Volume 5, Issue 2, February 2015 ISSN: 2277 128X
International Journal of Advanced Research in Computer Science and Software Engineering
Research Paper
Available online at: www.ijarcsse.com

A Random Key Distribution Technique based on Memetic Theory for Securing Clustered Wireless Sensor Networks

P.V. Ranjith Kumar
Dept. of Electronics & Communication Engg.
M.S. Ramaiah Institute of Technology,
Bangalore, Karnataka, India

Sandeep Kumar E.
Dept. of Telecommunication Engg.
J.N.N. College of Engineering,
Shimoga, Karnataka, India

Abstract— Wireless Sensor Networks (WSNs) are always under the risk of security threats and vulnerabilities. This is because these networks are operated under less human intervention with self- organizing capabilities. Hence, there is always a thirst for novel security protocols and techniques to combat against the attacks. In this context, we propose a random keying technique based on the concepts of memetic theory as a counter measure against spoofing attacks and serves as an improvement over [1] by increasing the randomness in choosing the keys for communication. The simulation results prove that the proposed technique provides an effective way of combating against the spoofing attacks.

Keywords— Clustered wireless sensor networks, Memetics, Bio-inspired computation.

I. INTRODUCTION

WIRELESS Sensor Networks are gaining lot of attentions in the present world scenario because of their low cost solutions to many of the problems. In these networks, security is one of the major concerns because of the resource constraints of the sensor nodes. The lack of resources in the nodes, impose a threshold on the protocols and techniques that which combat against the attacks compared to traditional wireless and wired networks. This has also been a thirst area for researchers because of the attack varieties and its difficulty in combating. Few are the literatures in this regard for dealt with the combating mechanisms against the attacks in WSNs.

Suman *et al.* [1] propose a novel memetic based keying technique to combat against the spoofing attacks. In this paper, the crossing over characteristics of memes is employed, which are keys in the security context. The mutation of the memes were the bit complement of the keys. In the proposed work of this paper, the technique used for the mutation is changed with a novel concept that introduces much more randomness in the security technique of [1]. Ranjith *et al.* [2] propose a novel technique of combating against spoofing attacks using the concept of genetics. Sandeep *et al.* [3] proposed a random keying technique based on the concept of Negative Selection of Immune System against the spoofing attacks. Chuan- Kang Ting *et al.* [5] propose a technique to enhance the network lifetime by increasing the coverage area using memetics. Konstantinos *et al.* [6] propose a method for improving network lifespan using memetic algorithm as an improvement on the genetic algorithm taking into accounts of communication parameters and overheads of the sensor nodes.

Memetics serves as a recent advancement over genetics under evolutionary intelligence of artificial intelligence.

The proposed work in this paper uses the memetic theory concept against spoofing attacks and serves as an improvement over [1]. The detailed description of the work is dealt in the later sections of the paper. The algorithm was implemented in MATLAB 2013 and the simulation results prove that the technique is robust and serves as an effective way of combating against the spoofing attacks.

The rest of the paper is organized as follows: The rest of the paper is organized as follows: section II deals with memetics, section III with the proposed methodology, section IV with radio model, section V with the attack scenario, section VI with the simulations, section VII with the results and discussions and section VIII with the concluding remarks of the paper.

II. MEMETIC THEORY

Meme is an information pattern, held in an individual's memory, which is capable of being copied to another individual's memory. Memetics is the theoretical and empirical science that deals with the study of the replication, spread and evolution of memes [10].

Memetic algorithms have elements of metaheuristic and computational intelligence. Although they have principles of evolutionary algorithms, they may not strictly be considered an evolutionary technique. Using ideas of memes and memetic algorithms in optimization may be referred to as memetics computing [9].

A meme is a cognitive pattern that can be transmitted from one person to another. Since the individual who transmitted the meme will continue to carry it, the transmission can be interpreted as replication making him or her to be the carrier of meme. This process of self- reproduction leading to spreading over a growing group individuals, defines the meme as a replicator, similar in that respect to the gene.

The memetic algorithm can simply be considered as the improvement over the genetic algorithm in the notion that, the genes are transferred directly to the individual but the memes are processed locally and then transferred. Hence, adding local search to the genetic algorithm results in memetic algorithm.

The algorithm is given below:

1. **Start:** Randomly generate a population of N chromosomes.
2. **Fitness:** Calculate the fitness of all chromosomes.
3. Create a new population:
    a. **Selection:** According to the selection method, select two chromosomes from the population, which are best chromosomes.
    c. **Crossover:** Perform crossover on the two chromosomes selected.
    d. **Local search:** search for the best chromosomes.
    e. **Mutation:** Perform mutation on the chromosomes obtained with small probability.
4. **Replace:** Replace the current population with the new population.
5. **Test:** Test whether the termination condition is satisfied. If so, stop. If not, return the best solution in current population and go to Step 2.

This algorithm is modified for providing security in the WSNs as a light- weight protocol. Majority applications of memetic algorithms are used for solving optimization problems.

III. DEVISED METHODOLOGY

The proposed method uses the memetics based approach for combating against the spoofing attacks. The technique is developed for clustered wireless sensor networks.

A) Random key range distribution

1. At the Base Station (BS)- Set up phase

i. Set the range with in which the keys have to be selected. The keys (numbers) between these ranges are the initial set of populations (memes). Let this be (A, B).
ii. From the range (A, B) a random set of keys will be selected by scaling down the range, this indicates the optimal set of the keys, which participate in the further process. Let this be (X, Y), where X is the lower limit and Y is the upper limit.
iii. Within (X, Y) range, randomly two numbers will be picked and sent to the Cluster Heads (CH). Step iii is repeated until all the CHs receive two random numbers from the BS. Let the number received at the CHs be (S, T) where, S is the lower limit and T is the upper limit. For the further process, the memes will be selected based on this range.

2. At the Cluster Heads

The received range from the BS will be sent all the member nodes of its cluster. This is also (S, T). Hence, the entire cluster will be synchronized with the range (S, T) for further security measures.

B) Steady phase communication

i. Ordinary member node, if it wants to communicate with its CH, it randomly picks two numbers from within the range (S, T). The numbers (keys) in the range (S, T) is the pool of population of memes. The chosen numbers in this pool indicates the best locally picked memes for the further processes. Let this be (p, n).
ii. These memes are allowed to crossover with each other. The procedure of the crossover is dealt in the later sections of the paper.
iii. The crossovered numbers (memes) are now checked for fittest candidate for the further mutation process. The result of crossover will be two numbers, let this be (B, D) and out of two, one candidate is picked based on the presence of number of ones. The candidate is now allowed for mutation, whose process is explained in the further sections of this paper, the other number is kept as it is without any change. Let the picked candidate be h, and the result of the mutation be v, the result after the process is (k, v).
iv. (p, q) is place in the header and (k, v) is substituted as the trailer and the packet is sent to the CH.
v. The process is repeated by all the ordinary nodes in a network, which wants to communicate with the CH. The respective CHs wait until it receives the data from all the ordinary nodes and again follows step i to step iv and places header and trailer information in the packet and sends to the BS.

C) Crossover

Let the range received by the higher hierarchy node be (p, q).

Select two numbers randomly between this range and let this be (m, n). The step involved is given below:

1. Initially, calculate two intermediate numbers.

$$E = (m-1) + (n-1);$$
$$F = (m+1) + (n+1); \quad (1)$$

2. Find the smallest multiple of 3 between the range (S, E), let this be I. Here 3 is as example in the future this can also be made a random choice. If I exists then H=I, else H=S.
3. Find (H mod 8). let this be C. This value in turn indicates the point at which the crossover has to start.
   Ex: (p, q) = (12, 70) and let (m, n) = (15, 56);

E = (15-1) + (56-1) = 69;
F= (15+1) + (56+1) = 73;
The smallest multiple between (15, 69) is H= 15;

4. (15 mod 8)= 7; hence 7 is the crossover point. The bits from 7th position to the 8th position of m and n are crossovered. Here 8 indicates that each of the key length is of 8 bits.

Before Crossover:
m= 15 = 0000 1111
n= 56 = 0011 1000
After Crossover:
m= **00** 00 1111= 15
n= **00** 00 1000 = 56
The result of crossover is (m, n) = (15, 56). Whichever is having more number of bits will be considered for further mutation process.

D) Mutation

The two bytes obtained after the crossover is checked for number of 1's individually and the number with the highest number of ones are chosen as the best candidate for mutation. From the example dealt in the crossover, section the best candidate chosen is 15 because it has more number of 1's in it.

1. Select a random number between N= (E, F).
2. Find a multiple of V= (N mod 3), 3 is chosen as an example but in the future works this can be chosen as a random number. If V is zero then H= E else H=F. this step indicates the selection of the
3. Find (H mod8). Let this be R. The point R is the point of mutation.

Ex: N= 73. V= (73 mod 3) = 1, hence H= 73.
Based on the highest number of ones, choose either m or n. From the above example, consider 15. Find (15 mod 8) = 7. This indicates that bit 7 of 15 should be mutated. Hence, 1 will be changed to 0 and vice-versa. The result after mutation is 79. In the header of the packet we have (15, 56) and as the trailer information we have (79, 56).

E) Verification at the CH for the packet sent by ordinary node or Verification at the BS for the packet sent by CH.

1. Start
2. Receive the packet
3. Extract header
4. Check header, whether it is in the range that was sent by itself. **Let the received header be m, n and trailer be k, v.**

```
If (m>= Sand n<=T)
{
/* packet cleared stage-1*/
(g, h) = Crossover (m, n); /*H1 and H2 are results of crossover*/
Select the best candidate for mutation. Let this be H.
(g1, h1)= Mutation (H);
If (g1==k and h1==v)
        {
        /* packet cleared stage-2*/
        Else
        /* packet is malicious*/
        }
Else
{
/* packet is malicious*/
}
```

5. Stop

E) Packet Description

i. Packet sent from BS to CH/ CH to its member nodes

MAC	S	T

Where, MAC→ MAC address of the intended CH node p,
q→ Keys randomly picked by the BS for a CH.

ii. Packet sent from ordinary node to CH/ CH to BS

This packet consists of the details regarding randomly picked keys by the node and the trailer.

m	n	CRITICAL INFO	k	v

Where, m, n→ keys randomly picked by the node for communication with its CH and g1, h1 are the trailers after crossover and mutation, CRITICAL INFO→ consists of various fields including, preamble, sync bits, destination address, type, group identity, length of message, counter for message sent, source address, error checking bits, payload.

IV. RADIO MODEL

The proposed methodology uses a classical radio model. The sensor node is a transceiver. Hence, this radio model gives the energy consumed for the transmission and reception. The block diagram representation is shown in fig. 1. The radio model consists of transmitter and receiver equivalent of the nodes separated by the distance'd'. Where E_{tx}, E_{rx} are the energy consumed in the transmitter and the receiver electronics.

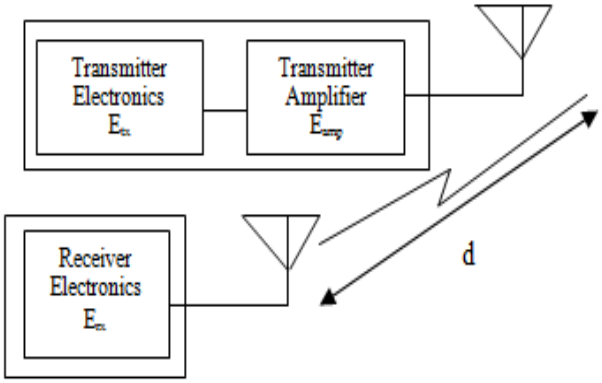

Fig.1Radio Model

E_{amp} is the energy consumed in the transmitter amplifier in general, and it depends on the type of propagation model chosen either free space or multipath with the acceptable bit error rate. We consider E_{fs} for free space propagation and E_{mp} for multipath propagation as the energy consumed in the amplifier circuitry. The transmitter and the receiver electronics depends on digital coding, modulation, filtering and spreading of data. Additional to this there is an aggregation energy consumption of E_{agg} per bit if the node is cluster head. The various parameters chosen is according to [3].

A. Energy Consumption

This section describes the energy consumed for communication.

Packet transmission

$E = (L_P * E_{tx}) + (L_P * E_{amp} * d^{n})$; . . . (2)

Where, L_P→ is the packet length in bits

n→ is the path loss component which is 2 for free space and 4 for multipath propagation.

Packet reception

$E = (L_P * E_{rx})$; . . . (3)

Where, L_P→ is the packet length in bits

V. ATTACK SCENARIO

The system relies on confusing the intruder by randomly varying the keys and ranges chosen for selecting the keys at the BS. The newly deployed malicious attacker may spoof unwanted packets to the CH or the BS. The attack scenarios are shown in the fig. 2 and fig.3

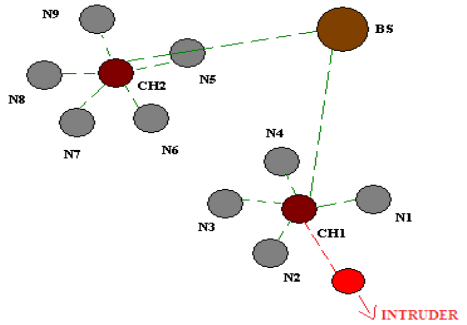

Fig.2 Malicious ordinary node sending a false packet to CH.

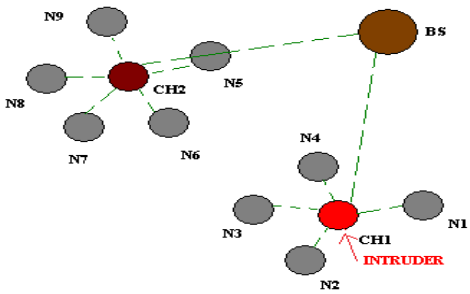

Fig.3 Malicious CH sending a false packet to the Base Station.

The new node carefully listens to the network paradigm and assigns its MAC address with that of another node, of which it may start disguising and spoofing packets to the higher hierarchical node. The packets follow the double verification steps and gets identified itself as either a legitimate or a spoofed packet. Suppose, the count of spoofed packets reaches above a pre-fixed threshold, an alarm is sent to the BS for preventing the further epidemic of the infected packet.

The spoofing can also be done at time by the legitimate nodes already deployed. The spoofing in this case can also be detected by the proposed methodology.

Since, the protocol protects the network using randomization concept, the attack not being identified is minimal. One scenario of attack was modeled in this paper, where a malicious node listens to the paradigm of the network and gets to know about the key ranges i.e. the keys are falling within the range (A, B), and puts header of the packet with those numbers and trailers with some random numbers. In this case, there are chances that the packet may pass the first verification stage, but the second stage clearance is difficult since the numbers in the headers has to undergo crossover, mutation and results has to match with the trailers. The results obtained for this scenario of attack is discussed in the fig. 4, fig.5, fig.6 fig. 7 and fig.8. Apart from this case, if the malicious node has to successfully spoof the packet in every attack, then it has to get the algorithmic and mathematical details burnt in the node, which is the case of a node capture attack. The protocol fails if the node undergoes a capture attack and the security details are hacked.

VI. SIMULATIONS

The algorithm was executed and tested using MATLAB 2013a on Intel core 5 Duo processor with windows operating system. CH requirement was set to 10% and the algorithm was verified on LEACH protocol till 1000 rounds. Table 1 contains the overhead in packet size due to the proposed security algorithm and table 2 depicts the various key sizes used for simulation. The parameters were set for modeling network environment is shown in table 3.

Table I. Bits overhead due to cryptographic framework (per communication)

Parameter	Value
Packet sent from BS to CHs	32 bits
Packet sent from CH to ordinary node	32 bits
Packet sent from end node to CH	32 bits
Packet sent from CH to BS	32 bits

Table II Key sizes used in packets for communication

Parameter	Size
p, q	1 byte each
MAC	2 bytes
m, n	1 byte each
k, v	1 byte each

Table III Radio characteristics and other parameters chosen for simulation

Parameter	Value
Number of nodes	100
Transmitter electronics, E_{tx}	50nJ/bit
Receiver electronics, E_{rx}	50nJ/bit
E_{mp}	0.0013pJ/bit
E_{fs}	10pJ/bit
E_{agg}	5nJ / bit
Length of plot	100 m
Width of plot	100 m
L_{pt} (packet sent from CH to BS)	6400 bits
L_{ctr} (packet sent from ordinary node to CH)	200 bits
Initial energy of the node	0.5 J

VII. RESULTS AND DISCUSSIONS

This section deals with the results obtained. The algorithm was tested on LEACH protocol. First six iterations are for analyzing the security, where number of rounds was limited to 100 in every iteration. Next, were again six iterations each with 500 rounds. In both cases, after every fifth round a malicious packet was made to spoof into the network, the probability of being identified is checked, and the graph is plotted. It was observed that in both the cases, the accuracy in identifying the malicious packets was 100% and is shown in fig. 5 and fig.7. In addition, in both the cases the number of

packets clearing first stage was plotted separately and is shown in fig.4 and fig.6. It was observed that even though the packets clear first stage, it was likely that they were caught in the second stage of verification; hence, the accuracy was always 100% and shows the robustness of the protocol in identifying the spoofed packets.

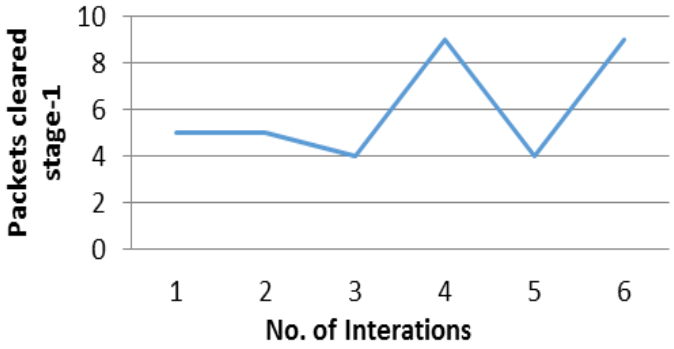

Fig. 4 count of spoofed packets identified for six iterations (each for 100 rounds of LEACH)

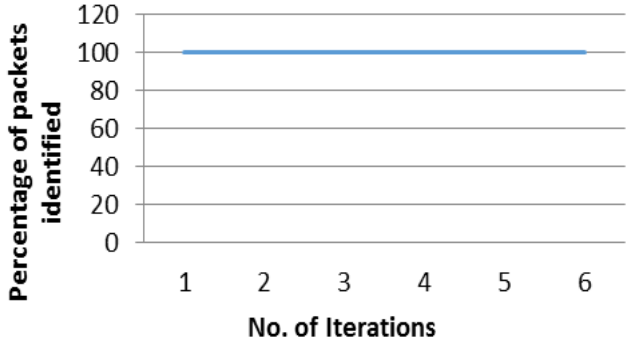

Fig. 5 Percentage of spoofed packets identified for six iterations (each for 100 rounds of LEACH)

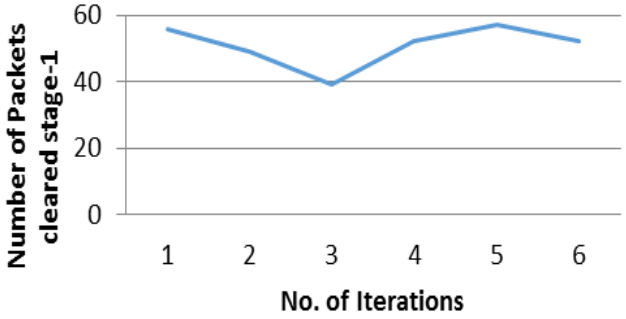

Fig. 6 Percentage of spoofed packets identified (each iteration with 500 rounds of LEACH)

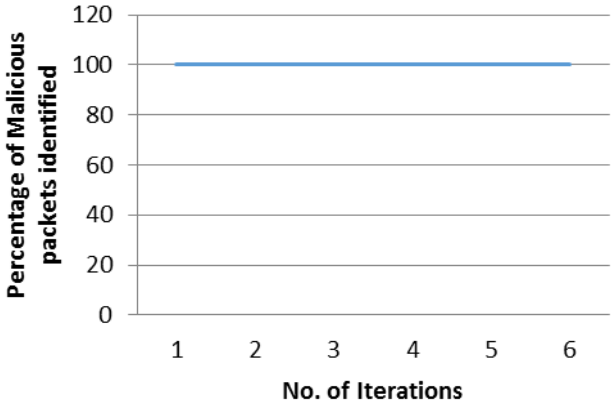

Fig. 7 Percentage of spoofed packets identified (each iteration with 500 rounds of LEACH)

The obtained results prove that the technique is robust in providing security in the network, serves as an improvement over author's previous work [1], and is shown in fig. 8. It was observed from fig.8 that due to the increase in the randomness via finding a random crossover point, less packets were able to clear verification stage-1 same was observed from the plots of fig.9.

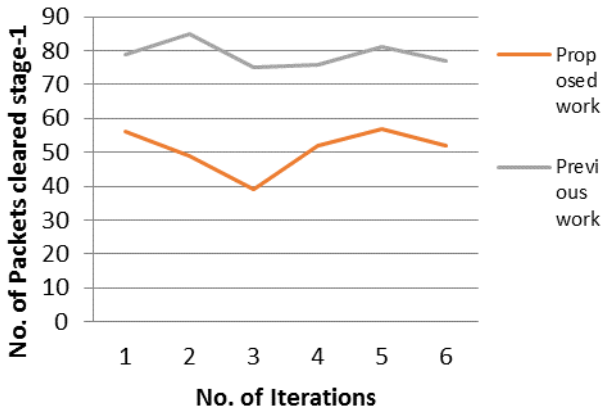

Fig. 8 Reduction in the number of packets clearing stage-1 (each iteration with 500 rounds of LEACH)

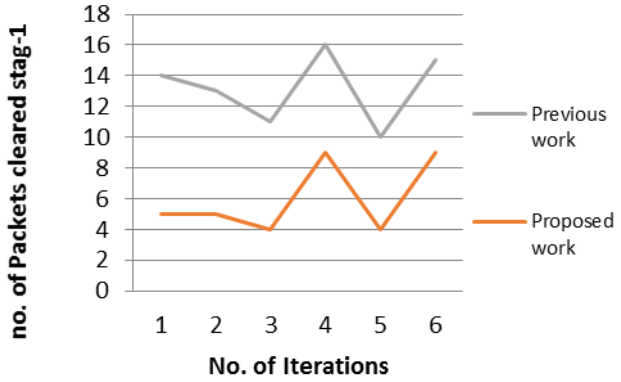

Fig. 8 Reduction in the number of packets clearing stage-1 (each iteration with 100 rounds of LEACH)

VIII. CONCLUSIONS

Security in WSNs has always been a difficult task in WSN to address due to the versatility in attacks and the complexity in handling them. In this context, we propose a Security Framework based on Memetics for Clustered Wireless Sensor Networks. It was observed 100 % accuracy in identifying the spoofed packets, since every packet has to undergo a double verification stage to get through into the network. Compared to our previous work more randomness was added with respect to the choice of the mutation point that reduced the number of packets clearing the first stage, thereby increasing the robustness of the technique. It can be concluded that more is the randomness more will be the technique robust in identifying the spoofed packets. The obtained results prove that the algorithm can be implemented in the future networks with an ease.

REFERENCES

[1] Suman S.B, P.V Ranjith Kumar, E. Sandeep Kumar, **"** Random Keying technique for Security in Wireless Sensor Networks based on Memetics", *International Journal of Computer Science: Theory and Applications (IJCSTA)*, vol. 1 (2), May 2014, Paris, France.

[2] P.V Ranjith Kumar, Sandeep P Nemagoud, Sandeep Kumar E and Vijaya Kumar B P, "A Novel Security Framework based on Genetics for Clustered Wireless Sensor Networks", International Journal of Computer Applications (IJCA), 96(5):8-13, June 2014, Published by Foundation of Computer Science, New York, USA.

[3] Sandeep Kumar E, Kusuma S.M, Vijaya Kumar B.P, "Random Key Distribution based Artificial Immune System for Security in Clustered Sensor Networks", IEEE conference, SCEECS-2014, March 1-2, Bhopal.

[4] Sandeep Kumar E, Kusuma S.M, Vijaya Kumar B.P, "An Intelligent Defense Mechanism for Security in Wireless Sensor Networks", *IEEE conference*, ICCSP-2014, April 3-5, Tamil Nadu.

[5] Chuan- Kang Ting, Chien- Chih Liao, "A Memetic Algorithm for extending Wireless Sensor Network lifetime", *Journal of Information Sciences*, Vol. 180(24), Dec 2010, pp 4818- 4833, Elsevier.

[6] Konstantinos P. Ferentinos, Theodore A. Tsiligiridis, "A Memetic Algorithm for Optimal Dynamic Design of Wireless Sensor Networks", *Journal of Computer Communications*, Vol. 33(2), 2010, pp 250-258.

[7] Wendi Rabiner Heinzelman, Anantha Chandrakasan, Hari Balakrishnan, "Energy-Efficient Communication Protocol for Wireless Microsensor Networks", *Proc. of* 33rd Hawaii International Conference on System Sciences – 2000, IEEE.

[8] Susan Blackmore, " The power of Memes", Scientific American, Oct. 2000, pp. 65- 73.

[9] Concepts of memetics from site nature- inspired algorithms h*ttp://www.cleveralgorithms.com/natureinspired/physical/memetic_algorithm.html*

[10] Few information regarding memetics is obtained from : http*://pespmc1.vub.ac.be/MEMES.html*

