumption.

In reference [15] the $LEACH$ (Low Energy Adaptive Clustering Hierarchy) routing protocol which is a conventional clustering communication protocol has been implemented. The proposed protocol is dominantly used in WSN. Then while there are certain limitations in LEACH, in as the nodes consume a lot of energy and the efficiency of nodes ultimately decreases because the nodes which are having low energy and are at remote from Base Station become the cluster head nodes. This work analyzes the energy model and considers three important factors: The energy for individual nodes, the number of times that the node is chosen as cluster heads and the distances between nodes and BS. In this research work the author changes the threshold function of the node so as to extend the lifetime of the network and to achieve the goal of balancing the energy of the network. This work has indicated that the implemented system can of course prolong the life span of the network, but the drawback of this work is that it does not consider the other network optimization problems like, throughput, delay, overheads etc.

The techniques incorporated by researchers to enhance the network lifetime of wireless sensor networks is also considered during the course of the research presented here [16] [17] [22].

III. Elephant Swarm Optimization in Wireless Sensor Networks

a) System Modeling of Sensor Networks

In this section of the paper the system modelling adopted to realize the elephant swarm optimization for wireless sensor networks is discussed.

Let us consider a w wireless sensor nodes represented by a set W which constitute a static network defined as

$$W = \{w_1, w_2, w_3, \ldots. w_w\}$$

In the considered network W, the wireless communication links that exist between two nodes $w_1 \in W$ and $w_2 \in W$, a relatively high transmission power allocation scheme is considered . The high power allocation scheme causes the higher power consumption that ultimately results into numerous interferences situation between other nodes as well as degraded network life time and hence poor efficiency. The communication channel being considered over the links is nothing but Additive White Gaussian Noise ($AWGN$) channel having confined noise power level. Here, one more factor called deterministic path loss model has been assumed. If the signal to noise ratio of a communication link is represented by γ then the maximum data rate supported (m_r) per unit bandwidth is defined as

$$m_r = log\big(1 + (B \times \gamma)\big)$$

Where

$$B = \frac{-1 \cdot 5}{log(5BER)}$$

This considered model can be realized using modulation schemes like $MQAM$. The constellation size for the $MQAM$ is ≥ 4 and varies with time over a considered link [23]. The model assumes a $TDMA$ scheduling system of communication between the nodes. The model considered assumes that there exists N_t time slots for the medium access control layer (MAC) and a unique transmission mode is applicable per slot.

Let us consider that a particular node $w_w \in W$ transmits at a power level P_t then the power consumption of the amplifier is defined as

$$(1 + \alpha)P_t$$

Where α is the efficiency of power amplifier and $\alpha > 0$ to achieve the desired signal amplification.

A homogenous sensor network model is considered $i.e. \forall\, w_w \in W : \alpha_1 = \alpha_2 = \cdots = \alpha_w$.

The directed graph that represents the network W under consideration, is defined as

$$D_g = (W\ L)$$

Where indicates set of directed links.

Let $\mathcal{A} \in \mathcal{R}^{|W| \times |L|}$ indicates the incidence matrix of the graph D_g then we can state that

$$\mathcal{A}(w_w, \ell) = \begin{Bmatrix} -1 & If\ w_w \text{ is the receiver of link } \ell \\ 0 & in\ other\ cases \\ +1 & If\ w_w \text{ is the transmitter of link } \ell \end{Bmatrix}$$

We present an expression

$$\mathcal{A} = \mathcal{A}^+ - \mathcal{A}^-$$

Such that $\mathcal{A}^+(v,\ell), \mathcal{A}^-(v,\ell) = 0$, $\mathcal{A}^+$, $\mathcal{A}^-$ and have the entries of 0 and 1.

As discussed N_t is the number of time slots in individual frame of the periodic schedule. L^{n_t} represents the set of link scheduled. These are allowed to transmit during time slot defined as

$$n_t \in \{1, \cdots\cdots\cdots, N_t\}$$

$P_l^{n_t}$ and ${m_r}_l^{n_t}$ represents the power of transmission and per unit bandwidth rate respectively over link l and n_t slots. The vectors of the time slot n_t are ${m_r}^{n_t}$ and $P^{n_t} \in \mathcal{R}^{|L|}$. P_ℓ^{max} is the maximum limit of allowable transmission power for the node which belongs to link. The analogous vector is $P^{max} \in \mathcal{R}^{|L|}$. The vectors $1_t(P^{n_t})$ id defined as

$$\big(1_t(P^{n_t})\big)_{w_w} = \begin{cases} 1 & if\ ((e_v^+)^T \times P^{n_t}) > 0 \\ 0 & In\ other\ cases \end{cases}$$

Where $(e^+)^T$ is the v^{th} row of the matrices $\mathcal{A}^+$. Also $\big(1_t(P^{n_t})\big)_{w_w} \in \mathcal{R}^{|W|}$

The vector $1_{m_r}(P^{n_t})$ is defined as

$$\big(1_{m_r}(P^{n_t})\big)_{w_w} = \begin{cases} 1 & if\ ((e_v^-)^T \times P^{n_t}) > 0 \\ 0 & In\ other\ cases \end{cases}$$

where $(e_v^-)^T$ is the v^{th} row of the matrices $\mathcal{A}^-$. Also $\big(1_{m_r}(P^{n_t})\big)_{w_w} \in \mathcal{R}^{|W|}$.

The initial homogenous energy of all the nodes $w_w \in W$ defined as $\mathcal{E}_{w_w}$ and the energy $\mathcal{E} \in \mathcal{R}^{|W|}$.

Let P_{tcon} represents power consumption of transmitter and P_{rcon} represents the power consumption of the receiver and is assumed to be homogenous for all the nodes. The consumed by each node $w_w \in W$ is $\leq \mathcal{E}_{w_w}$.

Let the sensing events that are induced in the network induce an information generation rate represented as $\mathcal{S}_{w_w}$. It can be stated that $\mathcal{S} \in \mathcal{R}^{|W|}$ represents a vector which constitute of $\mathcal{S}_{w_w}$.

The data aggregated at the sink is defined as

$$\mathcal{S}_{Sink} = -\sum_{w_w \in W, w_w \neq Sink} \mathcal{S}_{w_w}$$

The link gain matrix of the wireless sensor network considered is defined as

$$D_g = \mathcal{R}^{|L| \times |L|}$$

The power from the transmitter of the $\mathcal{K}^{th}$ link to the receiving node on link ℓ is represented as $D_{g_{l\mathcal{K}}}$ and $\mathcal{N}_0$ represents the total noise power over the operational bandwidth.

The T_{w_w} represent the network lifetime when a percentage of nodes $w\%$ runs out of energy. This is a common criterion considered by researchers to evaluate their proposed algorithms [16] [17].

The maximum data rate supported for transmission over a particular Link $l \in L$ is defined as

$$(1 + (\mathcal{K} \times log(SINR)))$$

b) *Problem Formulation*

A cross layer approach is adopted to enhance the network lifetime of the wireless sensor network. Elephants are social animals and are said to possess strong memory of the events that occur.

The problem of optimizing or maximizing the life span of the network can be presented as a function defined as follows

$$max.(\mathcal{T}_{net})$$

$$i.e. \ \frac{1}{N_t}\mathcal{A}(m_r{}^1 + \cdots\cdots + m_r{}^{N_t}) = \mathcal{S}$$

$$log\left(1 + \mathcal{K}\frac{D_{g_{ll}}\mathcal{P}_\ell^n}{\sum_{\mathcal{K}\neq\ell} D_{g_{lk}}\mathcal{P}_k^n + \mathcal{N}_0}\right) \geq m_{r_l}{}^{n_t}$$

The maximization function $max.(\mathcal{T}_{net})$ can be defined as

$$\frac{\mathcal{T}_{net}}{N_t}\sum_{n_t=1}^{N_t}\left((1 + \alpha)\mathcal{A}^+\mathcal{P}^{n_t} + P_{tcon}1_t(\mathcal{P}^{n_t}) + P_{rcon}1_{m_r}(\mathcal{P}^{n_t})\right) \preccurlyeq \mathcal{E}\, m_r{}^{n_t} \succcurlyeq 0,0 \preccurlyeq \mathcal{P}^{n_t} \preccurlyeq \mathcal{P}^{max}$$

For all time slots $n_t = 1,\cdots\cdots,N_t$ and $l \in L$, the constituting variables are $\mathcal{T}_{net}, m_{r_l}{}^{n_t}, \mathcal{P}_\ell^{n_t}$, for a set $n_t \in \{1,\cdots\cdots,N_t\}, l \in L$.
Let us define a variable O such that

$$O = (\mathcal{T}_{net})^{-1}$$

The elephant swarm optimization is applied to attain minimized function defined as

$$min.(O)$$

$$i.e. \ \mathcal{A}(m_r{}^1 + \cdots\cdots + m_r{}^{N_t}) = (\mathcal{S} \times N_t)$$

$$log\left(1 + \frac{D_{g_{ll}}\mathcal{P}_\ell^{n_t}}{\sum_{\mathcal{K}\neq\ell} D_{g_{lk}}\mathcal{P}_k^{n_t} + \mathcal{N}_0}\right) \geq m_{r_l}{}^{n_t}$$

The minimization function or the elephant swarm optimization objective $min.(O)$ can be defined as

$$\sum_{n^t=1}^{N_t}\left((1 + \alpha)\mathcal{A}^+\mathcal{P}^{n_t} + P_{tcon}1_t(\mathcal{P}^{n_t}) + P_{rcon}1_{m_r}(\mathcal{P}^{n_t})\right) \preccurlyeq O\, \mathcal{E}\, N_t$$

The model presented here considers $TDMA$ based MAC systems the minimization function can be defined as

$$min.(O)$$

$$i.e. \quad \sum_{l \in Tx(w_w)}(a_l) - \sum_{l \in Rx(w_w)}^{O}(a_l) = N_t\,\mathcal{S}_{w_w}$$

$$a_l - n_{t_l}\, log\left(1 - \frac{D_{g_{ll}}\mathcal{P}_l^{max}}{N_0}\right) \leq 0$$

$$\sum_{l \in Tx(w_w)} \zeta n_{t_l}\left(e^{\frac{a_\ell}{n_{tl}}} - 1 + \frac{P_{tcon}}{\zeta}\right) + \sum_{l \in Rx(w_w)} P_{rcon}\, n_{t_l} \leq O N_t \mathcal{E}_{w_w}$$

$$\sum_{l \in L} n_{t_l} \leq N_t\,,\ a_l\,, n_{t_l} \geq 0, n_{t_l} \in \{0,\cdots\cdots,N_t\}$$

Where l represents the link, the number of slots assigned on l is n_{t_l}. $Tx(w_w)$ is the set of transmitting links and $Rx(w_w)$ is the receiving links of the sensor node $w_w \in W$.The variable is ζ defined as follows

$$\zeta = \frac{N_0 (1+\alpha)}{D_{g_{ll}}}$$

And a_l is defined as

$$a_l = m_{r_l} \times n_{t_l}$$

The transmission power the l^{th} link represented as $\mathcal{P}_l$ is defined as

$$\mathcal{P}_l = \frac{N_0}{D_{g_{ll}}}(e^{m_r \ell} - 1).$$

It must be noticed that the power of transmission over a network link l is presented as

$$\mathcal{P}_l = \frac{N_0}{D_{g_{ll}}}(e^{m_r l} - 1)$$

c) Cross Layer Optimization to Realize Elephant Swarm Behavior

The presented section of this paper elaborates the elephant swarm optimization algorithm for routing, $TDMA\ MAC$ scheduling and advanced radio layer control techniques. The elephant swam optimization is applied taking into account unconstrained scheduling on the network links. The elephant swarm optimization enables simultaneous $TDMA$ scheduling of the sensing data on the interfering wireless communication links in the current considered scheduling time slot. The elephant swarm optimization iterates to obtain an optimal routing, power consumption and $TDMA\ MAC$ schedule to enhance the considered network lifetime. The elephant model is adopted to solve optimization objective $min.(O)$ defined in the former section of this paper.

Let us consider a $TDMA$ link schedule of data defined as L^{n_t} where $n_t \in \{1, \cdots\cdots\cdots, N_t\}$. The rate of transmission that can be supported over a link $l \in L$ can be expresses as based on approximations is defined as

$$m_{r_l}^{n_t} \leq \log\left(\frac{D_{g_{ll}}\mathcal{P}_l^{n_t}}{\sum_{k \neq \ell, k \in L^{n_t}} D_{g_{lk}}\mathcal{P}_k^{n_t} + \mathcal{N}_0}\right)$$

If the $SINR$ of a link $l \in L$ is γ then the minimum transmission rate is defined as follows

$$log(\gamma)$$

The elephant swarm optimization results arising based on the above approximations for $m_{r_l}^{n_t}$ are said to be a part of the $min.(O)$ function optimization set.

Let us define a variable

$$\mathcal{J}_l^{n_t} = \log(\mathcal{P}_l^{n_t})$$

Then the above equation for the maximum transmission rate optimization $m_{r_l}^{n_t}$ can be defined as can be

$$log\left(\frac{N_0}{D_{g_{ll}}} e^{m_{r_l}^{n_t}} - \mathcal{J}_l^n + \sum_{\mathcal{K} \in L^n, \mathcal{K} \neq L} \frac{D_{g_{l\mathcal{k}}}}{D_{g_{ll}}} e^{m_{r_\ell}^{n_t}} + \mathcal{J}_{\mathcal{k}}^{n_t} - \mathcal{J}_\ell^{n_t}\right) \leq 0$$

Based on the above arguments the elephant swarm optimization objective $min.(O)$ can be expressed as

$$\mathcal{A}(m_r^{1} + \cdots\cdots\cdots + m_r^{N_t}) = (\mathcal{S} \times N_t)$$

$$log\left(\frac{N_0}{D_{g_{ll}}} e^{m_{r_l}^{n_t}} - \mathcal{J}_l^n + \sum_{\mathcal{K} \in L^n, \mathcal{K} \neq L} \frac{D_{g_{l\mathcal{k}}}}{D_{g_{ll}}} e^{m_{r_\ell}^{n_t}} + \mathcal{J}_{\mathcal{k}}^{n_t} - \mathcal{J}_\ell^{n_t}\right) \leq 0\,, \ \forall\, l \in L$$

$$\sum_{n_t=1}^{N_t}\left(\sum_{l \in Tx(w_w) \cap L^{n_t}} \left((1+\alpha)e^{\mathcal{J}_l^{n_t}} + P_{tcon}\right) + \sum_{l \in Rx(w_w) \cap L^{n_t}} (P_{rcon})\right) \leq ON_t\mathcal{E}_{w_w}$$

The above defined elephant swarm optimization is applicable provided

$m_r^{n_t} \geq 0$

$\mathcal{J}_l^{n_t} \leq \log(\mathcal{P}_l^{max})$

$l \in L^{n_t}$ and

$n_t = \{1, \cdots\cdots\cdots, N_t\}$

In other terms the elephant swarm optimization is applicable if the links have a $SINR$ greater than unity.

The $TDMA\ MAC$ scheduling over all the links is not adopted as the power consumption would exponentially increase. The elephant swarm optimization is applied on all the $TDMA$ links scheduled L^{n_t}. The computational complexity of optimization under such circumstances can be defined as

$$C_{Complex} = 2^{(L \times N_t)}$$

From the above equation it is evident that the $TDMA\ MAC$ optimization is computationally heavy and increases exponentially as the links of the sensor nodes increase (i.e. for dense networks) and the $TDMA$ slot value increases. The computation complexity of the elephant swarm optimization can be reduced if the number of $TDMA\ MAC$ slots are doubled to $2N_t$. The two fold increase in the number of time slots enables achieving lower power consumption as the sensor nodes have numerous slot options and sleep induction is effective. Furthermore in the case of high sensing activity leading to greater data transmissions, the data to the sink is scheduled using multiple TDMA slots to enable energy conservation and accurate data aggregation.

The elephant swarm optimization model can be summarized in the form of the algorithm given below realized through multiple phases described below.

Phase A

Initialize the schedule L^{n_t} based on the data $\mathcal{S}_{w_w}$. The L^{n_t} is initialized such that link $l \in L^{n_t}\ \forall\ l \ \exists\ n_t \in N_t. i.e.$ the schedule is constructed in a manner such that all the links $l \in L^{n_t}$ are provided at least a slot in N_t.

Phase B

In this phase the following equation is solved

$$\sum_{n_t=1}^{N_t}\left(\sum_{l\,\in\,Tx(w_w)\cap L^{n_t}}\left((1+\alpha)e^{\mathcal{J}_l^{n_t}}+P_{tcon}\right)+\sum_{l\,\in\,Rx(w_w)\cap L^{n_t}}(P_{rcon})\right)$$

If the results obtained on solving are not suitable $.i.e. > ON_t\mathcal{E}_{w_w}$ then the optimization is not possible. If the solutions satisfies the condition $\leq ON_t\mathcal{E}_{w_w}$ then elephant swarm route optimization and radio layer optimizations are carried out to support the required transmission rate.

Phase C

Evaluate all the links $l \in L^{n_t}$ and retain the links if the following equation is satisfied.

$$\frac{D_{g\,ll}\mathcal{P}_l^{n_t}}{\sum_{k\neq\ell,k\in L^{n_t}} D_{g\,lk}\mathcal{P}_k^{n_t}+\mathcal{N}_0} > \gamma_o$$

This phase eliminates all the links whose $SINR$ is less than unity and retaining the links having an acceptable $SINR$.

Phase D

Compute $\ddot{l}$ using the following equation

$$\ddot{l} = l_{Max}^{Crnt}\left(\sum_{n_t=1}^{N_t}(\mathcal{P}_l^{n_t})\right)$$

Compute $\ddot{n}_t$ defined as

$$\ddot{n}_t = n_{t\,Min}^{\,Crnt}\left(\sum_{k\neq\ddot{l},k\in L^{n_t}} D_{g\,\ddot{l}k}\mathcal{P}_k^{n_t}+\mathcal{N}_0\right)$$

Using the above definitions we can obtain the new the $TDMA\ MAC$ layer schedule represented as $L^{\ddot{n}_t}$ and $\ddot{l} \in L^{\ddot{n}_t}$. If the optimized $TDMA\ MAC\ L^{\ddot{n}_t}$ schedule is equitant to the existing or previous schedule then no further optimization is possible. If the optimized $L^{\ddot{n}_t}$ is not similar to the current and previous MAC layer schedule the new schedule is adopted. $L^{\ddot{n}_t}$ enables to identify the maximum power utilization link l so we can schedule it the additional slots available thus aiding energy conservation.

Phase E

In the last phase of the elephant swarm optimization algorithm the optimal solution achieved using a cross layer approach is verified using the following definition

$$\left(\frac{D_{g\,ll}\mathcal{P}_l^{n_t}}{\sum_{k\neq\ell,k\in L^{n_t}} D_{g\,lk}\mathcal{P}_k^{n_t}+\mathcal{N}_0}\right) \geq 1.0\ \forall\ l \in L^{n_t}, n_t = \{1,\cdots\cdots\cdots,N_t\}$$

If the solution does not satisfy the above equation then no optimization is possible owing to current network dependent reasons. If optimal solution is obtained and incorporated network performance in terms of data aggregation, improved data rates and higher network lifetimes.

The elephant swarm optimization is realized using a cross layer design approach to enhance network lifetime. The efficiency and the performance measure of this optimization technique is discussed in the subsequent section of this paper.

IV. Experementail Study

In this section of the paper we shall discuss the experimental study conducted to compare the elephant swarm optimization algorithm introduced in this paper with the popular LEACH [15] protocol. The elephant swarm optimization model and the LEACH protocol was developed on the SENSORIA Wireless Sensor Network Simulator [18] [19] [20] [21]. The elephant swarm optimization algorithm was developed using the C# language on the Visual Studio 2010 platform. The simulations were executed on a $i7$ Quad Core CPU having 8GB of RAM to conduct the experimental study.

The wireless sensor network test bed was considered to be spread over a terrain measuring 25×25 meters. The wireless sensor nodes deployed over the terrain are varied from 450,500,550,600,650 and 700 nodes respectively. The test bed considered sensor nodes mounted with temperature sensors having a sensing range of 3m. The radio range considered is 5m. Sensing events are induced every 0.1 seconds. Inducing such high sensing activity and considering dense networks enables high traffic injection into the test bed. High traffic injection considered in the test beds results greater data transactions resulting in rapid energy depletion in the overall network. The simulation study was conducted to observe the network life time of the test bed. The threshold of the network lifetime analysis was set to 30% i.e. the simulation study was conducted until 30% of the network energy depletes.

To prove the efficiency of the elephant swarm optimization algorithm network test beds with varied nodes densities (i.e. 450,500,550,600,650 and 700) was simulated. The total network energy depletion was initiated by inducing sensing events. Similar network topology was considered to simulate the Elephant Swarm Optimization algorithm and the popular LEACH test bed. High traffic injection considered in the test beds results greater data transactions resulting in rapid energy depletion in the overall network. The simulation study was conducted to observe the network life time of the test bed. The threshold of the network lifetime analysis was set to 30% i.e. the simulation study was conducted until 30% of the network energy depletes.

To prove the efficiency of the elephant swarm optimization algorithm network test beds with varied nodes densities (i.e. 450,500,550,600,650 and 700) was simulated. The total network energy depletion was initiated by inducing sensing events. Similar network topology was considered to simulate the Elephant Swarm Optimization algorithm and the popular LEACH Algorithm. The simulation time was recorded when the total network energy depleted by 30%. The results obtained are shown in Figure 1 given below. The results obtain show that the cross layer optimization based on the elephant swarm model exhibits a 72.58% improvement in network lifetime when compared to the LEACH protocol.

The rate at which the sensor node energy decays with time is also observed ad the results obtained is shown in Figure 2. The Elephant Swarm optimization model proposed in this paper adopts a cross layer approach when compared to the LEACH protocol. The optimization technique proposed enables the balanced data scheduling on the links L that exist and hence reduces the energy decay rate of the sensors nodes by about 81.9%.

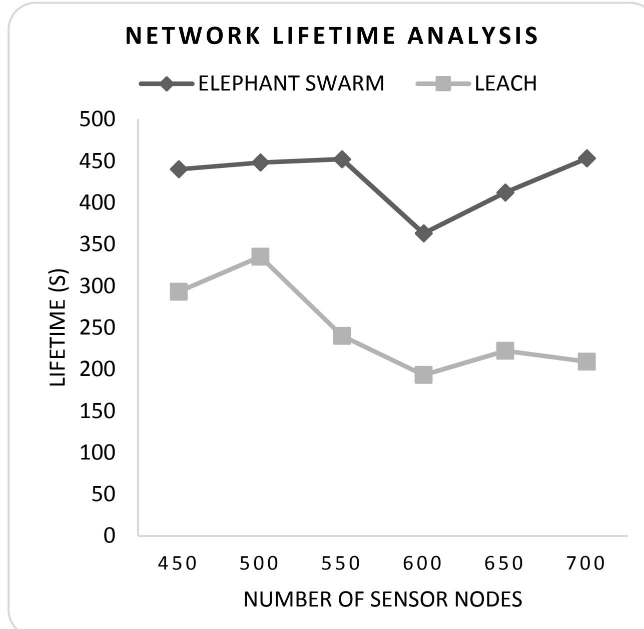


Figure 1 : Network Lifetime Analysis

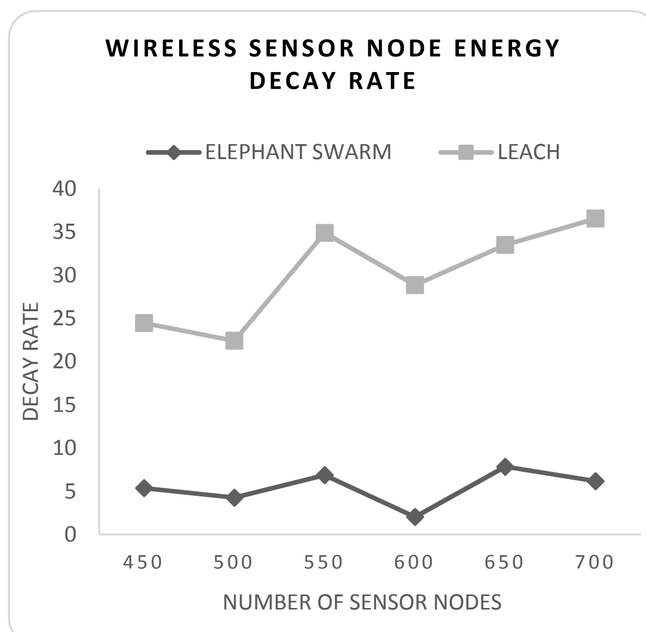


Figure 2 : Wireless Sensor Node Energy Decay Rate

The elephant swarm optimization proposed also enables communication overhead reduction even for dense wireless sensor networks. The communication overheads are reduced greatly by the reduction of the number of retransmissions of data packets and optimized routing incorporated in the elephant swarm model. The communication overhead of the LEACH protocol is about 36.6% greater than that of the proposed optimization model. The results obtained are as shown in Figure 3 of this paper.

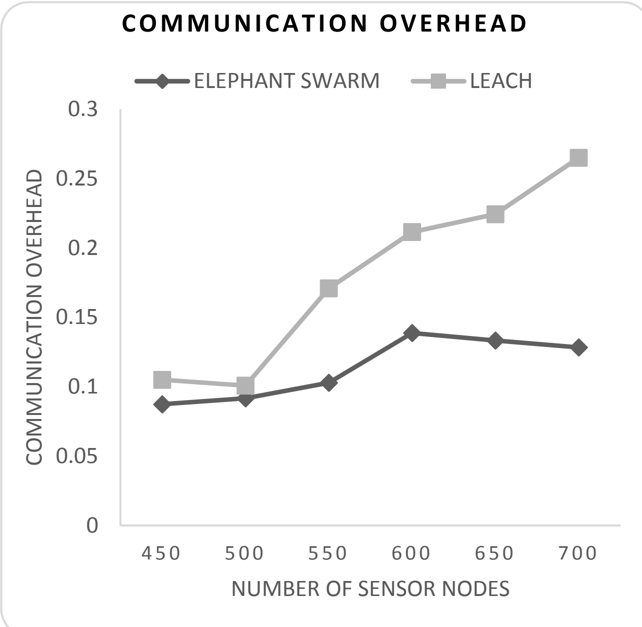


Figure 3 : Communication Overhead Analysis

To prove the increase in network lifetime the ratio of the sensor nodes active at regular time intervals is noted the results obtained are shown in Table 1. These results have been obtained for varying sensor node deployment densities. The graphical analysis is presented in Figure 4 of this paper given below. The results described in the table prove that the percentage of active nodes using the elephant swarm optimization is greater than the nodes alive while using the LEACH protocol.

Table 1 : Active Node Ratio with respect to the Simulation Instance and Network Topology Size

Number of Sensor Nodes	Sim Time (S)	Elephant Swarm Active Node Ratio	Leach Active Node Ratio
450	293	99.77777778	79.55555556
500	335	99.8	80.6
550	240	99.81818182	77.27272727
600	193	99.83333333	80.66666667
650	222	99.84615385	77.53846154
700	209	99.85714286	76.42857143

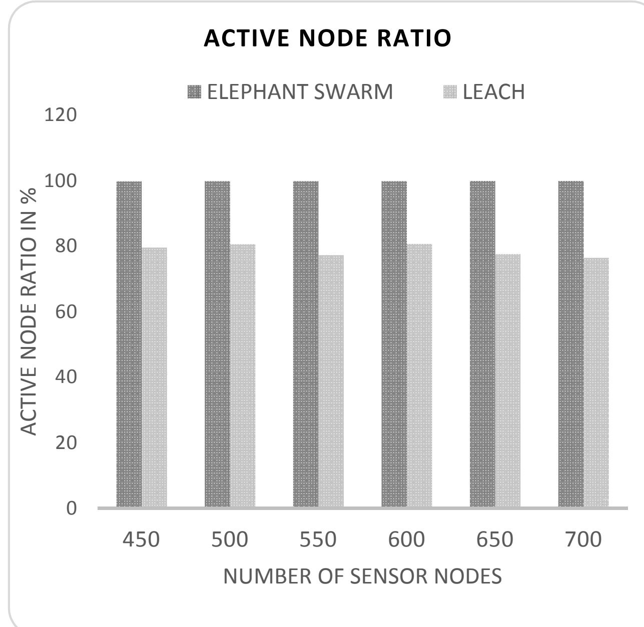


Figure 4 : Active Node Ratio in the Test Bed Observed at Constant Simulation Slots

The experimental study discussed in this section of this paper proves that the elephant swarm optimization technique proposed in this paper exhibits better network performance than the popular LEACH protocol commonly used. The enhanced networks performance is proved in terms of network lifetime, communication overhead reduction, reduced energy decay in the sensor nodes and enhanced active node ration in the network.

V. Conclusion and Future Work

In this manuscript the authors address the problem in enhancing the network lifetime of wireless sensor networks. The elephant swarm optimization technique is adopted to address the issue that exists. A cross layer approach is adopted to incorporate optimizations at the routing, radio and the MAC layers. A TDMA based MAC layer is considered and the MAC schedule is optimized in accordance to the routing and the radio link layer optimization. The system model considered is clearly discussed. The optimization function which needs to be solved using the elephant model is also discussed. The elephant swarm optimization is achieved using a phased approach discussed in this paper. The experimental evaluation conducted proves the efficiency of the proposed elephant swarm optimization technique over the popular LEACH protocol in terms of improved network lifetime, reduced sensor node energy decay rate, higher active node ratios and lower communication overheads. The overall network lifetime of the varied scenarios presented proves enhancement of about 73% thus justifying the robustness of the proposed elephant swarm optimization technique.

The future of this work can be considered to compare the elephant swarm optimization technique with other swarm optimization techniques like particle swarm, ant swarm and a few other evolutionary computing based optimization techniques and prove its robustness.

References Références Referencias

1. Wilson, E.O. 2000. Sociobiology - The New Synthesis. Twenty Fifth Anniversary Editions. The Belknap Press of Harvard University Press Cambridge, Massachusetts and London, England.
2. Krebs, J. R., Davies, N. B. 1993. An Introduction to Behavioural Ecology - Third Edition. Blackwell Publishing. Oxford, UK.
3. Elizabeth A. Archie, Cynthia J. Moss and Susan C. Alberts, "The ties that bind: genetic relatedness predicts the fission and fusion of social groups in wild African elephants." Proc. R. Soc. B (2006) 273, 513–522.
4. ELIZABETH A. ARCHIE and PATRICK I. CHIYO, "Elephant behaviour and conservation: social relationships, the effects of poaching, and genetic tools for management", Molecular Ecology (2012) 21, 765–778.
5. Rachael Adams, "Social Behaviour and Communication in Elephants- It's true! Elephants don't forget!" Available at: http://www.wildlife-pictures-online.com/elephant-communication.html Acessed March 14th 2013.
6. Wyatt, T.D. 2003. Pheromones and Animal behaviour - Communication by Smell and Taste. Cambridge University Press. UK.
7. I.F. Akyildiz; W. Su, Y; Sankara subramaniam; E.Cayirci, "Wireless sensor networks: a survey", Computer Networks 38 (2002) 393–422.
8. Supiya Ujjain; Peter J. Bentley; "Particle Swarm Optimization Recommender System", 2003.
9. Berry, Randall A.; Yeh, Edmund M.; "Cross-layer wireless resource allocation", Signal Processing Magazine, IEEE on Sept. 2004, Volume: 21, Issue:5 Page(s): 59 – 68.
10. Jin, Lizhong; Jia, Jie; Chen, Dong; Li, Fengyun; Dong, Zhicao; Feng, Xue; "Research on Architecture, Cross-Layer MAC Protocol for Wireless Sensor Networks", Genetic and Evolutionary Computing (ICGEC), 2011 Fifth International Conference on Aug. 29 2011-Sept. 1 2011, Page(s): 291–294.
11. Pacharintanakul, Peera, Tipper, David W., "Differentiated crosslayer network mapping in multilayered network architectures", Telecommunications Network Strategy and Planning Symposium (NETWORKS), 2010 14th International on 27-30 Sept. 2010, Page(s): 1 – 6.
12. Kamatam, G.R.; Srinivas, P.V.S.; Chandra Sekaraiah, K., "SC3ERP: Stratified Cross Layer Congestion Control and Endurance Routing Protocol for Manets", Computational Intelligence, Communication Systems and Networks (CICSyN), 2012 Fourth International Conference on 24-26 July 2012, Page(s): 382 – 388.
13. Hang Su; Xi Zhang; "Cross-Layer Based Opportunistic MAC Protocols for QoS Provisioning Over Cognitive Radio Wireless Networks", IEEE Journal on Selected Areas in Communication on Volume 26 Issue 1, January 2008, Page 118-129.
14. Zheng Guoqiang; Ning Yonghai; Tang Shengyu; "Cross layer-based MAC protocol for wireless sensor networks", Control Conference (CCC), 2010 29th Chinese, 29-31 July 2010, Page(s): 4748– 4752.
15. Yingqi Lu; Du Zhang; Ya Chen; Xiao Liu; Ping Zong; "Improvement of LEACH in Wireless Sensor Networks based on balanced energy strategy", Information and Automation (ICIA), 2012 International Conference on 6-8 June 2012, Page(s): 111–115.
16. Sankar and Z. Liu, "Maximum lifetime routing in wireless ad-hoc networks," in Proc. INFOCOM, Mar. 2004, vol. 2, pp. 1089–1097.
17. J.-H. Chang and L. Tassiulas, "Energy conserving routing in wireless ad-hoc networks," in Proc. IEEE INFOCOM, Mar. 2000, vol. 1, pp. 22–31.
18. Jamal N. Al-Karaki and Ghada A. Al-Mashaqbeh, "SENSORIA: A New Simulation Platform for Wireless Sensor Networks", 2007 International Conference on Sensor Technologies and Applications, 2007 IEEE DOI 10.1109/SENSORCO-MM.2007.43.
19. Laiali Almazaydeh, Eman Abdelfattah, Manal Al-Bzoor, and Amer Al- Rahayfeh, "PERFORMANCE EVALUATION OF ROUTING PROTOCOLS IN WIRELESS SENSOR NETWORKS", International Journal of Computer Science and Information Technology, Volume 2, Number 2, April 2010 pp 64-73.
20. Amer A. Al-Rahayfeh, Muder M. Almi'ani, and Abdelshakour A. Abuzneid, "PARAMETERIZED AFFECT OF TRANSMISSIONRANGE ON LOST OF NETWORK CONNECTIVITY (LNC) OF WIRELESS SENSOR NETWORKS", International Journal of Wireless & Mobile Networks (IJWMN), Vol.2, No.3, August 2010. pp 63-80.
21. K. Dwivedi and O. P. Vyas, "An Exploratory Study of Experimental Tools for Wireless Sensor Networks", Wireless Sensor Network, 2011, 3, pp 215-240.
22. Jyoti Saraswat, Neha Rathi & Partha Pratim Bhattacharya, "Techniques to Enhance Lifetime of Wireless Sensor Networks: A Survey", Global Journal of Computer Science and Technology Network, Web & Security Volume 12 Issue 14 Version 1.0 Year 2012.

23. G. J. Foschini and J. Salz, "Digital communications over fading radio channels," Bell Systems Technical J., pp. 429–456, Feb. 1983.

Global Journal of Computer Science and Technology
Network, Web & Security
Volume 13 Issue 4 Version 1.0 Year 2013
Type: Double Blind Peer Reviewed International Research Journal
Publisher: Global Journals Inc. (USA)
Online ISSN: 0975-4172 & Print ISSN: 0975-4350

Enhancing Network Security using Ant Colony Optimization

By Parul Chhikara & Arun K. Patel
Gitm, Gurgaon, India

Abstract - Security of the information in the computer networks has been one of the most important research area. To preserve the secure condition it is essential to be aware of the behavior of the incoming data. Network Security is becoming an important issue for all the organizations, and with the increase in knowledge of hackers and intruders they have made many successful attempts to bring down high-pro le company networks and web service. The technology of artificial intelligence breaks a new way in the area of network security. Ant-colony optimization algorithm is an evolutionary learning algorithm which could be applied to solve the complex problems. Applying the idea of ant colony optimization into network vulnerability detection and enhancing security can improve the performance of network security management. This paper attempts to apply ACO Algorithm to find out vulnerabilities in the network and ensure its security.

Keywords : ACO, network security, pheromone intensity, NMAP, NESSUS.

GJCST-E Classification : D.4.6

ENHANCING NETWORK SECURITY USING ANT COLONY OPTIMIZATION

Strictly as per the compliance and regulations of:

Enhancing Network Security using Ant Colony Optimization

Parul Chhikara [α] & Arun K. Patel [σ]

Abstract - Security of the information in the computer networks has been one of the most important research area. To preserve the secure condition it is essential to be aware of the behavior of the incoming data. Network Security is becoming an important issue for all the organizations, and with the increase in knowledge of hackers and intruders they have made many successful attempts to bring down high-pro le company networks and web service. The technology of artificial intelligence breaks a new way in the area of network security. Ant-colony optimization algorithm is an evolutionary learning algorithm which could be applied to solve the complex problems. Applying the idea of ant colony optimization into network vulnerability detection and enhancing security can improve the performance of network security management. This paper attempts to apply ACO Algorithm to find out vulnerabilities in the network and ensure its security.

Keywords : ACO, network security, pheromone intensity, NMAP, NESSUS.

I. Introduction

Network Security can be views as local or global point of view depending upon the network design. Managing Security means understanding risks and deciding how to overcome if any security is violated. Network security is a level of guarantee that all the machines in a network are working optimally and the users of these machines only possess the rights that were granted to them. Network security is the most vital component in information security because it is responsible for securing all information passed through networked computers [1]. After gaining access to the network with a valid IP address, the attacker can modify, reroute, or delete your data [2]. A stack overflow attack on the BIND program, used by many Unix and Linux hosts for DNS, giving immediate account access [14]. In this paper we attempt to augment NESSUS Script using Java Plugin to include ACO behaviour in order to detect common vulnerabilities with ease.

II. Literature Review

Vulnerability in the system means having weakness in system. These weaknesses are greatly exploits by the hacker to gain access into your system. Any vulnerable system is open to the hacker they can do anything to your system. They can steal any type of information from your computer. Main cause of presence of any type of vulnerabilities in the system is due to lack of programming. When hackers came to know about this weaknesses about your system they can easily hook on to your system and can exploits them up to any extent.

Author α : M.tech Scholar, Dept. of Computer Science, GITM, Gurgaon, India. E-mail : pc.ggn1@gmail.com
Author σ : Dept. of Computer Science, GITM, Gurgaon, India. E-mail : arun.patel2001@gmail.com

a) Trojan A

Trojan in software security means a seemingly attractive or innocuous program that hides malicious software inside. Trojans can also be staged on download sites and disguised as utility programs, games, etc. and the victim is tricked into downloading them because they look like a useful program the victim might want to use [10].

b) Network Vulnerability

Network vulnerabilities are present in every system. Network technology advances so rapidly that it can be very difficult to overcome vulnerabilities altogether. Following are the type of vulnerabilities an administrator should take care of this: [11]

Internal network vulnerabilities result over extension of bandwidth (user needs exceeding total resources) and bottlenecks (user needs exceeding resources in specific network sectors).

DOS and DDOS are external attacks as the result of one attack or a number of coordinated attacks, respectively.

A war dialer is a tool used to scan a large pool of telephone numbers to detect vulnerable modems to provide access to the system. Following are the list of most vulnerable ports [12]:

- 139 (SMB over NetBIOS)
- 80 (HTTP)
- 25 (SMTP)
- 23 (Telnet)
- 20 21 (FTP)

Vulnerability analysis consists of several steps [13]:

- Defining and classifying network or system resources.
- Assigning relative levels of importance to the resources.
- Identifying potential threats to each resource.

III. Ant Colony Optimization

In a colony of social ants, each ant usually has its own duty and performs its own tasks independently from other members of the colony. However, tasks done by different ants are usually related to each other in such a way that the colony, as a whole, is capable of solving complex problems through cooperation [5, 6]. For example, for survival-related problems such as selecting the shortest walking path, finding and storing food, which require sophisticated planning, are solved by ant colony without any kind of supervisor.

Ants communicate through pheromone trails to exchange information about which path should be followed. As ants move, a certain amount of pheromone is dropped to make the path with the trail of this substance. Ants tend to converge to the shortest trail (or path), since they can make more trips, and hence deliver more food to their colony. The more ants follow a given trail, the more attractive this trail becomes to be followed by other ants. This process can be described as a positive feedback loop, in which the probability that an ant chooses a path is proportional to the number of ants that has already passed through that path [4, 5].

Researchers try to simulate the natural behavior of ants, including mechanisms of cooperation, and devise ant colony optimization (ACO) algorithms based on such an idea to solve the real world complex problems, such as the travelling salesman problem [7], data mining [6].

ACO algorithms solve a problem based on the following concept:

- Each path followed by an ant is associated with a candidate solution for a given problem.
- When an ant follows a path, it drops varying amount of pheromone on that path in proportion with the quality of the corresponding candidate solution for the target problem.
- Path with a larger amount of pheromone will have a greater probability to be chosen to follow by other ants. The process is thus characterized by a positive feedback loop, where the probability with which an ant chooses a path increases with the number of ants that previously chose the same path [3].

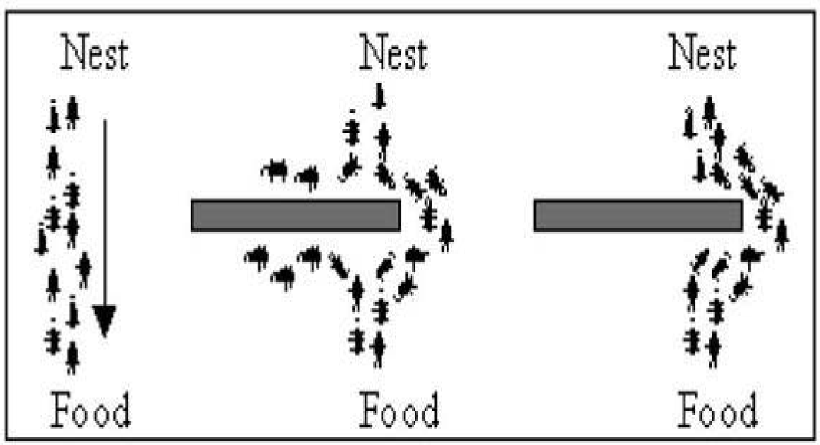


Figure 1 : How ants find food from the nest

The idea of the ant colony algorithm is to mimic this behaviour with simulated ants" walking around the graph representing the problem to solve [8]. In the real world, ants (initially) wander randomly, and upon finding food return to their colony while laying down pheromone trails [9].

IV. Experimental Design

a) Operating System Fingerprinting

Network scanning, and particularly remote OS/application detection, is generally the first step in mapping out a network; whether for penetration testing or simply maintaining a network device inventory. Remote active operating system finger-printing is the process of determining the identity of a remote host's operating system. This is done by actively sending packets to the remote host and analyzing the responses. Tools like Nmap and Xprobe 2 take the responses and form a finger-print that can be queried against a signature database of known operating systems. Learning which operating system is running on a remote host can be very valuable for both pen testers and black-hats.

b) NMAP

NMAP is a network auditing tool that scans network hosts for open ports. Port scans can determine if a host is offering errant services or failing to over required services. Examples of errant service are an http daemon on a host not listed as a web server and a backdoor opened by a Trojan horse. Nmap can also determine the operating system running on scanned host, and scan firewalls to determine the parts a re-wall effectively filters. NMAP can scan network host using one of six methods: TCP connect() scan, TCP SYN scans, stealth FIN scans, XMAS tree scans, NULL scans, UDP scans, and ping scans.

i. *OS Fingerprinting through NM AP*

Nmap is a network exploration tool and security scanner. It is designed to allow users to scan networks to determine which hosts are up and what services they offer. Nmap supports a number of scanning techniques that use the following protocols: TCP, ICMP, UDP and IP. Nmap also includes features like remote OS detection, parallel scanning and port filtering detection.

c) Fuzzing

Fuzzing is the art of automatic bug finding. This is done by providing an application with semi- valid input. The input should in most cases be good enough so applications will assume it's valid input, but at the same time be broken enough so that parsing done on this input will fail. Such failing can lead to unexpected results such as crashes, information leaks, delays, etc. It can be seen as part of quality assurance, although only with negative test cases. Fuzzing is mostly used to uncover security bugs, however, it can often also be used to spot bugs that aren't security critical but which can non-the-less improve robustness.

d) NESSUS

Nessus was created to be a free, powerful, remote security scanner. It is one of the top-rated security software products, and is endorsed by professional information security organizations such as the SANS Institute. The "Nessus" security scanner is a software which will audit remotely a given network and determine whether someone (or something - like a worm) may break into it, or misuse it in some way. Nessus can perform over 900 security checks.

i. *Web server Fingerprinting with NASL*

```
include("http func.inc");
sock=open sock tcp(80);
req=string("GET / HTTP/1.0 ","Accept: */* "," ");
send(socket:sock,d t :req);
r=revc(socket:sock, length:4096); if("Server:
Apache"><r) display("Apache Server running on
host"); else if("Server: Microsoft-IIS"><r)
display("IIS Server running on host"); http close
socket(sock);
```

ii. *Java based Ant Colony Optimization for Network Vulnerability Detection*

```
WHILE termination conditions not met
DO
PerformActivities
ACO NVD()
PheromoneUpdate()
ScheduledActions()
END PerformActivities
ENDWHILE
```

iii. *ACO NVD()*

This method builds a solution to the problem by detecting vulnerability moving from node to node and constructing graph G. Ants move by applying a stochastic local decision policy that makes use of the pheromone values (NVD score: Candidate or Non Candidate) on running apps. When adding a component to the current partial solution, an ant can update the values of the pheromone trails that were used for this construction step. This kind of pheromone update is called online step-by-step pheromone update. Once an ant has built a solution, it can retrace the same path backward and update the pheromone trails of the used apps according to the quality of the solution it has built. This is called online delayed pheromone update. Another important concept in Ant Colony Optimization is pheromone evaporation. Pheromone evaporation is the process by means of which the pheromone trail intensity on the apps decreases over time. It implements a useful form of forgetting, favoring the exploration of new areas in the search space. Each attack scenario is depicted by an attack path which is essentially a series of exploits with a severity score that presents a comparative desirability of a particular network ser-vice. In an attack graph with a large number of attack paths, it may not be feasible for the administrator to plug all the vulnerabilities.

Following nessus script is fabricated to create new packets and send over the network using send packet() function. Ip = forge ip packet(ip hl : 5; ip v : 4; ip tos : 0; ip len : 20; ip id : 12; ip off : 0; ip ttl : 255; ip p : 2; ip src : 172:31:9:15);

```
ACO NVD()
Display(this host(),"");
Send packet(ip,pcap active: FALSE);
172.31.9.91
```

The ip packet can be created using the function forge ip packet. This function takes up a large number of parameters. The first four bits is the version of ip used, 4 and set this value as the ip_c parameter. The next four bits are the length of the ip header and in this case as nothing is added to ip, it is 5.The length of the ip header can vary minimum 20 to maximum 60 as four bits hold a number from 0 to 15. The parameter name is ip_hl. Then we have the type of service which signifies the importance of packets to the routers. Unfortunately most routers ignore this field called ip_tos. Then there are two bytes that give the total length of Most of the time this field is ignored. Packet has an id of 12.

V. RESULTS AND CONCLUSION

Graph showing the comparison of Java Nessus. ACO API with the network vulnerability tool. It takes much less time in comparison with other algorithm. Thus, validating the research work.

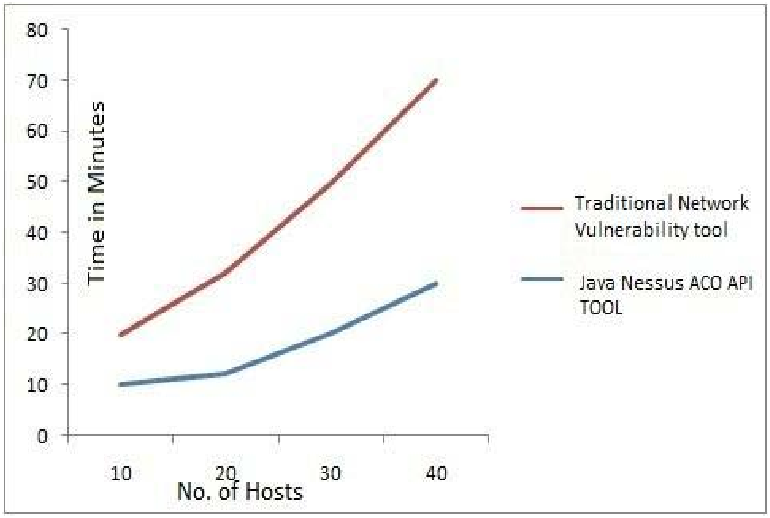


Figure 2 : Comparison of Nessus ACO API with other

References Références Referencias

1. Introduction to Network Security, Dr. Rahul Banerjee, BITS-Pilani, India www.discovery.bits-pilani.ac.in/rahul/CompNet/index.htm
2. http://technet.microsoft.com/enus/library/cc959354.asp.
3. Dorigo, M, Maniezzo V., & Colorni, A. (1996). The ant system: Optimization by a colony of cooperating agents. IEEE/ACM Transactions on System, Man and Cybernetics-Part B, 26(1), 1–13.
4. Dorigo M, Di Caro G, Gambardella LM (1999) Ant algorithms for discrete optimization. Artificial Life 5(2):137–172
5. Dorigo M, Maniezzo V, Coloni A (1996) Ant system: optimization by a colony of cooperating agents. IEEE Trans Syst Man Cybern 26(1):29–41
6. Parpinelli RS, Lopes HS, Freitas AA (2002) Data mining with an ant colony optimization algorithm. IEEE Trans Evol Comput 6(4):321–332
7. Dorigo M, Gambardella LM (1997) Ant colony system: a cooperative learning approach to the travelling salesman problem. IEEE Trans Evol Comput 1(1): 53–66
8. http://en.wikipedia.org/wiki/Ant colony optimization
9. http://www.antcolonies.net/howantscommunicate.htm
10. http://www.infosectoday.com/Articles/Exploiting_Software Vulnerabilities.htm
11. http://www.javvin.com/etrac/networkvulnerabilities.html
12. A Vulnerability Assessment of the East Tennessee State University Administrative Computer Network, Dr. Phillip E. Pfei er, IV, chair Dr. Gene Bailey Dr. QingYuan.
13. http://searchmidmarketsecurity.techtarget.com/sDenition/0,, sid198gci1176511,00.htm
14. Network Attack nd Defence, By Roger Needham and Butler Lamson. www.cl.cam.ac.uk/rja14/paper/SE-18.pdf

Global Journal of Computer Science and Technology
Network, Web & Security
Volume 13 Issue 4 Version 1.0 Year 2013
Type: Double Blind Peer Reviewed International Research Journal
Publisher: Global Journals Inc. (USA)
Online ISSN: 0975-4172 & Print ISSN: 0975-4350

A Secured Model for Resource Access in Grid Environment

By Dr. Gulshan Ahuja

Tilak Raj Chadha Institute of Management & Technology, India

Abstract - Grid computing provides a way to execute applications over autonomous, distributed and heterogeneous nodes. The main goal of grid technology is to allow sharing of resources and services under a set of rules and policies, which govern the conditions for access to the resources. This paper reviews the state of security and access control for resources in grid environment and presents a secured model for resource access in grid environment.

Keywords : grid computing, services, resource access.

GJCST-E Classification : H.3.5

A SECURED MODEL FOR RESOURCE ACCESS IN GRID ENVIRONMENT

Strictly as per the compliance and regulations of:

A Secured Model for Resource Access in Grid Environment

Dr. Gulshan Ahuja

Abstract - Grid computing provides a way to execute applications over autonomous, distributed and heterogeneous nodes. The main goal of grid technology is to allow sharing of resources and services under a set of rules and policies, which govern the conditions for access to the resources. This paper reviews the state of security and access control for resources in grid environment and presents a secured model for resource access in grid environment.

Keywords : grid computing, services, resource access.

I. Introduction

Grid computing aspires to integrate technology and solutions, which enable and control access to computing resources. These resources are generally located at diverse locations and very little information regarding their exact location is known. The need to share resources, coupled with distributed and heterogeneous nature of the web environment, entails the formation of virtual organization.

A virtual organization is defined as a set of individuals and institutions, sharing resources and services, under mutually decided and agreed set of rules and policies. The resources to be accessed are not only limited to file sharing, but expand to a wide spectrum such as computers, software data and other resources as are required by a range of collaborative problem solving and resource brokering strategies.

In a virtual organization setup, individuals and institutions agree to share resources and collaborate on an adhoc dynamic basis, where each real organization is governed by its own set of internal rules and policies. The virtual organization poses challenges such as interoperability among domains, need to maintain separation of the security policies etc.

Security of grid services is a fundamental requirement behind any grid security model. Securing web services consists of providing security services such as authentication, confidentiality, integrity etc. to the exchanged messages. A security model to secure grid services must ensure that grid services when invoked by a service requester adhere to policy constraints, as specified by the hosting environment.

A no. of security standards for web services have been proposed as shown in Figure 1.1. Ensuring the integrity, confidentiality and security of grid services through the application of a comprehensive security model is critical, for both the organization and their customers. This is done using web services. Web services [1] provide an architecture that has the ability to deliver integrated, interoperable, solutions. Web services are loosely coupled applications, which use well known XML protocols like WSDL [2], SOAP [3] and UDDI [4] for representation and communicating across different security domains in the distributed environment.

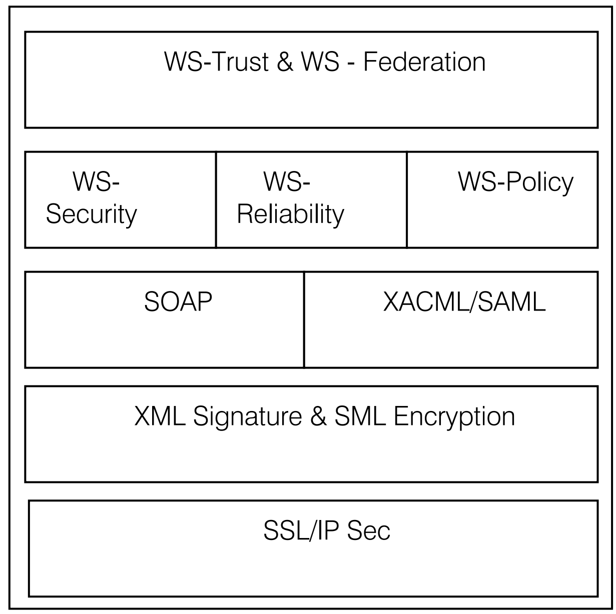


Figure 1.1 : Web Services Security Standards

Compared with the existing distributed object technologies such as DCOM, CORBA and J2EE, web services are opening and loose coupled. Web services create new security challenges because XML documents are encoded in text, rather than in binary form and can readily be transmitted through standard firewalls. These aspects make web services security more troubling and difficult. This paper presents a secured model for resource access in grid Environment. The security of the proposed approach has been improved by adopting secure certificates and use of users' attributes.

The remainder of the paper is organized as follows. Section II discusses the related work in the field of grid technology and web services. Section III presents details about web services security specifications. Section IV presents the problem statement. Section V presents a secured model for resource access in grid environment and discusses its working. Section VI concludes the paper and brings out future scope of work.

Author : Assistant Professor, Tilak Raj Chadha Institute of Management & Technology, Yamuna Nagar, India.
E-mail : ahujag_24@yahoo.com

II. Related Work

Over the past several years there has been a lot of work towards the development of grid technology. A good survey in this direction can be found in [5]. Most of the grid management systems provide various grid services such as security, data management, remote execution and monitoring. The grid applications pack different components in to a single package such as in case of Globus toolkit, Grid FTP for data management, GRAM for execution management and MDS for information service are packed together. The separation of service component provides flexibility in terms of selection of services but makes sharing of grid resources and authentication more complex.

An active grid at Grid Laboratory of Winsconsin [6], presented as a campus wide distributed computing environment, which was designed to meet the scientific computing needs of the university. It was built from autonomous sites from across the campus, which engineered to meet their own specific requirements and cooperated to join with the other sites. Natraj et al. [7] presented a comprehensive grid security architecture, which supported popular security models. Foster et al. [8, 9] presented an analysis of the unique security requirements of large scale distributed computing and a secure architecture. Damiani et al. [10] presented a fine grained access control model for SOAP e services.

III. Web Services Security Specification

Web services security specification (WSS) [11] allows protecting SOAP messages with XML security. WSS provides confidentiality using XML encryption and integrity using XML signature. An XML signature [12] provides integrity, authenticity and non repudiation by enabling entities to sign an entire XML document or some part of this document. An XML signature is an XML document containing information about the signing process, references to the signed parts and the signature value. To process an XML signature, the sender generates a digest for each referenced part before calculating the digital signature value using the specified algorithms. Then the signed XML message is formed by incorporating the signature value, the different digests and information about used algorithms and keys. This allows the recipient to proceed to the validation of this signature. XML encryption [13] provides confidentiality by allowing the encryption of XML data. The result of encryption is an XML document containing information about the encryption process and the encrypted data or reference to this data. The encryption of XML data requires the selection of an algorithm and a key that will be transmitted to the receiver of the message. Then data is serialized before using the chosen algorithm and key. Finally, the message to transmit is formed by adding the encrypted data or reference to this data.

WSS provides SOAP messages with security by using XML signature to sign a SOAP message and transmit the signature and XML encryption to encrypt the message. WSS transmits security information in the headers of SOAP messages, such as keys and security tokens that represent the identities and can be associated to digital signature in order to ensure authentication of the message origin. To secure a SOAP message, WSS denies security headers. In fact, the header of a SOAP message can contain one or more security headers where each of them provides security information on this message to a recipient that can be final or intermediate recipients. To sign one or more elements in a SOAP messages, the security header, added by the sender includes a signature, which conforms to that specified by XML signature. The recipient of the SOAP message proceeds to the validation of the signature. In case if validation fails, a fault message is delivered otherwise the signature is validated and a confirmation is sent to the sender in the header of the response message. To encrypt one or more elements of a SOAP message, the security header must include references to the encrypted elements and information about the used key. Then each element to encrypt is replaced by the equivalent encrypted data. The recipient of a SOAP message identifies the decryption key and the element to decrypt.

Thereafter, each encrypted element is decrypted. Encryption and decryption are performed according to XML encryption.

IV. Problem Statement

To provide security in the grid environment, a number of security implementation software's are available. These implementations use different techn-iques, protocols and tools for securing resource access in grid environment. GSI is the most common among these methods, which has been implemented in Globus Toolkit 4. GSI uses public key infrastructure (PKI) for encryption and decryption of data, secure socket layer (SSl) for authentication of entity, message integrity & message privacy, X509 public key certificate for delegation of rights etc.

There are middleware, which provide single sign on such as Microsoft's Passport and VeriSign. etc., but these cannot be used in the grid environment due to the following reasons. Passport uses a centralized server to provide authentication. It supports only user name and password method and does not support latest methods like delegation and proxy certificates. The services provided by these middleware agents are paid and a service requester must register with all service providers before utilizing services located at different sites. Moreover, these methods are not suitable for securing resource access in a grid environment. To address the above said problems, this paper proposes a certificate and attributes based model for secured resource access in a grid environment.

V. Proposed Model

Figure 1.2 depicts the detailed view of the proposed model. It mainly comprises of four entities such as (a) Client Requester (b) Service Provider (c) Certificate Authority (d) Attribute Authority.

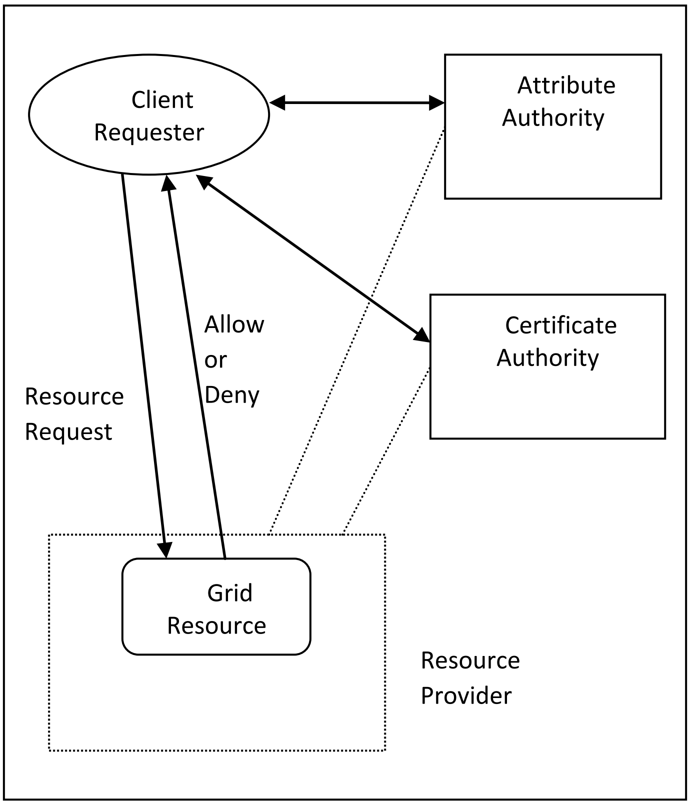


Figure 1.2 : Access Model for Resource Access

A detailed description of each entity is given below:

a) Client Requester (CR)

The CR a requester side component, which is responsible for obtaining digital certificate(s) from the CA, storing in requester's machine, obtaining required attributes from the AA and producing certificates and attributes as and when required for resource access.

b) Resource Provider (RP)

The RP controls the access top the requested resources and verifies the authenticity and authorization details corresponding to a resource request.

c) Certificate Authority (CA)

The CA is a server in the domain, which generates the X.509 certificates, which are used by the grid users and the RP for implementing security. The primary responsibilities of CA are to identify entities, which require certificates, Issuance, removal and archiving certificates and to maintain a name space of unique names for certificate owners. A certificate is represented as a data structure containing public key and pertinent details about the owner of the key. A certificate works as a tamper proof electronic document once signed by the certificate authority for use with the grid environment. A digital certificate contains information about the host who is being certified and its public key.

When a user wants to access a resource in a grid, he attaches a certificate to the request message. On receiving the message, the RP verifies the signature of the certificate within the certificate. After verification, the RP can safely accept the public key contained in the certificate,

d) Attribute Authority (AA)

An AA is an authority who is trusted by user to create and sign an attribute certificate (AC) on his behalf. The time and validity requirements for ACs allow creating ACs, which are long-lived and short-lived. The short validity period may be in number of hours instead of months or years as is the case is identity certificates. The longer-lived attribute certificates are issued where the authorization information is going to remain static for a long period. One more reason to use attribute certificates to contain and specify authorization information is for easily changing the authorization information without making any side effect.

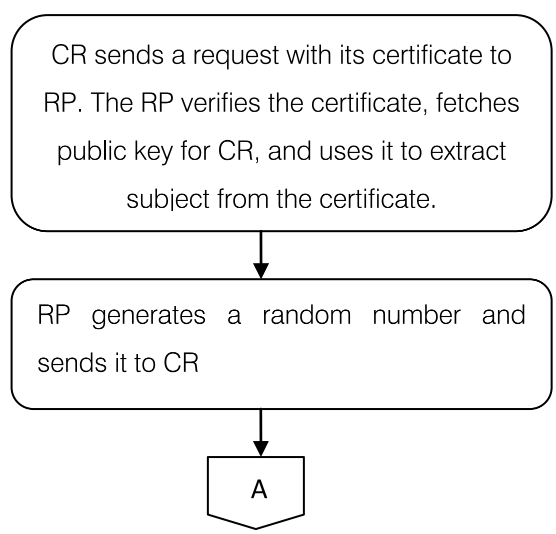
e) Working of the Proposed Model

The step by step working of the proposed model is as follows.

Step 1: CR registers with the CA to obtain digital certificate and registers with the AA for requesters' attributes.

Step 2: CR sends a request to RP for accessing a resource. This request contains the digital certificate and requester's attributes.

Step 3: RP carries the authentication of request using procedure as depicted in Figure 1.3.



Global Journal of Computer Science and Technology (E) Volume XIII Issue IV Version I Year 2013

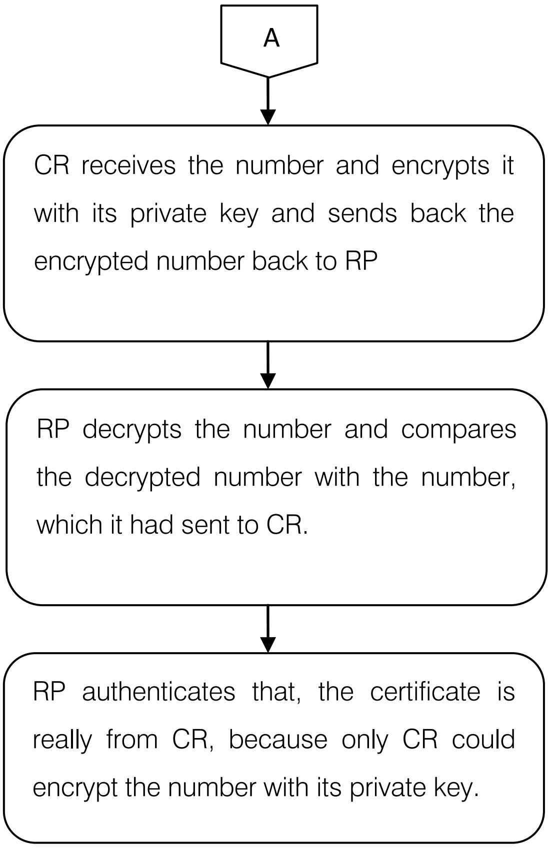


Figure 1.3 : Authentication Process

Step 4: CR sends an attribute query message to AA and receives a response for requester's attributes. The request message and response message is sent using SOAP handler.

Step 5: RP evaluates the obtained attributes as per algorithm as shown in Figure 1.4. Each accessible resource in the grid environment is assigned with a set of applicable policies. For each policy, a set of constraints specify the conditions, which must be satisfied for positive evaluation of the applicable policies. Each policy is evaluated against set of constraints to find out whether the resource access request can be granted or not.

```
Algorithm: EvaluateAttributes(Input:

RR_ID // Identifier of the
Requested Resource
AS = (A1, A2, A3..............An )
// Submitted Attribute Set

PS = (P1, P2, P3.....Pn) //Policy Set
CS // Constraints Set
Output: Allow/Deny)

        for all Pi in PS
          If (Pi _RRID == RR_ID)
            for each Ci in CS
                evaluate Ci against AS for
                outcome
                 if(outcome == false)
                        return Deny
                end if
            end loop
        end if
      end loop
                    return Allow
```

Figure 1.4 : Algorithm for Evaluation of Attributes

Step 6: The outcome of the algorithm is used to allow or deny access to the requested resource.

The use of requesters' attributes allows more robust access mechanism to be placed for resource access.

VI. Conclusion & Future Scope

This paper has presented a secured model for resource access in grid environment. The approach makes use of digital certificate and requesters' attributes for making decisions about resource access. The digital certificate is used to authenticate the user and requester's attributes are further used with an identified and requested resource type. The evaluation of attributes is carried by associating a set of constraints and policies with the resources. The paper has highlighted that how web services technology allows complex integration of technology and protocols to allow resource access.

References Références Referencias

1. Curbera F., Nagy W. A., Weerawarana S., "Web Services: Why and How", Workshop on Object-Oriented Web Services, October 2001.
2. Chinnici, R., M. Gudgin, J. Moreau, and S. Weerawarana, "Web Services Description Language (WSDL)", version 1.2, World Wide Web Consortium (W3C), http://www.w3.org/TR/wsdl12, July 2002.
3. Box, D., "Simple Object Access Protocol (SOAP) 1.1", "http://www.w3.org/TR/SOAP", May 2000.
4. Luc Clement et al., "OASIS UDDI Specifications", http://www.oasis-open.org/committees/uddi-spec/doc/tcspecs.htm, 2002-2004.
5. "A Taxonomy and Survey of Grid Resource Management Systems for Distributed Computing", Software Practice and Experience, pp. 135-163, 2002.
6. http://www.cs.wisc.edu/condoe/glow/index.html
7. Natraj Nagaratnam, Phillippe Janson, John Dayka, Anthony Nadalin, Frank Siebenlist, Ian Foster, "Security Architecture for Open Grid Services", Public Draft, July 2002.
8. Foster I., Kesselman C., "A Secure Architecture for Computational Grids", 5th ACM Conference on Computer and Communications Security, 1998.
9. Foster I., Kesselman C, "The Grid Blueprint for a new Computing Infrastructure", 1999.
10. E. Damiani, S.D.C di Vimercati, S. Paraboschi, and P. Samarati, "Fine grained access control for SOAP e-services", In Proceedings of 10th International Conference on World Wide Web (WWW), Hong Kong, pp. 504–513, 2001.
11. Nadalin et al., "Web Services Security Specification 1.1", OASIS Standard Specification, OASIS Committee, February 2006.
12. Mark Bartel, John Boyer, Barb Fox, Brian LaMacchia, Ed Simon, "XML Signature Syntax and Processing", W3C Recommendation, June 2008.
13. "XML Encryption Syntax and Processing", W3C Recommendation, Dec. 2002.

This page is intentionally left blank

Global Journal of Computer Science and Technology
Network, Web & Security
Volume 13 Issue 4 Version 1.0 Year 2013
Type: Double Blind Peer Reviewed International Research Journal
Publisher: Global Journals Inc. (USA)
Online ISSN: 0975-4172 & Print ISSN: 0975-4350

Performance Evaluation of AODV and FSR Routing Protocols in Manets

By M Ravi Kumar, Dr. N. Geethanjali & N. Ramesh Babu
Sri Krishnadevaraya University, India

Abstract - A mobile adhoc Network (MANET) is an infrastructure less, decentralized multi-hop network where the mobile nodes are free to move randomly, these making the network topology dynamic. MANET routing protocols show different performance in different mobile network scenarios. In this paper an attempt has been made to understand the characteristics/behavior of ad hoc on demand distance vector (AODV) and Fisheye State Routing (FSR)protocols. The analysis of these protocols has been done using NS-2.

Keywords : AODV, FSR, MANETs, NS-2.

GJCST-E Classification : C.2.5

PERFORMANCE EVALUATION OF AODV AND FSR ROUTING PROTOCOLS IN MANETS

Strictly as per the compliance and regulations of:

Performance Evaluation of AODV and FSR Routing Protocols in Manets

M Ravi Kumar α, Dr. N. Geethanjali σ & N. Ramesh Babu ρ

Abstract - A mobile adhoc Network (MANET) is an infrastructure less, decentralized multi-hop network where the mobile nodes are free to move randomly, these making the network topology dynamic. MANET routing protocols show different performance in different mobile network scenarios. In this paper an attempt has been made to understand the characteristics/behavior of ad hoc on demand distance vector (AODV) and Fisheye State Routing (FSR)protocols. The analysis of these protocols has been done using NS-2.

Keywords : AODV, FSR, MANETs, NS-2.

I. Introduction

Wireless networking is an emerging technology that allow user to access information and services electronically. Regardless of their geographic position. Wireless network can be classified in two types-Infrastructure network and Infrastructure Less networks or Ad-hoc Network [1].

a) Infrastructure Networks

Infrastructure mode wireless networking brides a wireless network to a wired Ethernet network. Infrastructure mode wireless also supports central connection points for WLAN clients. Infrastructure network consist of fixed and wired gateways. A mobile host communicates with a bridge in the network within in communicating radius. The mobile unit can move geographically while it is communicating. When it goes out of rage of one base station, it connects with new base station and start communicating through it. This is called handoff. In this approach the base station are fixed [2].

b) Infrastructure Less (ad-hoc) Networks

An Infrastructureless Networks is a collection of mobile nodes that are dynamically and arbitrarily located in such a manner that the interconnections between nodes are capable of changing on a continual basis. The primary goal of such an infrastructure less networks is correct and efficient route establishment between a pair of nodes so that messages may be delivered in a timely manner.

Author α ρ : Research Scholar, Department of Computer Science & Technology, Sri Krishnadevaraya University.
E-mail : www.mravikumar@gmail.com, ramesh.phd.sku@gmail.com
Author σ : Professor, Department of Computer Science & Technology, Sri Krishnadevaraya University, Anantapur, A.P, India.
E-mail : www.ngeethanjali@gmail.com

Multicasting is to send single copy of a packet to all of those of clients that requested it, and not to send multiple copies of a packet over the same portion of the network, nor to send packets to clients who don't want it. Ad-hoc network are basically peer-to-peer self-organizing and self-configuring multi-hop mobile wireless network where the structure of the network changes dynamically [3]. This is mainly due to the mobility of nodes. Nodes in this network utilize the same random access wireless Channel, cooperating in friendly manner to engaging themselves in multi-hop Forwarding. The nodes in the network not only act as hosts but also as routers that route data to/from other nodes in the network [3]. Ad-hoc network flat routing protocols may classify as:

i. *Proactive routing (Table-driven) protocols*

Proactive routing or table-driven routing protocols attempt to maintain consistent, up-to date routing information from each node to every other node in the network. These protocols require each node to maintain one or more tables to store routing information, and they respond to change in network topology by propagating route update throughout the network to Maintain consistent network view.

ii. *Reactive (On-demand) routing protocols*

In reactive or on demand routing protocols, the routes are created as when required. When a source wants to send to a destination, it invokes the route discovery mechanism to find the path to the destination. This process is completed when once a source is found or all possible route permutation has been examined. Once a route has been discovered and established, it is maintained by some form of route maintenance procedure until either the destination becomes inaccessible along every path from the source or route is no longer desired.

The following point shows the importance of ad hoc networks.

a. *Instant Infrastructure*

Unplanned meetings, spontaneous inter-personal communications etc., cannot rely on any infrastructure, it needs planning and administration. It would take too long to set up this kind of infrastructure; therefore ad-hoc connectivity has to setup.

b. *Disaster Relief*

Infrastructure typically breakdown in disaster areas. Hurricanes cut phone and power lines, floods destroy Base stations, fires burn servers. No forward planning can be done, and the set-up must be externally fast and reliable. The same applies to many military activities, which are, to be honest, one of the major driving forces behind mobile ad-hoc networking research.

c. *Effectiveness*

Service provided by existing infrastructure might be too expensive for certain applications. If, for example only connection oriented cellular network exist, but an application sends only small status information every other minute, cheaper ad-hoc packet-oriented network might be a better solution. Registration procedure might take too long and communication overheads might be too high with existing networks. Tailored ad- hoc networks can offer a better solution [4].

d. *Remote Areas*

Even if infrastructure could be planned ahead, it is sometimes too expensive to set up an infrastructure in sparsely populated areas. Depending on the communication pattern, so ad-hoc networks or satellite infrastructure can be a solution.

II. Overview of the Protocol

a) *Ad hoc On Demand Distance Vector (AODV)*

Ad hoc On Demand Distance Vector Routing Protocol (AODV) is a reactive routing protocol designed for Ad hoc wireless network and it is capable of both unicast as well as multicast routing [5]. The Route Discovery process in this protocol is performed using control messages Route Request (RREQ) and Route Reply (RREP) whenever a node wishes to send packet to destination. Traditional routing tables is used, one entry per destination [6]. During a route discovery process, the source node broadcasts a Route Request packet to its neighbors. This control packet includes the last known sequence number for that destination. If any of the neighbors has a route to the destination, it replies to the query with Route Reply packet; otherwise, the neighbors rebroadcast the Route Request packet. Finally, some of these query control packets reach the destination, or nodes that have a route to the destination. At this point, a reply packet is generated and transmitted tracing back the route traversed by the query control packet. In the event when a valid route is not found or the query or reply packets are lost, the source node rebroadcasts the query packet if no reply is received by the source after a time-out. In order to maintain freshness node list, AODV normally requires that each node periodically transmit a HELLO message, with a default rate of one per second [13]. When a node fails to receive three consecutive HELLO messages from its neighbor, the node takes is as an indication that the link to its neighbor is down. If the destination with this neighbor as the next hop is believed not to be far away (from the invalid routing entry), local repair mechanism may be launched to rebuild the route towards the destination; otherwise, a Route Error (RERR) packet is sent to the neighbors in the precursor list associated with the routing entry to inform them of the link failure [14].

b) *Fisheye State Routing (FSR)*

Fisheye State Routing (FSR) [9] protocol is a proactive (table driven) ad hoc routing protocol and its mechanisms are based on the Link State Routing protocol used in wired networks. FSR is an implicit hierarchical routing protocol. It reduces the routing update overhead in large networks by using a fisheye technique. Fisheye has the ability to see objects the better when they are nearer to its focal point that means each node maintains accurate information about near nodes and not so accurate about far-away nodes. The scope of fisheye is defined as the set of nodes that can be reached within a given number of hops. The number of levels and the radius of each scope will depend on the size of the network. Entries corresponding to nodes within the smaller scope are propagated to the neighbors with the highest frequency and the exchanges in smaller scopes are more frequent than in larger. That makes the topology information about near nodes more precise than the information about far away nodes. FSR minimized the consumed bandwidth as the link state update packets that are exchanged only among neighboring nodes and it manages to reduce the message size of the topology information due to removal of topology information concerned far-away nodes. Even if a node doesn't have accurate information about far away nodes, the packets will be routed correctly because the route information becomes more and more accurate as the packet gets closer to the destination. This means that FSR scales well to large mobile ad hoc networks as the overhead is controlled and supports high rates of mobility.

III. Simulation Methodology

Simulation based study using Network Simulator NS-2 [10] has been used to compare two protocols viz. AODV and FSR under varying node density and varying pause time, assuming that the size of network, maximum speed of nodes and transmission rate are fixed. Tables 1 and 2 summarize the parameters used in the communication and movement models for simulation.

a) *Communication Model*

The simulator assumes constant bit rate (CBR) traffic with a transmission rate of 8 packets per second. The number of nodes varies from 25 to 100 in the denomination of 25, 50, 75 and 100. Given on the last line.

Parameter	Value
Traffic type	CBR
Number of nodes	25, 50, 75, 100
Transmission rate	8 packets/second

Table 1 : Parameters of Communication Model

b) Movement Model

In line with the realistic mobility pattern of the mobile nodes, the simulation assumes a Random Waypoint Model [7], where a node is allowed to move in any direction arbitrarily. The nodes select any random destination in the 500 X 500 space and moves to that destination at a speed distributed uniformly between 1 and nodes maximum speed (assumed to be 20 meter per second). Upon reaching the destination, the node pauses for fixed time, selects another destination, and proceeds there as discussed above. After testing all possible connection for a specific scenario, pause time changes to test the next scenario. This behavior repeats throughout the duration of the simulation (500 seconds). Meanwhile, number of nodes and pause time has been varied to compare the performance of the protocols for low as well as high density environment and for low mobility of the nodes to high mobility. Table 2 lists the movement parameters of the simulations.

Parameter	Value
Simulator	NS-2
Simulation time	500 seconds
Area of the network	500 m x 500 m
Number of nodes	25, 50, 100, 200
Pause time	10 seconds
Maximum speed of nodes	20 meters per second
Mobility Model	Random waypoint

Table 2 : Parameters of movement model

c) Performance Metrics

Three performance metrics has been measured for the protocols.

d) Throughput

Throughput is the number of packet that is passing through the channel in a particular unit of time [8]. This performance metric shows the total number of packets that have been successfully delivered from source node to destination node. Factors that affect throughput include frequent topology changes, unreliable communication, limited bandwidth and limited energy.

$$Throughput = \frac{Received\_Packet\_Size}{Time\ to\ Send} \quad (1)$$

e) Average End-to-End Delay

A specific packet is transmitting from source to destination node and calculates the difference between send times and received times. This metric describes the packet delivery time. Delays due to route discovery, queuing, propagation and transfer time are included metric [13].

$$Avg\_End\_to\_End\_Delay = \frac{\sum_1^n (CBR\_Sent\_Time - CBR\_Recv\_Time)}{\sum_i^n CBR\_Recv} \quad (2)$$

f) Normalized Routing Load

Normalized Routing Load is the ratio of total number of routing packet received and total number of data packets received [12].

Normalized_Routing_Load=

$$\frac{Number\_of\_Routing\_Pkts\_Recvd}{Number\_of\_Data\_Pkts\_Recvd} \quad (3)$$

IV. Simulation Result and Analysis

Figures 1, 2 and 3 represent the performance analysis in terms of throughput, average end-to-end delay and normalized routing load respectively. In all the cases the node density varies from 25 to 100 and pause time varies from 5 to 20 second.

a) Throughput

Based on the result of simulation as indicated in Fig 1(a) it is evident that performance of AODV is better than FSR in a low node density environment but with a rise innode density FSR out performs AODV which is evident from Fig 1(b), 1(c) and 1(d).

Another characteristic that has come to the notice is that pause time does not have significant bearing on the throughput whereas the performance is dictated only by the density of the network. The possible reason for the same is due to proactive nature of FSR routing protocol, which causes less number of table update in a stable topology, thus producing better throughput.

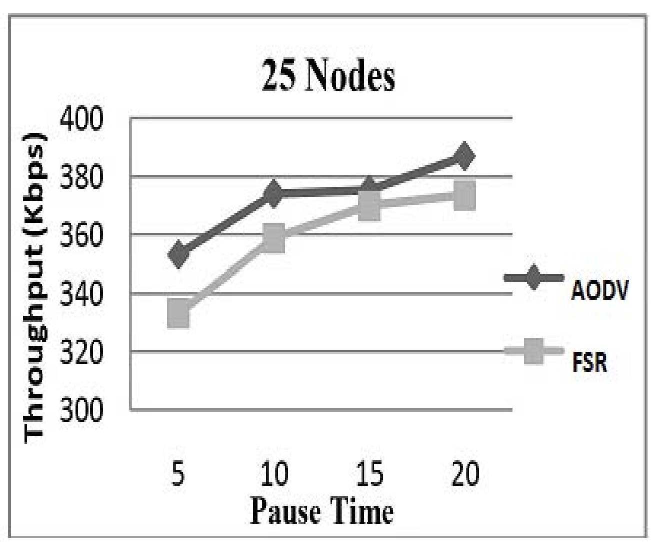


Figure 1(a) : Throughput for 25 nodes

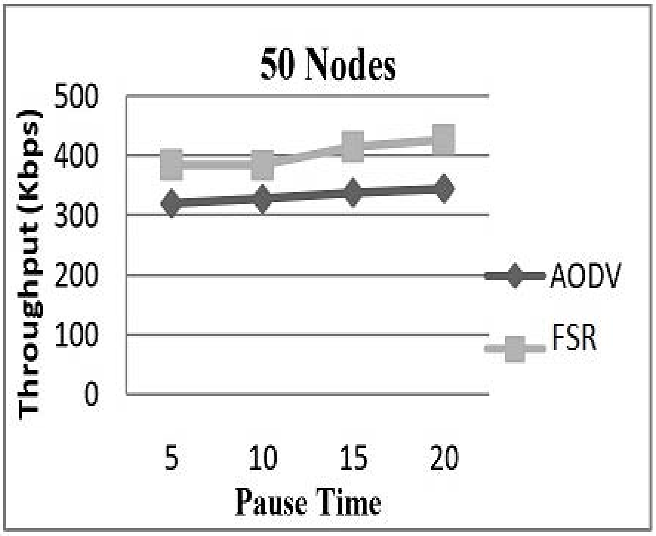


Figure 1(b) : Throughput for 50 Nodes

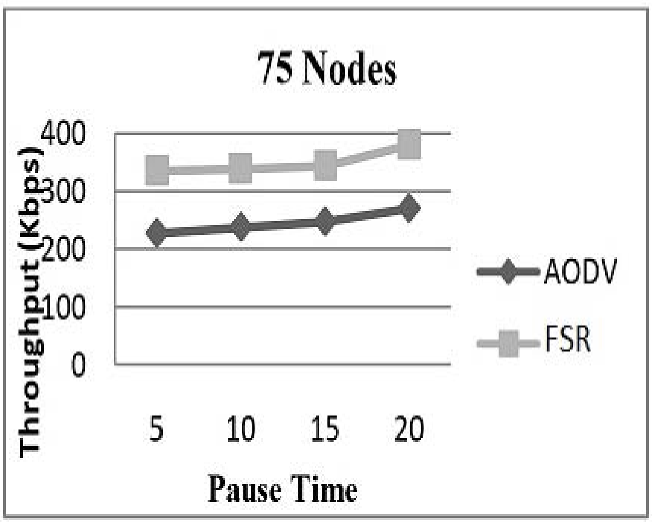


Figure 1(c) : Throughput for 75 Nodes

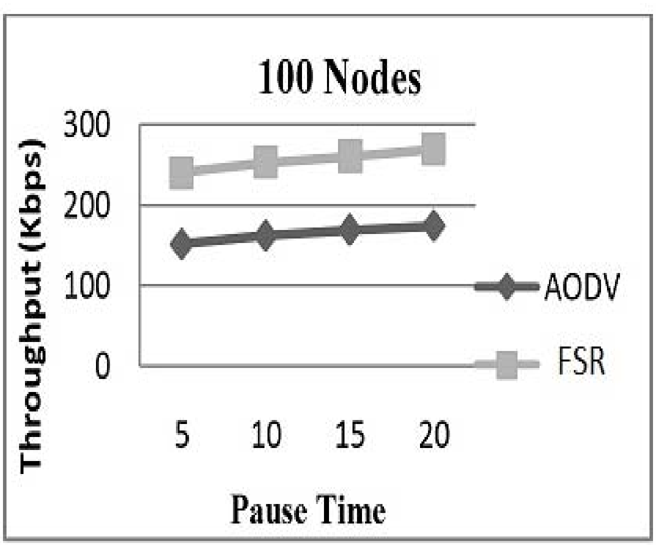


Figure 1(d) : Throughput for 100 Nodes

b) Average End-to-End Delay

The simulation result as indicated in Fig 2(a) and 2 (b) shows that in case of low node density, the average end-to-end delay of AODV is higher than FSR whereas Fig 2(c) and 2(d) indicates that with an increase in node density, AODV outperforms FSR.

It also has been observed that with an increase in pause time there is a decline in the average end-to-end for both the protocols under low node density environment (Fig 2a and 2b). However, this is not true when there is a rise in the network density. The possible reason for such behavior is the presence of more number of nodes between source and destination which effects in increase of hop count thus resulting in increased average end-to-end delay.

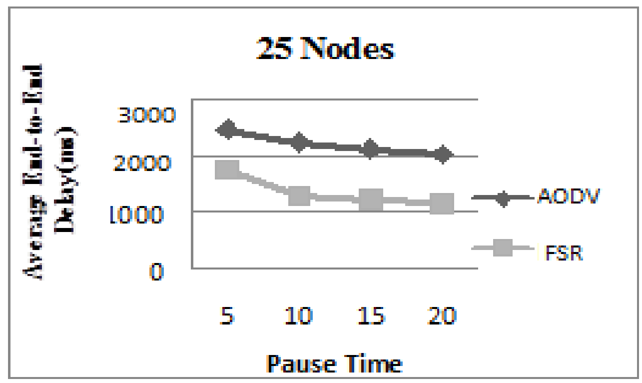


Figure 2(a) : Average End-to-End Delay for 25 Nodes

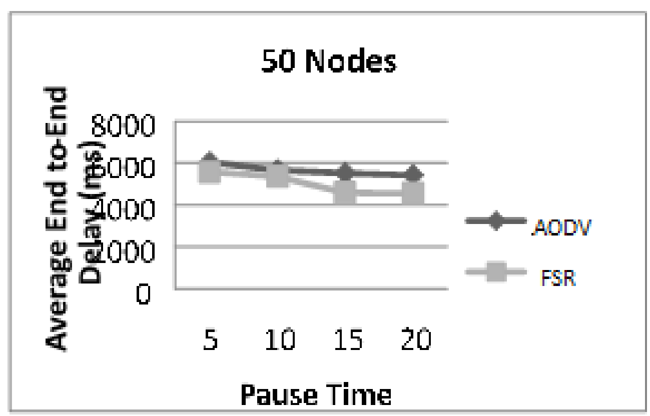


Figure 2(b) : Average End-to-End Delay for 50 Nodes

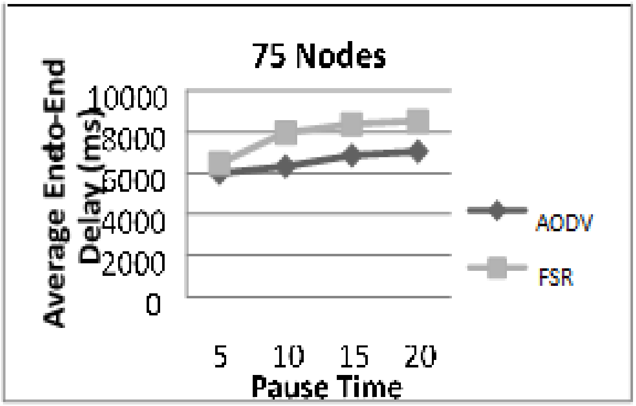


Figure 2(c) : Average End-to-End Delay for 75 Nodes

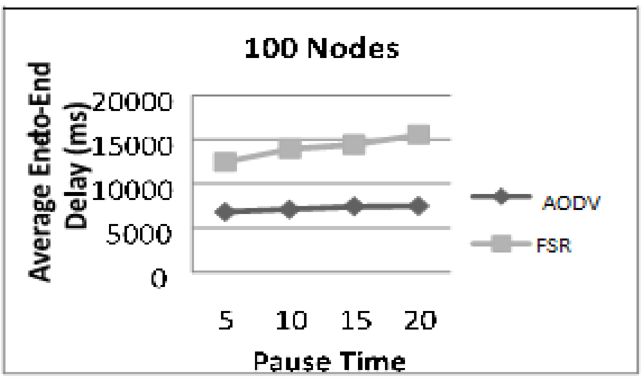


Figure 2(d) : Average End-to-End Delay for 100 Nodes

c) Normalized Routing Load

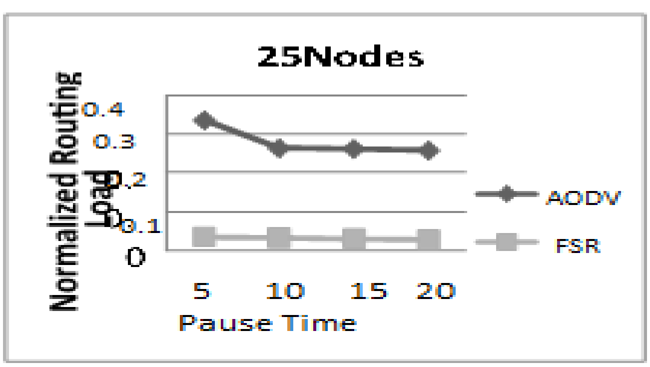


Figure 3(a) : Normalized Routing Load for 25 Nodes

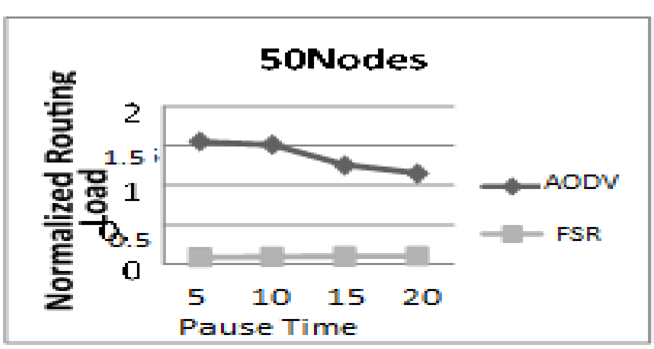


Figure 3(b): Normalized Routing Load for 50 Nodes

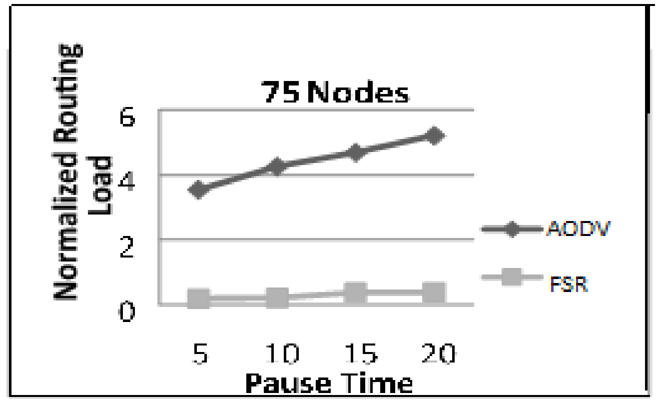


Figure 3(c) : Normalized Routing Load for 75 Nodes

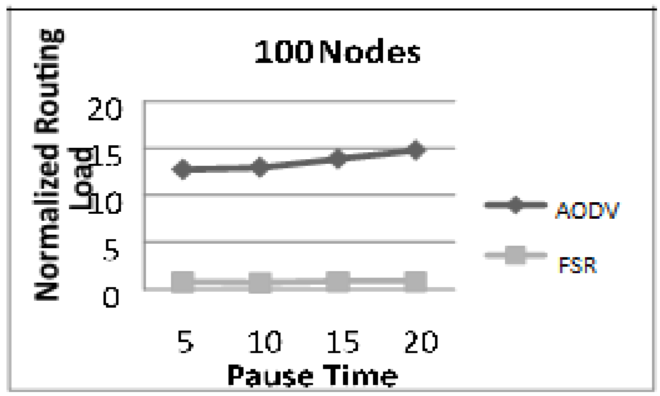


Figure 3(d): Normalized Routing Load for 100 Nodes

Fig 3(a), Fig 3(b), Fig 3(c) and Fig 3(d) indicates that normalized routing load of AODV is always higher than FSR under any scenario. The performance of FSR in terms of normalized routing load is not influenced in any way with respect to change in node density and pause time. The reactive nature of AODV routing protocol causes more number of control overhead than FSR. Therefore, normalized routing load for AODV will always be higher than FSR.

V. Conclusion

The performance evaluation of two routing protocols, AODV and FSR, has been done with respect to metrics viz. throughput, average end-to-end delay and normalized routing load under varying node density and varying pause time. From the result analysis, it has been observed that in high node density the performance of both protocols decreases significantly. The increase of node density in the network causes more number of control packets in the network for route establishment between a pair of source and destination nodes. This is the main reason of performance degradation of the routing protocols in high node density [15]. On other hand, increase of pause time indicates more stable network. Thus the performance of both routing protocols increases with the increment of pause time. It has been observed that in low node density the performance of AODV is better than FSR in terms of throughput, whereas the performance of DSDV is better in high node density (up to 100 nodes). Another observation has been found from the result that increment of pause time does not affect much in the performance of FSR where the performance of AODV varies significantly with the pause time. In Current work, only three performance metrics have been considered to analyze the performance of AODV and FSR. Inclusion of other performance metrics will provide in depth comparison of these two protocols which may provide an insight on the realistic behavior of the protocols under more challenging environment. The current work has been limited with fixed simulation area (500x500m) with CBR traffic and node density is up to 100 nodes. From previous work [15], it has been observed that in higher node density (200 nodes) AODV performs better than FSR. Varying simulation area and higher node density with different traffic will provide in depth performance analysis of these two protocols.

References Références Referencias

1. Siva Ram Murthy C. and Manoj B.S., Ad Hoc Wireless Networks, Architectures and Protocols, Second Edition, Low price Edition, Pearson Education (2007).
2. Mamatha G.S. and Sharma S.C., Analyzing the Manet Variations, Challenges, Capacity and Protocol Issues, International Journal of Computer Science & Engineering Survey (IJCSES), 1(1), (2010).
3. Mehran Abolhasan, Tadeusz Wysocki, and Eryk Dutkiewicz. A review of routing protocols for mobile ad hoc networks. Technical report, Telecommunication and Information Research Institute, University of Wollongong, Wollong, NSW 2522. Motorola Australia Research Centre, 12 Lord st., Botany, NSW 2525, Australia (2003).
4. Xiaoyan Hong, Kaixin Xu, and Mario Gerla, Scalable routing protocols for mobile ad hoc networks (2002).
5. Charles E. Perkins. Ad Hoc Networking, Addison Wesley, 2001
6. Charles E. Perkins, Elizabeth M. Royer, Samir R. Das and Mahesh K. Marina, Performance Comparison of Two On-Demand Routing Protocols for Ad Hoc Networks, IEEE Personal Communications and February 2001.
7. Deepanshu Shukla and Prof. Sridhar Iyer, Mobilty models in Ad Hoc Networks, KReSIT-IIT Bombay, November 2001.
8. Sachin Kumar Gupta and R. K. Saket, Performance Metric Comparison of AODV and DSDV Routing Protocols in MANETs Using NS-2, IJRRAS, June 2011.
9. Guangyu Pei; Gerla, M.; Tsu-Wei Chen; "Fisheye state routing: a routing scheme for ad hoc wireless networks," IEEE International Conference on Communications, 2000.
10. Kevin Fall, Kannan Varadhan, The ns Manual, November 2011.
11. Ramesh, Dr. P. Subbaiah, N. Koteswar Rao and M. Janardhana Raju, Performance Comparison and Analysis of DSDV and AODV for MANET, International Journal on Computer Science and Engineering, 2010.
12. Comer and Douglas E., Computer Networks and Internet, Prentice Hall, 2008.
13. S H Manjula, C N Abhilash, Shaila K, K R Venugopal, and L M Patnaik, Performance of AODV Routing Protocol using Group and Entity Models in Wireless Sensor Networks, IMECS, Hong Kong, March 2008 .
14. C. E. Perkins, E. M. Royar and S. Das, Ad Hoc On Demand Distance Vector (AODV) Routing, IETF Internet Draft, draft-ietf-manet-aodv-08.txt, March 2001.
15. Sanku Sinha and Biswaraj Sen. Performance Analysis of AODV And DSDV Routing Protocols in Mobile Ad Hoc Networks Under Varying Node Density, in the proceedings of international conference RTCMC2012, OITM, Hissar, February 25-26, 2012 pp. 171174.

Global Journal of Computer Science and Technology
Network, Web & Security
Volume 13 Issue 4 Version 1.0 Year 2013
Type: Double Blind Peer Reviewed International Research Journal
Publisher: Global Journals Inc. (USA)
Online ISSN: 0975-4172 & Print ISSN: 0975-4350

Routing Based Ant Colony Optimization in Wireless Sensor Networks

By Anjali & Navpreet Kaur
Lovely Professional University Phagwara, India

Abstract - Wireless Sensor Networks (WSN's) have become an important and challenging issue in last year. Wireless Sensor Networks consist of nodes with limited power are deployed to gather useful information from the field and send the gathered data to the users. In WSNs, it is critical to collect the information in an energy efficient manner. Ant Colony Optimization, a swarm intelligence based optimization technique, is widely used in network routing. In this paper, we introduce a heuristic way to reduce energy consumption in WSNs routing process using Ant Colony Optimization. We introduce three Ant Colony Optimization algorithms, the Ant System, Ant Colony System and improved AS and their application in WSN routing process. The simulation results show that ACO is an effective way to reduce energy consumption and maximize WSN lifetime.

Keywords : ant colony optimization, routing, wireless sensor network.

GJCST-E Classification : C.2.1

ROUTING BASED ANT COLONY OPTIMIZATION IN WIRELESS SENSOR NETWORKS

Strictly as per the compliance and regulations of:

Routing Based Ant Colony Optimization in Wireless Sensor Networks

Anjali [α] & Navpreet Kaur [σ]

Abstract - Wireless Sensor Networks (WSN's) have become an important and challenging issue in last year. Wireless Sensor Networks consist of nodes with limited power are deployed to gather useful information from the field and send the gathered data to the users. In WSNs, it is critical to collect the information in an energy efficient manner. Ant Colony Optimization, a swarm intelligence based optimization technique, is widely used in network routing. In this paper, we introduce a heuristic way to reduce energy consumption in WSNs routing process using Ant Colony Optimization. We introduce three Ant Colony Optimization algorithms, the Ant System, Ant Colony System and improved AS and their application in WSN routing process. The simulation results show that ACO is an effective way to reduce energy consumption and maximize WSN lifetime.

Generalterms : ant colony optimization, delay, energy consumption, routing, routing protocols, sensors, wireless sensor networks.

Keywords : ant colony optimization, routing, wireless sensor network.

I. Introduction

Due to advance information technology, Wireless sensor networks (WSN's) are rapidly developing area in both research and application. The wireless sensor networks are based on the cooperation of a number of tiny sensors and which are depending upon the four parts: sensor (motes), processor, transceiver, and battery. The Sensor get information from surrounding area and processor change the analog information into digital information. Wireless sensors have the ability to perform simple calculations and communicate in a small area. Wireless sensor networks have critical applications in the scientific, medical, commercial, and military domains. Although WSNs are used in many applications, they have several limitations including limited energy supply and limited computation and communication abilities. These limitations should be considered when designing protocols for WSNs.

Author α : Dept. of Electronics and Communication Lovely Professional University Phagwara, India. E-mail : anjalisehgal1988@gmail.com

Author σ : Assistant Professor Lovely Professional University Phagwara, India. E-mail : Navpreet.kaur@lpu.co.in

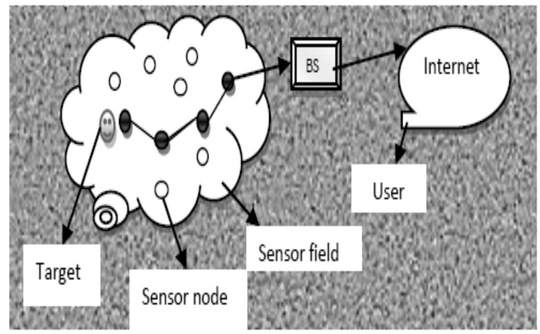


Figure 1 : Wireless Sensor Network

In sensor networks, minimization of energy consumption is considered a major performance criterion to provide maximum network lifetime. When considering energy conservation, routing protocols should also be designed to achieve fault tolerance in communications.

There are two types of WSNs: structured and unstructured. An unstructured WSN is one that contains a dense collection of sensor nodes. The sensor nodes may be deployed in an ad hoc manner into the field. Once deployed, the network is left unattended to perform monitoring and reporting functions. In an unstructured WSN, network maintenance such as connection management and failures detection is difficult since there are so many nodes to take care of. In a structured WSN, all or some of the sensor nodes are deployed in a pre-planned manner. The advantage of a structured network is that fewer nodes can be deployed with lower network maintenance and management cost. Fewer nodes can be deployed now since nodes are placed at specific locations to provide coverage while ad hoc deployment can have uncovered regions.

The basic method to transfer information from a sensor node to the base is called flooding. The optimization of network parameters for WSN routing process to provide maximum service life of the network can be regarded as a combinatorial optimization problem. Many researchers have recently studied the collective behavior of biological species such as ants as an analogy providing a natural model for combinatorial optimization problems. Ants in a colony are able to converge on the shortest among multiple paths connecting their nest and a food source. The driving force behind this behavior is the use of a volatile chemical substance called pheromone. While locating food, ants lay pheromone on the ground, and they also go in the direction where the concentration of pheromone is higher. This mechanism allows them to mark paths and subsequently guide other ants, and let good paths arise from the overall behavior of the colony.

The main goal of our study was to maintain network life time at a maximum, while discovering the shortest paths from the source nodes to the base node using swarm intelligence based optimization technique called ACO. The Ant Colony Optimization (ACO) is a family member of the Swarm Intelligence based approaches applied for optimization problems. A multi-path data transfer is also accomplished to provide reliable network operations, while considering the energy levels of the nodes. Wireless Sensor Network architecture, ACO algorithm for network routing and Simulation Results are presented in the following sections.

II. Overview of Routing Based Ant Algorithm for WSN

a) Ant Colony Optimization

The ant colony optimization algorithm (ACO) is a probabilistic technique for solving computational problems which can be reduced to finding good paths through graphs. This algorithm is a member of the ant colony algorithms family, in swarm intelligence methods, and it constitutes some metheuristic optimizations. Initially proposed by Marco Dorigo in 1992 in his PhD thesis, the first algorithm was aiming to search for an optimal path in a graph, based on the behavior of an ants seeking path between their colony and a source of food. The original idea has since diversified to solve a wider class of numerical problems, and as a result, several problems have emerged, drawing on various aspects of the behavior of ants.

A combinatorial optimization problem is a problem defined over a set C = c1, ... , cn of basic components. A subset S of components represents a solution of the problem; F ⊆ 2C is the subset of feasible solutions, thus a solution S is feasible if and only if S ∈ F. A cost function z is defined over the solution domain, z : 2C □ R, the objective being to find a minimum cost feasible solution S*, i.e., to find S*: S* ∈ F and z(S*) ≤ z(S), ∀S∈F. Given this, the functioning of an ACO algorithm can be summarized as follows:-

A set of computational concurrent and asynchronous agents (a colony of ants) moves through states of the problem corresponding to partial solutions of the problem to solve. They move by applying a stochastic local decision policy based on two parameters, called trails and attractiveness.

By moving, each ant incrementally constructs a solution to the problem. When an ant completes a solution, or during the construction phase, the ant evaluates the solution and modifies the trail value on the components used in its solution. This pheromone information will direct the search of the future ants.

Furthermore, an ACO algorithm includes two more mechanisms: trail evaporation and, optionally, daemon actions. Trail evaporation decreases all trail values over time, in order to avoid unlimited accumulation of trails over some component. Daemon actions can be used to implement centralized actions which cannot be performed by single ants, such as the invocation of a local optimization procedure, or the update of global information to be used to decide whether to bias the search process from a non-local perspective.

More specifically, an ant is a simple computational agent, which iteratively constructs a solution for the instance to solve. Partial problem solutions are seen as states. At the core of the ACO algorithm lies a loop, where at each iteration, each ant moves (performs a step) from a state ι to another one ψ, corresponding to a more complete partial solution. That is, at each step σ, each ant k computes a set Ak σ(ι) of feasible expansions to its current state, and moves to one of these in probability. The probability distribution is specified as follows. For ant k, the probability pιψk of moving from state ι to state ψ depends on the combination of two values:

- The attractiveness ηιψ of the move, as computed by some heuristic indicating the a priori desirability of that move;
- The trail level τιψ of the move, indicating how proficient it has been in the past to make that particular move: it represents therefore an a posteriori indication of the desirability of that move. Trails are updated usually when all ants have completed their solution, increasing or decreasing the level of trails corresponding to moves that were part of "good" or "bad" solutions, respectively.

b) AS (Ant system algorithm)

The first ACO algorithm was called the Ant system [10] and it was aimed to solve the travelling salesman problem, in which the goal is to find the shortest round-trip to link a series of cities. The general algorithm is relatively simple and based on a set of ants, each making one of the possible round-trips along the cities. At each stage, the ant chooses to move from one city to another according to some rules:

1. It must visit each city exactly once;
2. A distant city has less chance of being chosen (the visibility).
3. The more intense the pheromone trail laid out on an edge between two cities, the greater the probability that that edge will be chosen.
4. Having completed its journey, the ant deposits more pheromones on all edges it traversed, if the journey is short.

5. After each iteration, trails of pheromones evaporate.

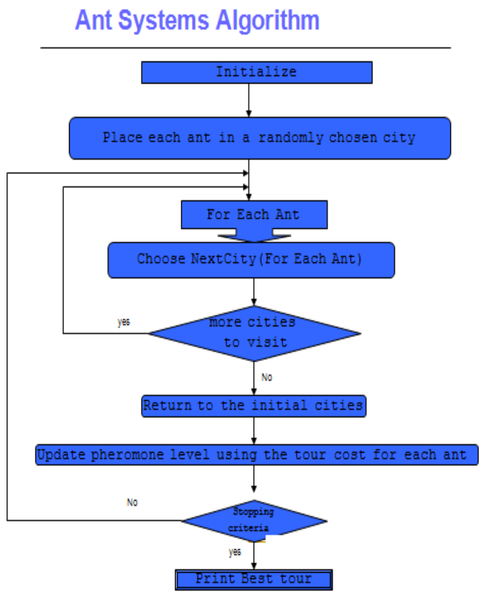


Figure 2 : Ant System Algorithm

c) ACS (Ant Colony System)

ACS was the first algorithm inspired by real ant's behavior. The merit is used to introduce the ACO algorithms and to show the potentiality of using artificial pheromone and artificial ants to drive the search of always better solutions for complex optimization problems. In ACS once all ants have computed their tour (i.e. at the end of each iteration) AS updates the pheromone trail using all the solutions produced by the ant colony. Each edge belonging to one of the computed solutions is modified by an amount of pheromone proportional to its solution value. At the end of this phase the pheromone of the entire system evaporates and the process of construction and update is iterated. On the contrary, in ACS only the best solution computed since the beginning of the computation is used to globally update the pheromone. As was the case in AS, global updating is intended to increase the attractiveness of promising route but ACS mechanism is more effective since it avoids long convergence time by directly concentrate the search in a neighborhoods of the best tour found up to the current iteration of the algorithm.

ANTS algorithm within the ACO frame-work has two mechanisms:

i. *Attractiveness*

The attractiveness of a move can be effectively estimated by means of lower bounds (upper bounds in the case of maximization problems) on the cost of the completion of a partial solution. In fact, if a state ι corresponds to a partial problem solution it is possible to compute a lower bound on the cost of a complete solution containing ι.

ii. *Trail Update*

A good trail updating mechanism avoids stagnation, the undesirable situation in which all ants repeatedly construct the same solutions making any further exploration in the search process impossible. Stagnation derives from an excessive trail level on the moves of one solution, and can be observed in advanced phases of the search process, if parameters are not well tuned to the problem. The trail updating procedure evaluates each solution against the last k solutions globally constructed by ANTS. As soon as k solutions are available, their moving average z is computed; each new solution z is compared with z. If z is lower than z, the trail level of the last solution's moves is increased, otherwise it is decreased.

$$\Delta\tau i,j = \tau 0 \ . \ (1 - z\ curr - LB/z - LB)$$

Where z is the average of the last k solutions and LB is a lower bound on the optimal problem solution cost.

III. ACO Approach

In the ACO based approach, each ant tries to find a path in the network, providing minimum cost. Ants are launched from a source node *s* and move through neighbor repeater nodes r_i, and reach a final destination node (sink) *d*. Whenever, a node has data to be transferred to the destination which is described as a base or base station, launching of the ants is performed. After launching, the choice of the next node *r* is made according to a probabilistic decision rule (1):

$$P_k(r,s)=\begin{cases} \dfrac{[\tau(r,s)]^{\alpha}\cdot[\eta(r,s)]^{\beta}}{\sum_{r\in R_s}[\tau(r,s)]^{\alpha}\cdot[\eta(r,s)]^{\beta}} & \text{if } k \notin tabu^r \\ 0 & \text{otherwise} \end{cases} \qquad (1)$$

Where τ (r,s) is the pheromone value, n (r,s) is the value of the heuristic related to energy, R_s is the receiver nodes. For node *r*, *tabu* ^{r} is the list of identities of received data packages previously. α and β are two parameters that control the relative weight of the pheromone trail and heuristic value. Pheromone trails are connected to arcs. Each *arc*(*r,s*) has a trail value. τ (r,s) ∈ lsqb;0,1rsqb; Since the destination *d* is a stable base station, the last node of the path is the same for each ant travel. The heuristic value of the node *r* is expressed by equation (2):

$$\eta(r, s)=\frac{(I-e_r)^{-1}}{\sum_{n\in R_s}(I-e_n)^{-1}} \tag{2}$$

Where I is the initial energy, and e_r is the current energy level of receiver node r. This enables decision making according to neighbor nodes' energy levels, meaning that if a node has a lower energy source then it has lower probability to be chosen. Nodes inform their neighbors about their energy levels when they sense any change in their energy levels.

In traditional ACO, a special memory named M_k is held in the memory of an ant to retain the places visited by that ant (which represent nodes in WSNs). In equation (1), the identities of ants (as sequence numbers) that visited the node previously, are kept in the node's memories, instead of keeping node identities in ant's memories, so there is no need to carry M_k lists in packets during transmission. This approach decreases the size of the data to be transmitted and saves energy.

In equation (1) each receiver node decides whether to accept the upcoming packet of ant k or not, by checking its tabu list. So, the receiver node r has a choice about completing the receiving process by listening and buffering the entire packet. If the receiver node has received the packet earlier, it informs the transmitter node by issuing an ignore message, and switches itself to idle mode until a new packet arrives.

After all ants have completed their tour, each ant k deposits a quantity of pheromone $\Delta\tau^k(t)$ given in equation (3), where $J^k_w(t)$ is the length of tour, $w^k(t)$ which is done by ant k at iteration t. The amount of pheromone at each connection ($(l(r,s)$)of the nodes is given in equation (4). In WSNs, $J^k_w(t)$ represents the total number of nodes visited by ant k of tour w at iteration t:

$$\Delta\tau^k(t)=1/J^k_w(t) \tag{3}$$

$$\tau(r, s)(t) \leftarrow \tau(r, s)(t)+ \Delta\tau(r, s)(t), \forall\, l(r, s) \in wk(t), k = 1, , m \tag{4}$$

Pheromone values are stored in a node's memory. Each node has information about the amount of pheromone on the paths to their neighbor nodes. After each tour, an amount of pheromone trail $\Delta\tau^k$ is added to the path visited by ant k. This amount is the same for each arc(r, s) visited on this path. This task is performed by sending ant k back to its source node from the base along the same path, while transferring an acknowledgement signal for the associated data package. Increasing pheromone amounts on the paths according to lengths of tours, $J_w(t)$ would continuously cause an increasing positive feedback. In order to control the operation, a negative feedback, the operation of pheromone evaporation after the tour is also accomplished in equation (5). A control coefficient $\rho \in (0, 1)$ is used to determine the weight of evaporation for each tour [19]:

$$\tau ij(t) \leftarrow (1-\rho)\tau ij(t \tag{5}$$

In simulations, ACO parameter settings are set to values 2 for α, 6 for β, and 0.5 for ρ, which were experimentally found to be good by Dorigo [20].

IV. Simulation

In this section, we present the performance results of the simulation experiments. To accomplish the experiments, a parallel discrete event-based platform was developed in MATLAB. The fig. 2. are represent sensor node are randomly deploy in the network and connect with each other. Fig. 3 represent the node are randomly deployed and node are in range of each other. The nodes are connected within radius of each other.

The figure 4. Represent all the node is communicating in range of each other and data can be transfer in small area. The fig. 5 represents ant movement in network to find optimize path. All Sensor node are communicating bidirectional and data can be transfer through ants.

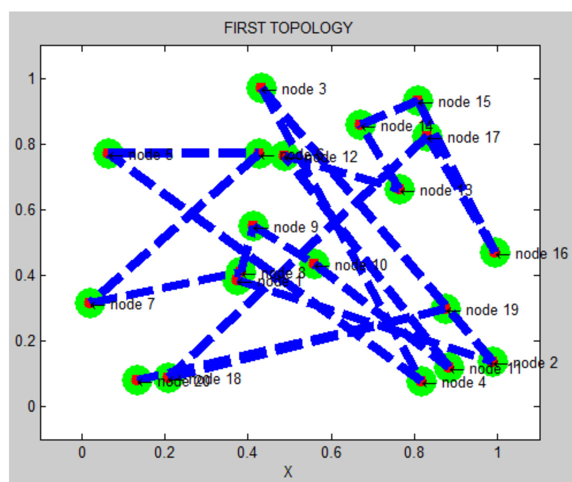


Figure 3 : Node are deploy randomly

Global Journal of Computer Science and Technology (E) Volume XIII Issue IV Version I Year 2013

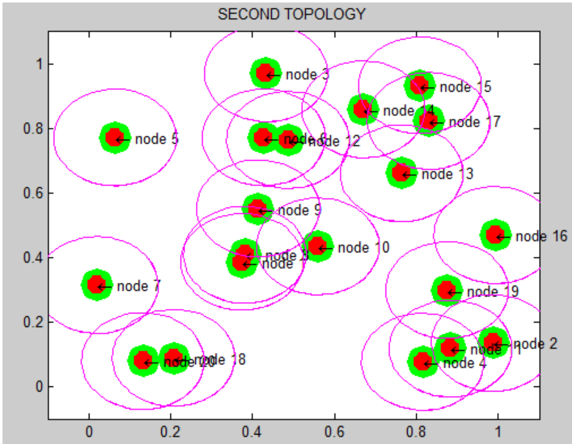


Figure 3 : All sensor node are in range of each other

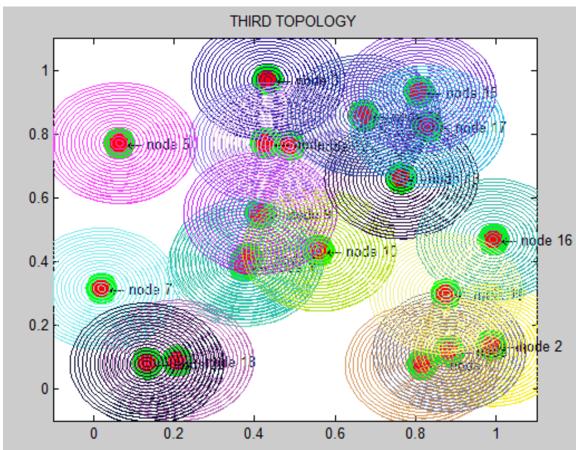


Figure 4 : All node are communicating in range of each other

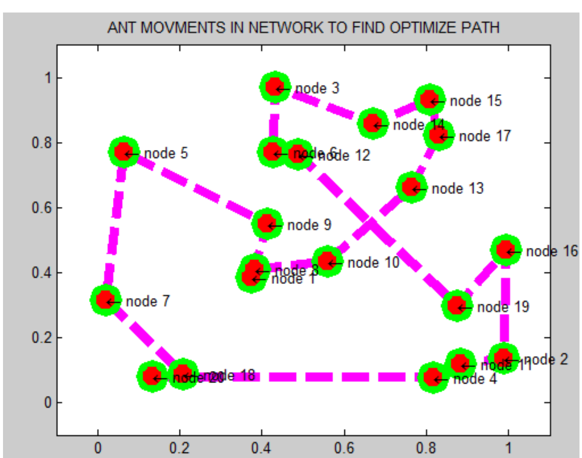


Figure 5 : Ant movement in network to find optimize path

V. Conclusion

In this paper, Ant Colony Optimization based routing algorithm was implemented. In WSN, the life time network is depended essentially to the density and the rate of communications of sensors which affect the battery level and so the network. We act on the routing level and present a new routing algorithm, which uses ant colony optimization algorithm for WSNs. This solution improves actively the life time network of the WSN. The next work will be focused on the mobility context of sensors witch considered as a huge challenge in WSN area with energy consumption metric.

Acknowledgement

The authors also would like to thank the anonymous reviewers for their comments and suggestions to improve this paper. The authors also would like to thanks my friends.

References Références Referencias

1. J.-Y. Heo, J.-M.Hong, and Y.-K. Cho, “EARQ: Energy aware routing for real-time and reliable communication in wireless industrial sensor networks,” IEEE Trans. Ind. Informat, vol. 5, no. 1, pp. 3–11, Feb. 2009.
2. Marco Dorigo, Mauro Bimttari, and Thomas, "Ant Colony Optimization Artificial Ants as a Computational Intelligence Technique", IRIDIA – TECHNICAL REPORT SERIES: TRIIRIDIAI2006-023.
3. Camara, D.; Loureiro, AAF, "A novel routing algorithm for ad hoc networks", System Sciences, 2000.
4. M.Golshahi, M.Mosleh, M.Kheyrandish, "Implementing An ACO Routing Algorithm For AD-HOC Networlcs," IEEE, International Conference on Advanced Computer Theory and Engineering, 2008.
5. Gianni Di Caro, Frederick Ducatelle and Luca Maria Gambardella, "SWARM INTELLIGENCE FOR ROUTING IN MOBILE AD HOC ETWORKS" 2005 IEEE.
6. Bonabeau E., Dorigo M. Natural to Artificial Systems. Oxford Univ. Press; London, U.K.: 1999. G.T. Swarm Intelligence; pp. 1–278.
7. White T., Pagurek B. Toward Multi-Swarm Problem Solving in Networks. International Conference on Multi Agent Systems. 1998:333–340.

This page is intentionally left blank

Global Journal of Computer Science and Technology
Network, Web & Security
Volume 13 Issue 4 Version 1.0 Year 2013
Type: Double Blind Peer Reviewed International Research Journal
Publisher: Global Journals Inc. (USA)
Online ISSN: 0975-4172 & Print ISSN: 0975-4350

Fast and Secure Routing Protocol in Manet

By Vivek Anand Singh & Vineet Yadav
Shri Ramswaroop Memorial College, India

Abstract - This paper proposes an enhanced mobile ad-hoc routing protocol FSR (Fast and Secure Routing), which is enhanced version of best features of ZBR (Zone Based routing Protocol). FSR deals with speed and security both at the same time. The ZBR enhances the speed of the network whether TCP has provided the primary means to transfer data reliably across the Internet. Modern networks routinely drop packets when the load temporarily exceeds their buffering capacities. Early detection protocols have tried to address this problem with a user-defined threshold, the finding of detecting and removing compromised routers can be thought of as an instance of anomalous behaviour based intrusion detection. That can be the compromised router can that identified by correct routers when it deviates from exhibiting expected behaviour. This protocol can be evaluated in a small experimental network.

Keywords : *MANET, BGP (broader gateway protocol), ZBR (zone based routing), TCP, protocol X, TV (traffic validation).*

GJCST-E Classification : *C.2.5*

FAST AND SECURE ROUTING PROTOCOL IN MANET

Strictly as per the compliance and regulations of:

Fast and Secure Routing Protocol in Manet

Vivek Anand Singh [α] & Vineet Yadav [σ]

Abstract - This paper proposes an enhanced mobile ad-hoc routing protocol FSR (Fast and Secure Routing), which is enhanced version of best features of ZBR (Zone Based routing Protocol). FSR deals with speed and security both at the same time. The ZBR enhances the speed of the network whether TCP has provided the primary means to transfer data reliably across the Internet. Modern networks routinely drop packets when the load temporarily exceeds their buffering capacities. Early detection protocols have tried to address this problem with a user-defined threshold, the finding of detecting and removing compromised routers can be thought of as an instance of anomalous behaviour based intrusion detection. That can be the compromised router can that identified by correct routers when it deviates from exhibiting expected behaviour. This protocol can be evaluated in a small experimental network.

Keywords : MANET, BGP (broader gateway protocol), ZBR (zone based routing), TCP, protocol X, TV (traffic validation).

I. Introduction

Active research work for MANETs is carrying on mainly in the fields of Medium Access Control (MAC), routing, resource management, power control, and security. Because of the importance of routing protocols in dynamic multi-hop networks, a lot of MANET routing protocols have been proposed in the last few years. Considering the special properties of MANET, when thinking about any routing protocol, generally the following properties are expected, though all of these might not be possible to incorporate in a single solution.

- A routing protocol for MANET should be distributed in manner in order to increase its reliability.
- The routing protocol should consider its security.
- A hybrid routing protocol should be much more reactive than proactive to avoid overhead.
- A hybrid routing protocol should be much more reactive than proactive to avoid overhead.
- A routing protocol must be designed considering unidirectional links because wireless medium may cause a wireless link to be opened in one direction only due to physical factors.
- A routing protocol should be aware of Quality of Service.
- The routing protocol should be power-efficient.

Author α σ : Shri Ramswaroop Memorial College of Engineering and Management, Uttar Pradesh, India. E-mails : vcyrus90@gmail.com, vineetabhiraaj@gmail.com

II. Previous and Related Work

Previous work on TCP and ZBR is as follows-

ZBR - ZBR combines the proactive and reactive routing approaches. It divides the network into routing zones. The routing zone of a node X includes all nodes within hop distance at most d from node X. All nodes at hop distance exactly d are said to be the peripheral nodes of node X's routing zone. The parameter d is the zone radius. ZBR proactively maintains the routes within the routing zones and reactively searches for routes to destinations beyond a node's routing zone. Route discovery is similar to that in DSR with the difference that route requests are propagated only via peripheral nodes. ZBR can be dynamically configured to a particular network through adjustment of the parameter d. ZBR will be a purely reactive routing protocol when d = 0 and a purely proactive routing protocol when d is set to the diameter of the network. ZBR discovers routes as follows. When a source node wants to send data to a destination, it first checks whether or not the destination is within its routing zone. If it is, then a route can be obtained directly. Otherwise, it floods a route request to its peripheral nodes. The peripheral nodes in turn execute the same algorithm to check whether the destination is within their routing zone. If it is, a route reply message is sent back to the source. Otherwise, the peripheral node floods the route request to its peripheral nodes again. This procedure is repeated until a route is found.

TCP-TCP is used for transmission services in ZBR which has provided the primary means to transfer data reliably across the Internet; however TCP has imposed limitation on several applications. Measurement and estimation of packet loss characteristics are challenging due to the relatively rare occurrence and typically short duration of packet loss episodes. While active probe tools are commonly used to measure packet loss on end-to end paths, there has been little analysis of the accuracy of these tools or their impact on the network. The main objective is to understand the problem of detecting whether a compromised router is maliciously manipulating its stream of packets. In particular to this concern a simple yet effective attack in which a router selectively drops packets destined for some Victim. Unfortunately, it is quite challenging to attribute a missing packet to a malicious action because normal network congestion can produce the same effect .Such attacks are not mere theoretical curiosities, but they are actively employed in practice. Attackers have repeatedly demonstrated their ability to compromise routers, through combinations of social engineering and exploitation of weak passwords and latent software vulnerabilities. One network operator recently documented Over 5,000 compromised routers as well as an underground market for trading Access to them several researchers has developed.

III. Proposed Protocol Technique

Our project`s main objective is to remove the vulnerability in the ad-hoc network due to compromised routers and reducing delay generated due to route discovery. The FSR (Fast and Secure Routing) protocol is Combination of best features of TCP and ZBR which results in very efficient and secure network configuration. Since there is no central node in ad-hoc network in other words all nodes are mobile. Routing zone is determined by setting a zone radius (represented by parameter d) from a certain node. Peripheral nodes from that node form a routing zone.

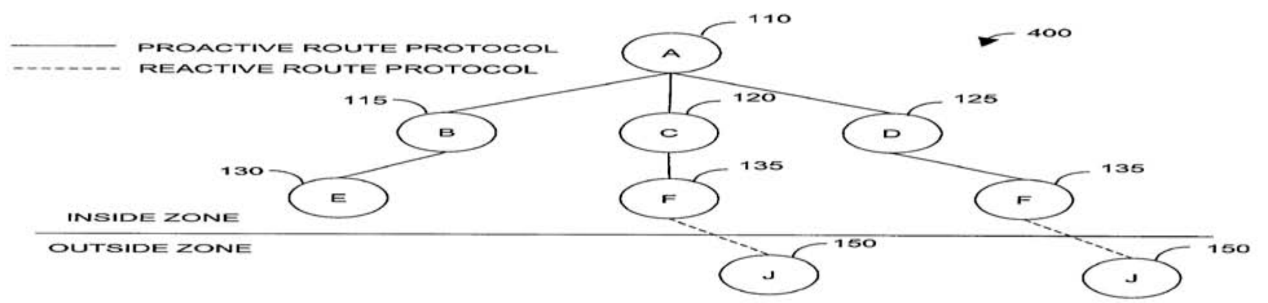


Figure 1 : Working of proactive and reactive routing protocol

The FSR works on algorithm which comprises of three modes and switches between first mode and second mode according to network demand which is implementation of ZBR. Third mode is always applicable. Functions of these three modes are as follows:

- In first mode, the FSR proactively maintains the route within the routing zone.
- In Second mode, FSR reactively searches for routes to destinations beyond a node's routing zone. Dynamic configuration of FSR is possible as it inherits ZBR features.
- In the Third mode, we set a deterministic behaviour for all routers in all routing zones by using TCP security policies and if any router deviates from this behaviour that is considered to be malicious. All packets incoming from malicious router will be dropped and another interface from that zone will be selected for communication. This action will prevent any loss of packets in network.

The concept discussed above can be implemented using "protocol X" and ZBR. Considering this scenario if any router will be compromised by the attacker that will be automatically identified and blocked in the network. In other scenario if there will be any increase in network traffic that will be managed by ZBR configuration and hence result in great reduction in network overhead and delay of packets. So, this is how we can implement a fast and secure routing.

a) MODE 1- Maintaining routes proactively

In order to maintain correct route information proactively, a node must periodically send control messages. Therefore, proactive routing protocols may waste bandwidth since control messages are sent out unnecessarily when there is no data traffic. The main advantage of this category of protocols is that hosts can quickly obtain route information and quickly establish a session.

For Example: GSR introduced below is a proactive routing protocol.

Global State Routing (GSR) is based on the Link State (LS) routing method. In the LS routing method, each node floods the link state information into the whole network (global flooding) once it realises that links change between itself and its neighbours. The link state information includes the delay to each of its neighbours. A node will know the whole topology when it obtains all link information. LS routing works well in networks with static topologies. When links change quickly, however, frequent global flooding will inevitably lead to huge control overhead. Unlike the traditional LS method, GSR does not flood the link state packets. Instead, every node maintains the link state table based on up-to-date LS information received from neighbouring nodes, and periodically exchanges its LS information with its neighbours only (no global flooding). Before sending an LS packet, a node assigns the LS packet a unique sequence number to identify the newest LS information. LS information is disseminated as the LS packets with larger sequence numbers replace the ones with smaller sequence numbers.

The convergence time required to detect a link change in GSR is shorter than in the Distributed Bellman-Ford (DBF) protocol. The convergence time in GSR is O(D*I) where D is the diameter of the network and I is the link state update interval. The convergence time is normally smaller than O(N*I) in DBF, where N is the number of nodes in the networks and I is the update interval. Since the global topology is maintained in every node, preventing routing loops is simple and easy.

The drawbacks of GSR are the large size of the update messages, which consume a considerable amount of bandwidth, and the latency of the LS information propagation, which depends on the LS information update interval time. ``Fisheye" technology can be used to reduce the size of update messages. In this case, every node maintains highly accurate network information about the immediate neighbouring nodes, with progressively fewer details about farther nodes.

b) MODE 2- Searching routes to destination reactively

Reactive routing protocols can dramatically reduce routing overhead because they do not need to search for and maintain the routes on which there is no data traffic. This property is very appealing in the resource-limited environment.

i. *Ad hoc On-Demand Distance Vector (AODV) Routing*

Since DSR includes the entire route information in the data packet header, it may waste bandwidth and degrade performance, especially when the data contents in a packet are small. Ad hoc On-Demand Distance Vector (AODV) Routing tries to improve performance by keeping the routing information in each node. The main difference between AODV and DSR is that DSR uses source routing while AODV uses forwarding tables at each node. In AODV, the route is calculated hop by hop. Therefore, the data packet need not include the total path.

The route discovery mechanism in AODV is very similar to that in DSR. In AODV, any node will establish a reverse path pointing toward the source when it receives an RREQ packet. When the desired destination or an intermediate node has a fresh route (based on the destination sequence number) to the destination, the destination/intermediate node responds by sending a route reply (RREP) packet back to the source node using the reverse path established when the RREQ was forwarded. When a node receives the RREP, it establishes a forward path pointing to the destination. The path from the source to the destination is established when the source receives the RREP.

For example: Dealing with path failures in AODV is more complicated than in DSR. When a node detects the link failure to its next hop, it propagates a link failure notification message (an RREP with a very large hop count value to the destination) to each of its active upstream neighbours to inform them to erase that part of the route. These nodes in turn propagate the link failure notification message to their upstream neighbours, and so on, until the source node is reached. A neighbour is considered active for a route entry if the neighbour sends a packet, which was forwarded using that entry, within the active-route-timeout interval. Note that the link failure notification message will also update the destination sequence number. When the source node receives the link failure notification message, it will re-initiate a route discovery for the destination if a route is still needed. A new destination sequence number is used to prevent routing loops formed by the entangling of stale and newly established paths.

AODV saves bandwidth and performs well in a large MANET since a data packet does not carry the whole path information. As in DSR, the response time may be large if the source node's routing table has no entry to the destination and thus must discover a path before message transmission. Furthermore, the same problems exist as in DSR when network partitions occur.

c) MODE 3- Securing network

i. *Protocol X*

The Protocol x detects traffic faulty routers by validating the queue of each output interface for each router. Given the buffer size and the rate at which traffic enters and exits a queue, the behaviour of the queue is deterministic. If the actual behaviour deviates from the predicted behaviour, then a failure has occurred. We present the failure detection protocol in terms of the solutions of the distinct sub-problems: traffic validation, distributed detection, response, and the correctness of the protocol.

ii. *Traffic Validation Correctness*

The Traffic validation of the failure of detecting malicious attack by TV results in a false negative, and any misdetection of legitimate behaviour by TV results in a false positive. Within the given system model of Section the example TV predicate is correct. However, the system model is still simplistic. In a real router, packets may be legitimately dropped due to reasons other than congestion errors in hardware, software or memory, and transient link errors. Classifying these as arising from a router being compromised might be a problem, especially if they are infrequent enough that they would be best ignored rather than warranting repairs the router or link. A larger concern is the simple way that a router is modelled in how it internally multiplexes packets. This model is used to compute time stamps. If the time stamps are incorrect, then TV could decide incorrectly. We hypothesize that a sufficiently accurate timing model of a router is attainable but have yet to show this to be the case. A third concern is with clock synchronization. This version of TV requires that all the routers feeding a queue have synchronized clocks. This requirement is needed in order to ensure that the packets are interleaved correctly by the model of the router. The synchronization requirement is not necessarily daunting; the tight synchronization is only required by routers adjacent to the same router. With low-level time stamping of packets and repeated exchanges of time it should be straightforward to synchronize the clocks sufficiently tightly. Other representations of collected traffic information and TV that we have considered has their own problems with false positives and false negatives. It is an open question as to the best way to represent TV. We suspect any representation will admit some false positives or false negatives.

IV. Conclusion

In this paper, we propose an adaptive algorithm which adapts itself according to network demand by maintaining balance between zones based routing (ZBR) and transmission control protocol (TCP). Routes are maintained proactively in routing zone and Route discovery is done using reactive protocol. While faulty routers are detected by using protocol x by setting a constant buffer size and deterministic behaviour of queue at which traffic enters and exits. Proactive routing is done using global state routing (GSR) which is based on the Link State (LS) routing method. The link state information includes the delay to each of its neighbours. A node will know the whole topology when it obtains all link information. While reactive routing is done using Ad-hoc on demand Vector (AODV) routing. Ad hoc On-Demand Distance Vector (AODV) Routing tries to improve performance by keeping the routing information in each node. AODV saves bandwidth and performs well in a large MANET since a data packet does not carry the whole path information. Thus the overall algorithm brings efficiency and reliability in MANET.

References Références Referencias

1. Perkins CE, Bhagwat P (1994) Highly Dynamic Destination-Sequenced Distance-Vector Routing (DSDV) for Mobile Computers. Proceedings of ACM SIGCOMM 1994: 234–244.
2. Cheng C, Riley R, Kumar SPR, Garcia-Luna-Aceves JJ (1989). A Loop-Free Extended Bellman-Ford Routing Protocol Without Bouncing Effect. ACM SIGCOMM Computer Communications Review, Volume 19, Issue 4: 224–236.
3. Murthy S, Garcia-Luna-Aceves JJ (1996). An Efficient Routing Protocol for Wireless Networks. Mobile Networks and Applications, Volume 1, Issue 2:183–197 ISSN: 0975-3397 711 G. Vijaya Kumar et. al. / (IJCSE) International Journal on Computer Science and Engineering Vol. 02, No. 03, 2010, 706-713.
4. Humblet PA (1991) another Adaptive Distributed Shortest-Path Algorithm. IEEE Transactions on Communications, Volume 39, Issue 6: 995–1003.
5. Rajagopalan B, Faiman M (1991). A Responsive Distributed Shortest-Path Routing Algorithm With in Autonomous Systems. Journal of Internetworking Research and Experiment, Volume 2, Issu.
6. R. Thomas, ISP Security BOF, NANOG 28, http://www.nanog org/mtg-0306/pdf/thomas.pdf, June 2003.
7. K.A. Bradley, S. Cheung, N. Puketza, B. Mukherjee, and R.A. Ols- son, “Detecting Disruptive Routers: A Distributed Network Monitoring Approach,” Proc. IEEE Symp. Security and Privacy (S&P ’98), pp. 115-124, May 1998.
8. A.T. Mizrak, Y.-C. Cheng, K. Marzullo, and S. Savage, “Detecting and Isolating Malicious Routers,” IEEE Trans. Dependable and Secure Computing, vol. 3, no. 3, pp. 230-244, July-Sept. 2006.
9. L. Subramanian, V. Roth, I. Stoica, S. Shenker, and R. Katz, “Listen and Whisper: Security Mechanisms for BGP,” Proc. First Symp. Networked Systems Design and Implementation (NSDI ’04), Mar. 2004.
10. S. Kent, C. Lynn, J. Mikkelson, and K. Seo, “Secure Border Gate- way Protocol (Secure-BGP),” IEEE J. Selected Areas in Comm., vol. 18, no. 4, pp. 582-592, Apr. 2000.
11. Y.-C. Hu, A. Perrig, and D.B. Johnson, “Ariadne: A Secure On- Demand Routing Protocol for Ad Hoc Networks,” Proc. ACM MobiCom’ 02, Sept. 2002.
12. B.R. Smith and J. Garcia-Luna-Aceves, “Securing the Border Gate- way Routing Protocol,” Proc. IEEE Global Internet, Nov. 1996.
13. S. Cheung, “An Efficient Message Authentication Scheme for Link State Routing,” Proc. 13th Ann. Computer Security Applications Conf. (ACSAC ’97), pp. 90-98, 1997.
14. M.T. Goodrich, Efficient and Secure Network Routing Algorithms, provisional patent filing, Jan. 2001.
15. R. Perlman, “Network Layer Protocols with Byzantine Robust-ness,” PhD dissertation, MIT LCS TR-429, Oct. 1988.

Global Journals Inc. (US) Guidelines Handbook 2013

www.GlobalJournals.org

FELLOW OF ASSOCIATION OF RESEARCH SOCIETY IN COMPUTING (FARSC)

- 'FARSC' title will be awarded to the person after approval of Editor-in-Chief and Editorial Board. The title 'FARSC" can be added to name in the following manner. eg. **Dr. John E. Hall, Ph.D., FARSC or William Walldroff Ph. D., M.S., FARSC**
- Being FARSC is a respectful honor. It authenticates your research activities. After becoming FARSC, you can use 'FARSC' title as you use your degree in suffix of your name. This will definitely will enhance and add up your name. You can use it on your Career Counseling Materials/CV/Resume/Visiting Card/Name Plate etc.
- 60% Discount will be provided to FARSC members for publishing research papers in Global Journals Inc., if our Editorial Board and Peer Reviewers accept the paper. For the life time, if you are author/co-author of any paper bill sent to you will automatically be discounted one by 60%
- FARSC will be given a renowned, secure, free professional email address with 100 GB of space eg.johnhall@globaljournals.org. You will be facilitated with Webmail, Spam Assassin, Email Forwarders, Auto-Responders, Email Delivery Route tracing, etc.
- FARSC member is eligible to become paid peer reviewer at Global Journals Inc. to earn up to 15% of realized author charges taken from author of respective paper. After reviewing 5 or more papers you can request to transfer the amount to your bank account or to your PayPal account.
- Eg. If we had taken 420 USD from author, we can send 63 USD to your account.
- FARSC member can apply for free approval, grading and certification of some of their Educational and Institutional Degrees from Global Journals Inc. (US) and Open Association of Research, Society U.S.A.
- After you are FARSC. You can send us scanned copy of all of your documents. We will verify, grade and certify them within a month. It will be based on your academic records, quality of research papers published by you, and 50 more criteria. This is beneficial for your job interviews as recruiting organization need not just rely on you for authenticity and your unknown qualities, you would have authentic ranks of all of your documents. Our scale is unique worldwide.
- FARSC member can proceed to get benefits of free research podcasting in Global Research Radio with their research documents, slides and online movies.
- After your publication anywhere in the world, you can upload you research paper with your recorded voice or you can use our professional RJs to record your paper their voice. We can also stream your conference videos and display your slides online.
- FARSC will be eligible for free application of Standardization of their Researches by Open Scientific Standards. Standardization is next step and level after publishing in a journal. A team of research and professional will work with you to take your research to its next level, which is worldwide open standardization.

- FARSC is eligible to earn from their researches: While publishing his paper with Global Journals Inc. (US), FARSC can decide whether he/she would like to publish his/her research in closed manner. When readers will buy that individual research paper for reading, 80% of its earning by Global Journals Inc. (US) will be transferred to FARSC member's bank account after certain threshold balance. There is no time limit for collection. FARSC member can decide its price and we can help in decision.

MEMBER OF ASSOCIATION OF RESEARCH SOCIETY IN COMPUTING (MARSC)

- 'MARSC' title will be awarded to the person after approval of Editor-in-Chief and Editorial Board. The title 'MARSC" can be added to name in the following manner. eg. Dr. John E. Hall, Ph.D., MARSC or William Walldroff Ph. D., M.S., MARSC
- Being MARSC is a respectful honor. It authenticates your research activities. After becoming MARSC, you can use 'MARSC' title as you use your degree in suffix of your name. This will definitely will enhance and add up your name. You can use it on your Career Counseling Materials/CV/Resume/Visiting Card/Name Plate etc.
- 40% Discount will be provided to MARSC members for publishing research papers in Global Journals Inc., if our Editorial Board and Peer Reviewers accept the paper. For the life time, if you are author/co-author of any paper bill sent to you will automatically be discounted one by 60%
- MARSC will be given a renowned, secure, free professional email address with 30 GB of space eg.johnhall@globaljournals.org. You will be facilitated with Webmail, Spam Assassin, Email Forwarders, Auto-Responders, Email Delivery Route tracing, etc.
- MARSC member is eligible to become paid peer reviewer at Global Journals Inc. to earn up to 10% of realized author charges taken from author of respective paper. After reviewing 5 or more papers you can request to transfer the amount to your bank account or to your PayPal account.
- MARSC member can apply for free approval, grading and certification of some of their Educational and Institutional Degrees from Global Journals Inc. (US) and Open Association of Research, Society U.S.A.
- MARSC is eligible to earn from their researches: While publishing his paper with Global Journals Inc. (US), MARSC can decide whether he/she would like to publish his/her research in closed manner. When readers will buy that individual research paper for reading, 40% of its earning by Global Journals Inc. (US) will be transferred to MARSC member's bank account after certain threshold balance. There is no time limit for collection. MARSC member can decide its price and we can help in decision.

ANNUAL MEMBER

- Annual Member will be authorized to receive e-Journal GJCST for one year (subscription for one year).
- The member will be allotted free 1 GB Web-space along with subDomain to contribute and participate in our activities.
- A professional email address will be allotted free 500 MB email space.

PAPER PUBLICATION

- The members can publish paper once. The paper will be sent to two-peer reviewer. The paper will be published after the acceptance of peer reviewers and Editorial Board.

Process of submission of Research Paper

The Area or field of specialization may or may not be of any category as mentioned in 'Scope of Journal' menu of the GlobalJournals.org website. There are 37 Research Journal categorized with Six parental Journals GJCST, GJMR, GJRE, GJMBR, GJSFR, GJHSS. For Authors should prefer the mentioned categories. There are three widely used systems UDC, DDC and LCC. The details are available as 'Knowledge Abstract' at Home page. The major advantage of this coding is that, the research work will be exposed to and shared with all over the world as we are being abstracted and indexed worldwide.

The paper should be in proper format. The format can be downloaded from first page of 'Author Guideline' Menu. The Author is expected to follow the general rules as mentioned in this menu. The paper should be written in MS-Word Format (*.DOC,*.DOCX).

The Author can submit the paper either online or offline. The authors should prefer online submission.Online Submission: There are three ways to submit your paper:

(A) (I) First, register yourself using top right corner of Home page then Login. If you are already registered, then login using your username and password.

(II) Choose corresponding Journal.

(III) Click 'Submit Manuscript'. Fill required information and Upload the paper.

(B) If you are using Internet Explorer, then Direct Submission through Homepage is also available.

(C) If these two are not convenient, and then email the paper directly to dean@globaljournals.org.

Offline Submission: Author can send the typed form of paper by Post. However, online submission should be preferred.

MANUSCRIPT STYLE INSTRUCTION **<u>(Must be strictly followed)</u>**

Page Size: 8.27" X 11'"

- Left Margin: 0.65
- Right Margin: 0.65
- Top Margin: 0.75
- Bottom Margin: 0.75
- Font type of all text should be Swis 721 Lt BT.
- Paper Title should be of Font Size 24 with one Column section.
- Author Name in Font Size of 11 with one column as of Title.
- Abstract Font size of 9 Bold, “Abstract” word in Italic Bold.
- Main Text: Font size 10 with justified two columns section
- Two Column with Equal Column with of 3.38 and Gaping of .2
- First Character must be three lines Drop capped.
- Paragraph before Spacing of 1 pt and After of 0 pt.
- Line Spacing of 1 pt
- Large Images must be in One Column
- Numbering of First Main Headings (Heading 1) must be in Roman Letters, Capital Letter, and Font Size of 10.
- Numbering of Second Main Headings (Heading 2) must be in Alphabets, Italic, and Font Size of 10.

You can use your own standard format also.
Author Guidelines:

1. General,

2. Ethical Guidelines,

3. Submission of Manuscripts,

4. Manuscript’s Category,

5. Structure and Format of Manuscript,

6. After Acceptance.

1. GENERAL

Before submitting your research paper, one is advised to go through the details as mentioned in following heads. It will be beneficial, while peer reviewer justify your paper for publication.

Scope

The Global Journals Inc. (US) welcome the submission of original paper, review paper, survey article relevant to the all the streams of Philosophy and knowledge. The Global Journals Inc. (US) is parental platform for Global Journal of Computer Science and Technology, Researches in Engineering, Medical Research, Science Frontier Research, Human Social Science, Management, and Business organization. The choice of specific field can be done otherwise as following in Abstracting and Indexing Page on this Website. As the all Global

Journals Inc. (US) are being abstracted and indexed (in process) by most of the reputed organizations. Topics of only narrow interest will not be accepted unless they have wider potential or consequences.

2. ETHICAL GUIDELINES

Authors should follow the ethical guidelines as mentioned below for publication of research paper and research activities.

Papers are accepted on strict understanding that the material in whole or in part has not been, nor is being, considered for publication elsewhere. If the paper once accepted by Global Journals Inc. (US) and Editorial Board, will become the copyright of the Global Journals Inc. (US).

Authorship: The authors and coauthors should have active contribution to conception design, analysis and interpretation of findings. They should critically review the contents and drafting of the paper. All should approve the final version of the paper before submission

The Global Journals Inc. (US) follows the definition of authorship set up by the Global Academy of Research and Development. According to the Global Academy of R&D authorship, criteria must be based on:

1) Substantial contributions to conception and acquisition of data, analysis and interpretation of the findings.

2) Drafting the paper and revising it critically regarding important academic content.

3) Final approval of the version of the paper to be published.

All authors should have been credited according to their appropriate contribution in research activity and preparing paper. Contributors who do not match the criteria as authors may be mentioned under Acknowledgement.

Acknowledgements: Contributors to the research other than authors credited should be mentioned under acknowledgement. The specifications of the source of funding for the research if appropriate can be included. Suppliers of resources may be mentioned along with address.

Appeal of Decision: The Editorial Board’s decision on publication of the paper is final and cannot be appealed elsewhere.

Permissions: It is the author's responsibility to have prior permission if all or parts of earlier published illustrations are used in this paper.

Please mention proper reference and appropriate acknowledgements wherever expected.

If all or parts of previously published illustrations are used, permission must be taken from the copyright holder concerned. It is the author's responsibility to take these in writing.

Approval for reproduction/modification of any information (including figures and tables) published elsewhere must be obtained by the authors/copyright holders before submission of the manuscript. Contributors (Authors) are responsible for any copyright fee involved.

3. SUBMISSION OF MANUSCRIPTS

Manuscripts should be uploaded via this online submission page. The online submission is most efficient method for submission of papers, as it enables rapid distribution of manuscripts and consequently speeds up the review procedure. It also enables authors to know the status of their own manuscripts by emailing us. Complete instructions for submitting a paper is available below.

Manuscript submission is a systematic procedure and little preparation is required beyond having all parts of your manuscript in a given format and a computer with an Internet connection and a Web browser. Full help and instructions are provided on-screen. As an author, you will be prompted for login and manuscript details as Field of Paper and then to upload your manuscript file(s) according to the instructions.

To avoid postal delays, all transaction is preferred by e-mail. A finished manuscript submission is confirmed by e-mail immediately and your paper enters the editorial process with no postal delays. When a conclusion is made about the publication of your paper by our Editorial Board, revisions can be submitted online with the same procedure, with an occasion to view and respond to all comments.

Complete support for both authors and co-author is provided.

4. MANUSCRIPT'S CATEGORY

Based on potential and nature, the manuscript can be categorized under the following heads:

Original research paper: Such papers are reports of high-level significant original research work.

Review papers: These are concise, significant but helpful and decisive topics for young researchers.

Research articles: These are handled with small investigation and applications.

Research letters: The letters are small and concise comments on previously published matters.

5. STRUCTURE AND FORMAT OF MANUSCRIPT

The recommended size of original research paper is less than seven thousand words, review papers fewer than seven thousands words also.Preparation of research paper or how to write research paper, are major hurdle, while writing manuscript. The research articles and research letters should be fewer than three thousand words, the structure original research paper; sometime review paper should be as follows:

Papers: These are reports of significant research (typically less than 7000 words equivalent, including tables, figures, references), and comprise:

(a)Title should be relevant and commensurate with the theme of the paper.

(b) A brief Summary, "Abstract" (less than 150 words) containing the major results and conclusions.

(c) Up to ten keywords, that precisely identifies the paper's subject, purpose, and focus.

(d) An Introduction, giving necessary background excluding subheadings; objectives must be clearly declared.

(e) Resources and techniques with sufficient complete experimental details (wherever possible by reference) to permit repetition; sources of information must be given and numerical methods must be specified by reference, unless non-standard.

(f) Results should be presented concisely, by well-designed tables and/or figures; the same data may not be used in both; suitable statistical data should be given. All data must be obtained with attention to numerical detail in the planning stage. As reproduced design has been recognized to be important to experiments for a considerable time, the Editor has decided that any paper that appears not to have adequate numerical treatments of the data will be returned un-refereed;

(g) Discussion should cover the implications and consequences, not just recapitulating the results; conclusions should be summarizing.

(h) Brief Acknowledgements.

(i) References in the proper form.

Authors should very cautiously consider the preparation of papers to ensure that they communicate efficiently. Papers are much more likely to be accepted, if they are cautiously designed and laid out, contain few or no errors, are summarizing, and be conventional to the approach and instructions. They will in addition, be published with much less delays than those that require much technical and editorial correction.

The Editorial Board reserves the right to make literary corrections and to make suggestions to improve briefness.

It is vital, that authors take care in submitting a manuscript that is written in simple language and adheres to published guidelines.

Format

Language: The language of publication is UK English. Authors, for whom English is a second language, must have their manuscript efficiently edited by an English-speaking person before submission to make sure that, the English is of high excellence. It is preferable, that manuscripts should be professionally edited.

Standard Usage, Abbreviations, and Units: Spelling and hyphenation should be conventional to The Concise Oxford English Dictionary. Statistics and measurements should at all times be given in figures, e.g. 16 min, except for when the number begins a sentence. When the number does not refer to a unit of measurement it should be spelt in full unless, it is 160 or greater.

Abbreviations supposed to be used carefully. The abbreviated name or expression is supposed to be cited in full at first usage, followed by the conventional abbreviation in parentheses.

Metric SI units are supposed to generally be used excluding where they conflict with current practice or are confusing. For illustration, 1.4 l rather than 1.4 × 10-3 m3, or 4 mm somewhat than 4 × 10-3 m. Chemical formula and solutions must identify the form used, e.g. anhydrous or hydrated, and the concentration must be in clearly defined units. Common species names should be followed by underlines at the first mention. For following use the generic name should be constricted to a single letter, if it is clear.

Structure

All manuscripts submitted to Global Journals Inc. (US), ought to include:

Title: The title page must carry an instructive title that reflects the content, a running title (less than 45 characters together with spaces), names of the authors and co-authors, and the place(s) wherever the work was carried out. The full postal address in addition with the e-mail address of related author must be given. Up to eleven keywords or very brief phrases have to be given to help data retrieval, mining and indexing.

Abstract, used in Original Papers and Reviews:

Optimizing Abstract for Search Engines

Many researchers searching for information online will use search engines such as Google, Yahoo or similar. By optimizing your paper for search engines, you will amplify the chance of someone finding it. This in turn will make it more likely to be viewed and/or cited in a further work. Global Journals Inc. (US) have compiled these guidelines to facilitate you to maximize the web-friendliness of the most public part of your paper.

Key Words

A major linchpin in research work for the writing research paper is the keyword search, which one will employ to find both library and Internet resources.

One must be persistent and creative in using keywords. An effective keyword search requires a strategy and planning a list of possible keywords and phrases to try.

Search engines for most searches, use Boolean searching, which is somewhat different from Internet searches. The Boolean search uses "operators," words (and, or, not, and near) that enable you to expand or narrow your affords. Tips for research paper while preparing research paper are very helpful guideline of research paper.

Choice of key words is first tool of tips to write research paper. Research paper writing is an art.A few tips for deciding as strategically as possible about keyword search:

- One should start brainstorming lists of possible keywords before even begin searching. Think about the most important concepts related to research work. Ask, "What words would a source have to include to be truly valuable in research paper?" Then consider synonyms for the important words.
- It may take the discovery of only one relevant paper to let steer in the right keyword direction because in most databases, the keywords under which a research paper is abstracted are listed with the paper.
- One should avoid outdated words.

Keywords are the key that opens a door to research work sources. Keyword searching is an art in which researcher's skills are bound to improve with experience and time.

Numerical Methods: Numerical methods used should be clear and, where appropriate, supported by references.

Acknowledgements: Please make these as concise as possible.

References

References follow the Harvard scheme of referencing. References in the text should cite the authors' names followed by the time of their publication, unless there are three or more authors when simply the first author's name is quoted followed by et al. unpublished work has to only be cited where necessary, and only in the text. Copies of references in press in other journals have to be supplied with submitted typescripts. It is necessary that all citations and references be carefully checked before submission, as mistakes or omissions will cause delays.

References to information on the World Wide Web can be given, but only if the information is available without charge to readers on an official site. Wikipedia and Similar websites are not allowed where anyone can change the information. Authors will be asked to make available electronic copies of the cited information for inclusion on the Global Journals Inc. (US) homepage at the judgment of the Editorial Board.

The Editorial Board and Global Journals Inc. (US) recommend that, citation of online-published papers and other material should be done via a DOI (digital object identifier). If an author cites anything, which does not have a DOI, they run the risk of the cited material not being noticeable.

The Editorial Board and Global Journals Inc. (US) recommend the use of a tool such as Reference Manager for reference management and formatting.

Tables, Figures and Figure Legends

Tables: Tables should be few in number, cautiously designed, uncrowned, and include only essential data. Each must have an Arabic number, e.g. Table 4, a self-explanatory caption and be on a separate sheet. Vertical lines should not be used.

Figures: Figures are supposed to be submitted as separate files. Always take in a citation in the text for each figure using Arabic numbers, e.g. Fig. 4. Artwork must be submitted online in electronic form by e-mailing them.

Preparation of Electronic Figures for Publication

Even though low quality images are sufficient for review purposes, print publication requires high quality images to prevent the final product being blurred or fuzzy. Submit (or e-mail) EPS (line art) or TIFF (halftone/photographs) files only. MS PowerPoint and Word Graphics are unsuitable for printed pictures. Do not use pixel-oriented software. Scans (TIFF only) should have a resolution of at least 350 dpi (halftone) or 700 to 1100 dpi (line drawings) in relation to the imitation size. Please give the data for figures in black and white or submit a Color Work Agreement Form. EPS files must be saved with fonts embedded (and with a TIFF preview, if possible).

For scanned images, the scanning resolution (at final image size) ought to be as follows to ensure good reproduction: line art: >650 dpi; halftones (including gel photographs) : >350 dpi; figures containing both halftone and line images: >650 dpi.

Color Charges: It is the rule of the Global Journals Inc. (US) for authors to pay the full cost for the reproduction of their color artwork. Hence, please note that, if there is color artwork in your manuscript when it is accepted for publication, we would require you to complete and return a color work agreement form before your paper can be published.

Figure Legends: Self-explanatory legends of all figures should be incorporated separately under the heading 'Legends to Figures'. In the full-text online edition of the journal, figure legends may possibly be truncated in abbreviated links to the full screen version. Therefore, the first 100 characters of any legend should notify the reader, about the key aspects of the figure.

6. AFTER ACCEPTANCE

Upon approval of a paper for publication, the manuscript will be forwarded to the dean, who is responsible for the publication of the Global Journals Inc. (US).

6.1 Proof Corrections

The corresponding author will receive an e-mail alert containing a link to a website or will be attached. A working e-mail address must therefore be provided for the related author.

Acrobat Reader will be required in order to read this file. This software can be downloaded

(Free of charge) from the following website:

www.adobe.com/products/acrobat/readstep2.html. This will facilitate the file to be opened, read on screen, and printed out in order for any corrections to be added. Further instructions will be sent with the proof.

Proofs must be returned to the dean at dean@globaljournals.org within three days of receipt.

As changes to proofs are costly, we inquire that you only correct typesetting errors. All illustrations are retained by the publisher. Please note that the authors are responsible for all statements made in their work, including changes made by the copy editor.

6.2 Early View of Global Journals Inc. (US) (Publication Prior to Print)

The Global Journals Inc. (US) are enclosed by our publishing's Early View service. Early View articles are complete full-text articles sent in advance of their publication. Early View articles are absolute and final. They have been completely reviewed, revised and edited for publication, and the authors' final corrections have been incorporated. Because they are in final form, no changes can be made after sending them. The nature of Early View articles means that they do not yet have volume, issue or page numbers, so Early View articles cannot be cited in the conventional way.

6.3 Author Services

Online production tracking is available for your article through Author Services. Author Services enables authors to track their article - once it has been accepted - through the production process to publication online and in print. Authors can check the status of their articles online and choose to receive automated e-mails at key stages of production. The authors will receive an e-mail with a unique link that enables them to register and have their article automatically added to the system. Please ensure that a complete e-mail address is provided when submitting the manuscript.

6.4 Author Material Archive Policy

Please note that if not specifically requested, publisher will dispose off hardcopy & electronic information submitted, after the two months of publication. If you require the return of any information submitted, please inform the Editorial Board or dean as soon as possible.

6.5 Offprint and Extra Copies

A PDF offprint of the online-published article will be provided free of charge to the related author, and may be distributed according to the Publisher's terms and conditions. Additional paper offprint may be ordered by emailing us at: editor@globaljournals.org .

You must strictly follow above Author Guidelines before submitting your paper or else we will not at all be responsible for any corrections in future in any of the way.

Before start writing a good quality Computer Science Research Paper, let us first understand what is Computer Science Research Paper? So, Computer Science Research Paper is the paper which is written by professionals or scientists who are associated to Computer Science and Information Technology, or doing research study in these areas. If you are novel to this field then you can consult about this field from your supervisor or guide.

TECHNIQUES FOR WRITING A GOOD QUALITY RESEARCH PAPER:

1. Choosing the topic: In most cases, the topic is searched by the interest of author but it can be also suggested by the guides. You can have several topics and then you can judge that in which topic or subject you are finding yourself most comfortable. This can be done by asking several questions to yourself, like Will I be able to carry our search in this area? Will I find all necessary recourses to accomplish the search? Will I be able to find all information in this field area? If the answer of these types of questions will be "Yes" then you can choose that topic. In most of the cases, you may have to conduct the surveys and have to visit several places because this field is related to Computer Science and Information Technology. Also, you may have to do a lot of work to find all rise and falls regarding the various data of that subject. Sometimes, detailed information plays a vital role, instead of short information.

2. Evaluators are human: First thing to remember that evaluators are also human being. They are not only meant for rejecting a paper. They are here to evaluate your paper. So, present your Best.

3. Think Like Evaluators: If you are in a confusion or getting demotivated that your paper will be accepted by evaluators or not, then think and try to evaluate your paper like an Evaluator. Try to understand that what an evaluator wants in your research paper and automatically you will have your answer.

4. Make blueprints of paper: The outline is the plan or framework that will help you to arrange your thoughts. It will make your paper logical. But remember that all points of your outline must be related to the topic you have chosen.

5. Ask your Guides: If you are having any difficulty in your research, then do not hesitate to share your difficulty to your guide (if you have any). They will surely help you out and resolve your doubts. If you can't clarify what exactly you require for your work then ask the supervisor to help you with the alternative. He might also provide you the list of essential readings.

6. Use of computer is recommended: As you are doing research in the field of Computer Science, then this point is quite obvious.

7. Use right software: Always use good quality software packages. If you are not capable to judge good software then you can lose quality of your paper unknowingly. There are various software programs available to help you, which you can get through Internet.

8. Use the Internet for help: An excellent start for your paper can be by using the Google. It is an excellent search engine, where you can have your doubts resolved. You may also read some answers for the frequent question how to write my research paper or find model research paper. From the internet library you can download books. If you have all required books make important reading selecting and analyzing the specified information. Then put together research paper sketch out.

9. Use and get big pictures: Always use encyclopedias, Wikipedia to get pictures so that you can go into the depth.

10. Bookmarks are useful: When you read any book or magazine, you generally use bookmarks, right! It is a good habit, which helps to not to lose your continuity. You should always use bookmarks while searching on Internet also, which will make your search easier.

11. Revise what you wrote: When you write anything, always read it, summarize it and then finalize it.

12. Make all efforts: Make all efforts to mention what you are going to write in your paper. That means always have a good start. Try to mention everything in introduction, that what is the need of a particular research paper. Polish your work by good skill of writing and always give an evaluator, what he wants.

13. Have backups: When you are going to do any important thing like making research paper, you should always have backup copies of it either in your computer or in paper. This will help you to not to lose any of your important.

14. Produce good diagrams of your own: Always try to include good charts or diagrams in your paper to improve quality. Using several and unnecessary diagrams will degrade the quality of your paper by creating "hotchpotch." So always, try to make and include those diagrams, which are made by your own to improve readability and understandability of your paper.

15. Use of direct quotes: When you do research relevant to literature, history or current affairs then use of quotes become essential but if study is relevant to science then use of quotes is not preferable.

16. Use proper verb tense: Use proper verb tenses in your paper. Use past tense, to present those events that happened. Use present tense to indicate events that are going on. Use future tense to indicate future happening events. Use of improper and wrong tenses will confuse the evaluator. Avoid the sentences that are incomplete.

17. Never use online paper: If you are getting any paper on Internet, then never use it as your research paper because it might be possible that evaluator has already seen it or maybe it is outdated version.

18. Pick a good study spot: To do your research studies always try to pick a spot, which is quiet. Every spot is not for studies. Spot that suits you choose it and proceed further.

19. Know what you know: Always try to know, what you know by making objectives. Else, you will be confused and cannot achieve your target.

20. Use good quality grammar: Always use a good quality grammar and use words that will throw positive impact on evaluator. Use of good quality grammar does not mean to use tough words, that for each word the evaluator has to go through dictionary. Do not start sentence with a conjunction. Do not fragment sentences. Eliminate one-word sentences. Ignore passive voice. Do not ever use a big word when a diminutive one would suffice. Verbs have to be in agreement with their subjects. Prepositions are not expressions to finish sentences with. It is incorrect to ever divide an infinitive. Avoid clichés like the disease. Also, always shun irritating alliteration. Use language that is simple and straight forward. put together a neat summary.

21. Arrangement of information: Each section of the main body should start with an opening sentence and there should be a changeover at the end of the section. Give only valid and powerful arguments to your topic. You may also maintain your arguments with records.

22. Never start in last minute: Always start at right time and give enough time to research work. Leaving everything to the last minute will degrade your paper and spoil your work.

23. Multitasking in research is not good: Doing several things at the same time proves bad habit in case of research activity. Research is an area, where everything has a particular time slot. Divide your research work in parts and do particular part in particular time slot.

24. Never copy others' work: Never copy others' work and give it your name because if evaluator has seen it anywhere you will be in trouble.

25. Take proper rest and food: No matter how many hours you spend for your research activity, if you are not taking care of your health then all your efforts will be in vain. For a quality research, study is must, and this can be done by taking proper rest and food.

26. Go for seminars: Attend seminars if the topic is relevant to your research area. Utilize all your resources.

27. Refresh your mind after intervals: Try to give rest to your mind by listening to soft music or by sleeping in intervals. This will also improve your memory.

28. Make colleagues: Always try to make colleagues. No matter how sharper or intelligent you are, if you make colleagues you can have several ideas, which will be helpful for your research.

29. Think technically: Always think technically. If anything happens, then search its reasons, its benefits, and demerits.

30. Think and then print: When you will go to print your paper, notice that tables are not be split, headings are not detached from their descriptions, and page sequence is maintained.

31. Adding unnecessary information: Do not add unnecessary information, like, I have used MS Excel to draw graph. Do not add irrelevant and inappropriate material. These all will create superfluous. Foreign terminology and phrases are not apropos. One should NEVER take a broad view. Analogy in script is like feathers on a snake. Not at all use a large word when a very small one would be sufficient. Use words properly, regardless of how others use them. Remove quotations. Puns are for kids, not grunt readers. Amplification is a billion times of inferior quality than sarcasm.

32. Never oversimplify everything: To add material in your research paper, never go for oversimplification. This will definitely irritate the evaluator. Be more or less specific. Also too, by no means, ever use rhythmic redundancies. Contractions aren't essential and shouldn't be there used. Comparisons are as terrible as clichés. Give up ampersands and abbreviations, and so on. Remove commas, that are, not necessary. Parenthetical words however should be together with this in commas. Understatement is all the time the complete best way to put onward earth-shaking thoughts. Give a detailed literary review.

33. Report concluded results: Use concluded results. From raw data, filter the results and then conclude your studies based on measurements and observations taken. Significant figures and appropriate number of decimal places should be used. Parenthetical remarks are prohibitive. Proofread carefully at final stage. In the end give outline to your arguments. Spot out perspectives of further study of this subject. Justify your conclusion by at the bottom of them with sufficient justifications and examples.

34. After conclusion: Once you have concluded your research, the next most important step is to present your findings. Presentation is extremely important as it is the definite medium though which your research is going to be in print to the rest of the crowd. Care should be taken to categorize your thoughts well and present them in a logical and neat manner. A good quality research paper format is essential because it serves to highlight your research paper and bring to light all necessary aspects in your research.

Informal Guidelines of Research Paper Writing

Key points to remember:

- Submit all work in its final form.
- Write your paper in the form, which is presented in the guidelines using the template.
- Please note the criterion for grading the final paper by peer-reviewers.

Final Points:

A purpose of organizing a research paper is to let people to interpret your effort selectively. The journal requires the following sections, submitted in the order listed, each section to start on a new page.

The introduction will be compiled from reference matter and will reflect the design processes or outline of basis that direct you to make study. As you will carry out the process of study, the method and process section will be constructed as like that. The result segment will show related statistics in nearly sequential order and will direct the reviewers next to the similar intellectual paths throughout the data that you took to carry out your study. The discussion section will provide understanding of the data and projections as to the implication of the results. The use of good quality references all through the paper will give the effort trustworthiness by representing an alertness of prior workings.

Writing a research paper is not an easy job no matter how trouble-free the actual research or concept. Practice, excellent preparation, and controlled record keeping are the only means to make straightforward the progression.

General style:

Specific editorial column necessities for compliance of a manuscript will always take over from directions in these general guidelines.

To make a paper clear

· Adhere to recommended page limits

Mistakes to evade

- Insertion a title at the foot of a page with the subsequent text on the next page
- Separating a table/chart or figure - impound each figure/table to a single page
- Submitting a manuscript with pages out of sequence

In every sections of your document

· Use standard writing style including articles ("a", "the," etc.)

· Keep on paying attention on the research topic of the paper

· Use paragraphs to split each significant point (excluding for the abstract)

· Align the primary line of each section

· Present your points in sound order

· Use present tense to report well accepted

· Use past tense to describe specific results

· Shun familiar wording, don't address the reviewer directly, and don't use slang, slang language, or superlatives

· Shun use of extra pictures - include only those figures essential to presenting results

Title Page:

Choose a revealing title. It should be short. It should not have non-standard acronyms or abbreviations. It should not exceed two printed lines. It should include the name(s) and address (es) of all authors.

Abstract:

The summary should be two hundred words or less. It should briefly and clearly explain the key findings reported in the manuscript--must have precise statistics. It should not have abnormal acronyms or abbreviations. It should be logical in itself. Shun citing references at this point.

An abstract is a brief distinct paragraph summary of finished work or work in development. In a minute or less a reviewer can be taught the foundation behind the study, common approach to the problem, relevant results, and significant conclusions or new questions.

Write your summary when your paper is completed because how can you write the summary of anything which is not yet written? Wealth of terminology is very essential in abstract. Yet, use comprehensive sentences and do not let go readability for briefness. You can maintain it succinct by phrasing sentences so that they provide more than lone rationale. The author can at this moment go straight to shortening the outcome. Sum up the study, with the subsequent elements in any summary. Try to maintain the initial two items to no more than one ruling each.

- Reason of the study - theory, overall issue, purpose
- Fundamental goal
- To the point depiction of the research
- Consequences, including definite statistics - if the consequences are quantitative in nature, account quantitative data; results of any numerical analysis should be reported
- Significant conclusions or questions that track from the research(es)

Approach:

- Single section, and succinct
- As a outline of job done, it is always written in past tense
- A conceptual should situate on its own, and not submit to any other part of the paper such as a form or table
- Center on shortening results - bound background information to a verdict or two, if completely necessary
- What you account in an conceptual must be regular with what you reported in the manuscript
- Exact spelling, clearness of sentences and phrases, and appropriate reporting of quantities (proper units, important statistics) are just as significant in an abstract as they are anywhere else

Introduction:

The **Introduction** should "introduce" the manuscript. The reviewer should be presented with sufficient background information to be capable to comprehend and calculate the purpose of your study without having to submit to other works. The basis for the study should be offered. Give most important references but shun difficult to make a comprehensive appraisal of the topic. In the introduction, describe the problem visibly. If the problem is not acknowledged in a logical, reasonable way, the reviewer will have no attention in your result. Speak in common terms about techniques used to explain the problem, if needed, but do not present any particulars about the protocols here. Following approach can create a valuable beginning:

- Explain the value (significance) of the study
- Shield the model - why did you employ this particular system or method? What is its compensation? You strength remark on its appropriateness from a abstract point of vision as well as point out sensible reasons for using it.
- Present a justification. Status your particular theory (es) or aim(s), and describe the logic that led you to choose them.
- Very for a short time explain the tentative propose and how it skilled the declared objectives.

Approach:

- Use past tense except for when referring to recognized facts. After all, the manuscript will be submitted after the entire job is done.
- Sort out your thoughts; manufacture one key point with every section. If you make the four points listed above, you will need a least of four paragraphs.

- Present surroundings information only as desirable in order hold up a situation. The reviewer does not desire to read the whole thing you know about a topic.
- Shape the theory/purpose specifically - do not take a broad view.
- As always, give awareness to spelling, simplicity and correctness of sentences and phrases.

Procedures (Methods and Materials):

This part is supposed to be the easiest to carve if you have good skills. A sound written Procedures segment allows a capable scientist to replacement your results. Present precise information about your supplies. The suppliers and clarity of reagents can be helpful bits of information. Present methods in sequential order but linked methodologies can be grouped as a segment. Be concise when relating the protocols. Attempt for the least amount of information that would permit another capable scientist to spare your outcome but be cautious that vital information is integrated. The use of subheadings is suggested and ought to be synchronized with the results section. When a technique is used that has been well described in another object, mention the specific item describing a way but draw the basic principle while stating the situation. The purpose is to text all particular resources and broad procedures, so that another person may use some or all of the methods in one more study or referee the scientific value of your work. It is not to be a step by step report of the whole thing you did, nor is a methods section a set of orders.

Materials:

- Explain materials individually only if the study is so complex that it saves liberty this way.
- Embrace particular materials, and any tools or provisions that are not frequently found in laboratories.
- Do not take in frequently found.
- If use of a definite type of tools.
- Materials may be reported in a part section or else they may be recognized along with your measures.

Methods:

- Report the method (not particulars of each process that engaged the same methodology)
- Describe the method entirely
- To be succinct, present methods under headings dedicated to specific dealings or groups of measures
- Simplify - details how procedures were completed not how they were exclusively performed on a particular day.
- If well known procedures were used, account the procedure by name, possibly with reference, and that's all.

Approach:

- It is embarrassed or not possible to use vigorous voice when documenting methods with no using first person, which would focus the reviewer's interest on the researcher rather than the job. As a result when script up the methods most authors use third person passive voice.
- Use standard style in this and in every other part of the paper - avoid familiar lists, and use full sentences.

What to keep away from

- Resources and methods are not a set of information.
- Skip all descriptive information and surroundings - save it for the argument.
- Leave out information that is immaterial to a third party.

Results:

The principle of a results segment is to present and demonstrate your conclusion. Create this part a entirely objective details of the outcome, and save all understanding for the discussion.

The page length of this segment is set by the sum and types of data to be reported. Carry on to be to the point, by means of statistics and tables, if suitable, to present consequences most efficiently.You must obviously differentiate material that would usually be incorporated in a study editorial from any unprocessed data or additional appendix matter that would not be available. In fact, such matter should not be submitted at all except requested by the instructor.

Content

- Sum up your conclusion in text and demonstrate them, if suitable, with figures and tables.
- In manuscript, explain each of your consequences, point the reader to remarks that are most appropriate.
- Present a background, such as by describing the question that was addressed by creation an exacting study.
- Explain results of control experiments and comprise remarks that are not accessible in a prescribed figure or table, if appropriate.
- Examine your data, then prepare the analyzed (transformed) data in the form of a figure (graph), table, or in manuscript form.

What to stay away from

- Do not discuss or infer your outcome, report surroundings information, or try to explain anything.
- Not at all, take in raw data or intermediate calculations in a research manuscript.
- Do not present the similar data more than once.
- Manuscript should complement any figures or tables, not duplicate the identical information.
- Never confuse figures with tables - there is a difference.

Approach

- As forever, use past tense when you submit to your results, and put the whole thing in a reasonable order.
- Put figures and tables, appropriately numbered, in order at the end of the report
- If you desire, you may place your figures and tables properly within the text of your results part.

Figures and tables

- If you put figures and tables at the end of the details, make certain that they are visibly distinguished from any attach appendix materials, such as raw facts
- Despite of position, each figure must be numbered one after the other and complete with subtitle
- In spite of position, each table must be titled, numbered one after the other and complete with heading
- All figure and table must be adequately complete that it could situate on its own, divide from text

Discussion:

The Discussion is expected the trickiest segment to write and describe. A lot of papers submitted for journal are discarded based on problems with the Discussion. There is no head of state for how long a argument should be. Position your understanding of the outcome visibly to lead the reviewer through your conclusions, and then finish the paper with a summing up of the implication of the study. The purpose here is to offer an understanding of your results and hold up for all of your conclusions, using facts from your research and generally accepted information, if suitable. The implication of result should be visibly described. Infer your data in the conversation in suitable depth. This means that when you clarify an observable fact you must explain mechanisms that may account for the observation. If your results vary from your prospect, make clear why that may have happened. If your results agree, then explain the theory that the proof supported. It is never suitable to just state that the data approved with prospect, and let it drop at that.

- Make a decision if each premise is supported, discarded, or if you cannot make a conclusion with assurance. Do not just dismiss a study or part of a study as "uncertain."
- Research papers are not acknowledged if the work is imperfect. Draw what conclusions you can based upon the results that you have, and take care of the study as a finished work
- You may propose future guidelines, such as how the experiment might be personalized to accomplish a new idea.
- Give details all of your remarks as much as possible, focus on mechanisms.
- Make a decision if the tentative design sufficiently addressed the theory, and whether or not it was correctly restricted.
- Try to present substitute explanations if sensible alternatives be present.
- One research will not counter an overall question, so maintain the large picture in mind, where do you go next? The best studies unlock new avenues of study. What questions remain?
- Recommendations for detailed papers will offer supplementary suggestions.

Approach:

- When you refer to information, differentiate data generated by your own studies from available information
- Submit to work done by specific persons (including you) in past tense.
- Submit to generally acknowledged facts and main beliefs in present tense.

Administration Rules Listed Before Submitting Your Research Paper to Global Journals Inc. (US)

Please carefully note down following rules and regulation before submitting your Research Paper to Global Journals Inc. (US):

Segment Draft and Final Research Paper: You have to strictly follow the template of research paper. If it is not done your paper may get rejected.

- The **major constraint** is that you must independently make all content, tables, graphs, and facts that are offered in the paper. You must write each part of the paper wholly on your own. The Peer-reviewers need to identify your own perceptive of the concepts in your own terms. NEVER extract straight from any foundation, and never rephrase someone else's analysis.
- Do not give permission to anyone else to "PROOFREAD" your manuscript.
- Methods to avoid Plagiarism is applied by us on every paper, if found guilty, you will be blacklisted by all of our collaborated research groups, your institution will be informed for this and strict legal actions will be taken immediately.)
- To guard yourself and others from possible illegal use please do not permit anyone right to use to your paper and files.

Criterion for Grading a Research Paper (Compilation) by Global Journals Inc. (US)

Please note that following table is only a Grading of "Paper Compilation" and not on "Performed/Stated Research" whose grading solely depends on Individual Assigned Peer Reviewer and Editorial Board Member. These can be available only on request and after decision of Paper. This report will be the property of Global Journals Inc. (US).

Topics	Grades		
	A-B	**C-D**	**E-F**
Abstract	Clear and concise with appropriate content, Correct format. 200 words or below	Unclear summary and no specific data, Incorrect form Above 200 words	No specific data with ambiguous information Above 250 words
Introduction	Containing all background details with clear goal and appropriate details, flow specification, no grammar and spelling mistake, well organized sentence and paragraph, reference cited	Unclear and confusing data, appropriate format, grammar and spelling errors with unorganized matter	Out of place depth and content, hazy format
Methods and Procedures	Clear and to the point with well arranged paragraph, precision and accuracy of facts and figures, well organized subheads	Difficult to comprehend with embarrassed text, too much explanation but completed	Incorrect and unorganized structure with hazy meaning
Result	Well organized, Clear and specific, Correct units with precision, correct data, well structuring of paragraph, no grammar and spelling mistake	Complete and embarrassed text, difficult to comprehend	Irregular format with wrong facts and figures
Discussion	Well organized, meaningful specification, sound conclusion, logical and concise explanation, highly structured paragraph reference cited	Wordy, unclear conclusion, spurious	Conclusion is not cited, unorganized, difficult to comprehend
References	Complete and correct format, well organized	Beside the point, Incomplete	Wrong format and structuring

INDEX

T

U

V

save our planet

Global Journal of Computer Science and Technology

Visit us on the Web at www.GlobalJournals.org | www.ComputerResearch.org
or email us at helpdesk@globaljournals.org

ISSN 9754350