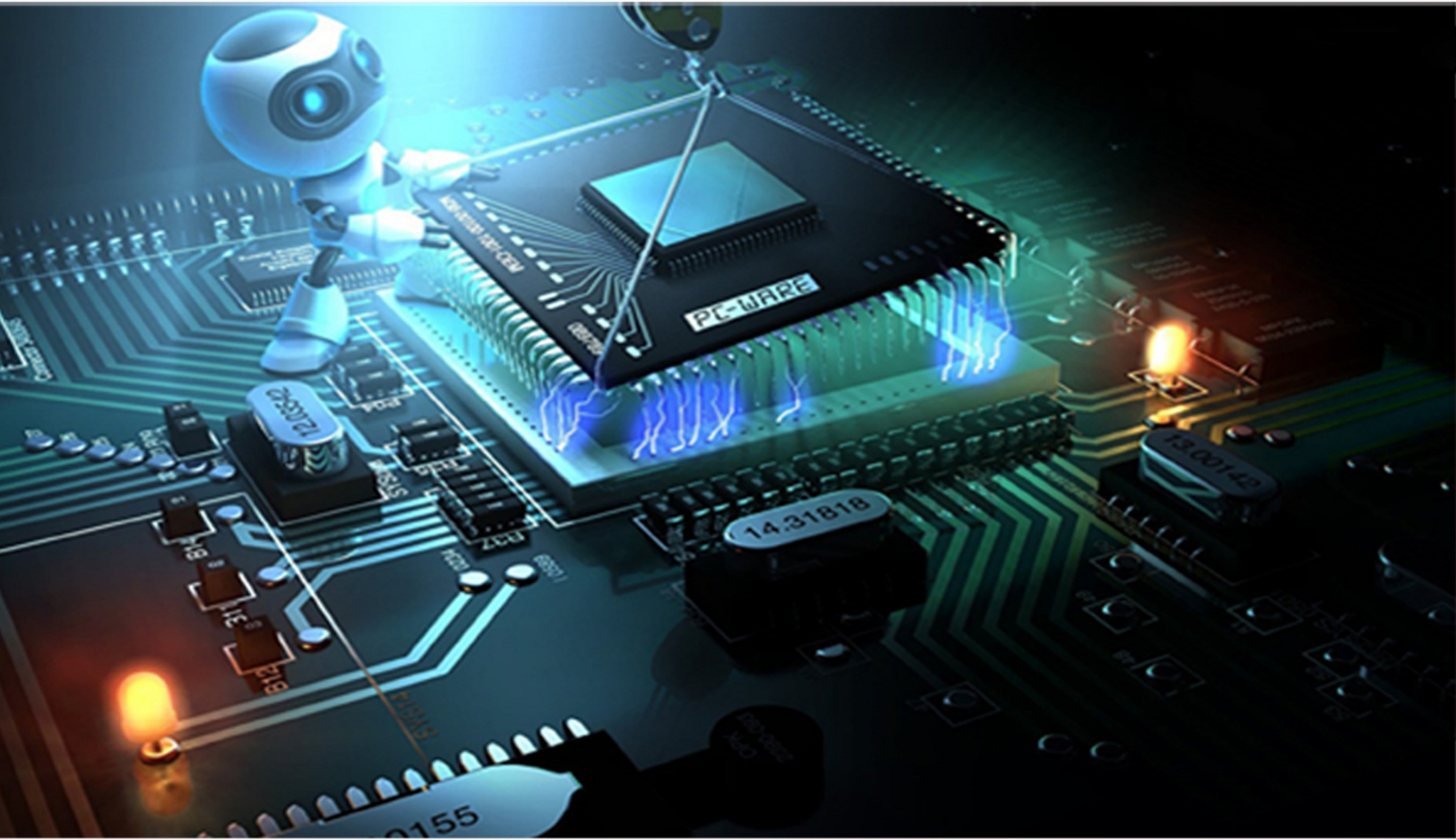
ISSN: 2054-7390

Volume 7 No 3, June 2019

Transactions on Machine Learning and Artificial Intelligence



Society for Science and Education
UNITED KINGDOM

TABLE OF CONTENTS

EDITORIAL ADVISORY BOARD

DISCLAIMER

All the contributions are published in good faith and intentions to promote and encourage research activities around the globe. The contributions are property of their respective authors/owners and the journal is not responsible for any content that hurts someone’s views or feelings etc.

SOCIETY FOR SCIENCE AND EDUCATION
UNITED KINGDOM

TMLAI TRANSACTIONS ON
MACHINE LEARNING AND ARTIFICIAL INTELLIGENCE

Volume 7 No 3
ISSN 2054-7390

Ten Artificial Human Optimization Algorithms

[1]Satish Gajawada, [2]Hassan M.H. Mustafa
[1]Alumnus, Indian Institute of Technology Roorkee
Founder and Father of Artificial Human Optimization Field
[2]Faculty of Specified Education, Dept. of Educational Technology,
Banha University, Egypt
Grand Father of Artificial Human Optimization Field
satish.gajawada.iit@gmail.com; prof.dr.hassanmoustafa@gmail.com

ABSTRACT

The term "Artificial Human Optimization" was first coined by the corresponding author of this work in December 2016 when he published a paper titled "Entrepreneur : Artificial Human Optimization" at Transactions on Machine Learning and Artificial Intelligence (TMLAI) Volume 4, No 6 (December 2016). According to that paper published in 2016, Artificial Human Optimization Field is defined as the collection of all those optimization algorithms which were proposed based on Artificial Humans. In real world we (Humans) solve the problems. In the same way Artificial Humans imitate real Humans in the search space and solve the optimization problems. In Particle Swarm Optimization (PSO) the basic entities in the solution space are Artificial Birds where as in Artificial Human Optimization the basic entities in search space are Artificial Humans. Each Artificial Human corresponds to a point in the solution space. Ten Artificial Human Optimization methods titled "Human Bhagavad Gita Particle Swarm Optimization (HBGPSO)", "Human Poverty Particle Swarm Optimization (HPPSO)", "Human Dedication Particle Swarm Optimization (HuDePSO)", "Human Selection Particle Swarm Optimization (HuSePSO)", "Human Safety Particle Swarm Optimization (HuSaPSO)", "Human Kindness Particle Swarm Optimization (HKPSO)", "Human Relaxation Particle Swarm Optimization (HRPSO)", "Multiple Strategy Human Particle Swarm Optimization (MSHPSO)", "Human Thinking Particle Swarm Optimization (HTPSO)", "Human Disease Particle Swarm Optimization (HDPSO)" are applied on various benchmark functions and results obtained are shown in this work.

Keywords: Computational Intelligence, Evolutionary Computing, Artificial Humans, Artificial Human Optimization, Particle Swarm Optimization, Genetic Algorithms, Hybrid Algorithms, Global Optimization Techniques, Nature Inspired Computing, Bio-Inspired Computing, Artificial Intelligence, Machine Learning

Highlights:

1) World's First Hybrid PSO algorithm based on Human Bhagavad Gita is designed in this work.
2) World's First Hybrid PSO algorithm based on Human Poverty is designed in this work.
3) World's First Hybrid PSO algorithm based on Human Dedication is designed in this work.
4) World's First Hybrid PSO algorithm based on Human Selection is designed in this work.

DOI: 10.14738/tmlai.73.6631
Publication Date: 21st June, 2019
URL: http://dx.doi.org/10.14738/tmlai.73.6631

5) The concept of Money is introduced into Particle Swarm Optimization algorithm for the first time in research industry history to create a new Hybrid PSO algorithm which comes under Artificial Human Optimization Field.
6) Ten Hybrid PSO algorithms which come under Artificial Human Optimization Field are shown in this work.

1 Introduction

The goal of 'Human Optimization' is to increase the performance of real humans through various methods. But 'Artificial Human Optimization' is a new field which took its birth recently in December 2016 as explained in abstract of this paper. This new filed is a sub-field of Evolutionary Computing which in turn is a sub-field of Computational Intelligence field. Hence 'Human Optimization (Real Human Optimization)' is different from Artificial Human Optimization (AHO).

The following is the review obtained from an expert in 2013 for a work under AHO Field. The review is shown below in double quotes as it is:

"The motivation of the paper is interesting. But the paper does not present any evaluation of the proposed algorithm. So we have an idea but we are not able to assess it on the basis of the paper. Next, there seems to be a difference between birds, fishes, ants, bacteria, bees etc. on one side, and human beings on the other side. Birds, fishes, ants, bacteria, bees etc. are more or less the same. People are different. I dare say that taxi drivers are different from politicians, or preschool teachers for example. Some people prefer money or power than love. It is not so difficult to guess which way ants will go but it is not so obvious when we consider people behavior. In my opinion the paper is a very first step to build the algorithm assumed but still lots of work is needed to achieve the goal."

The algorithms under Artificial Human Optimization Field (AHO Field) were proposed in literature starting from year 2003. But from the above review it is clear that the expert felt there are no algorithms under Artificial Human Optimization Field as on 2013 and corresponding author's work is the very first step. Experts are very familiar with Genetic Algorithms, Particle Swarm Optimization, Ant Colony Optimization etc but according to corresponding author's observation many experts are unaware of the fact that there are algorithms under AHO Field before 2013. Even corresponding author of this work felt that his work submitted for review in 2013 is the beginning of Artificial Human Optimization Field Algorithms. But this was a mistake and it was corrected in later papers. It is also clear from above review shown in double quotes that imitating Humans and creating Evolutionary Computing algorithms is not as easy as imitating beings Birds, fishes, ants, bacteria, bees etc and creating algorithms under Evolutionary Computation domain.

In this work the focus is on creating new AHO Field algorithms by modifying Particle Swarm Optimization (PSO) algorithm. Articles [1-7] give an overview of existing PSO algorithms and other details. Artificial Human Optimization Algorithms that are created by modifying PSO algorithm were shown in [8-12]. Articles [13-25] gives complete details related to Artificial Human Optimization Field and its algorithms. Benchmark Functions used in this paper are taken from [26].

The rest of the article is organized as follows:

Section 2 shows Particle Swarm Optimization algorithm. Section 3 to Section 12 shows "Human Bhagavad Gita Particle Swarm Optimization (HBGPSO)", "Human Poverty Particle Swarm Optimization (HPPSO)", “Human Dedication Particle Swarm Optimization (HuDePSO)”, “Human Selection Particle Swarm Optimization (HuSePSO)”, “Human Safety Particle Swarm Optimization (HuSaPSO)”, “Human Kindness Particle Swarm Optimization (HKPSO)”, “Human Relaxation Particle Swarm Optimization (HRPSO)”, “Multiple Strategy Human Particle Swarm Optimization (MSHPSO)”, “Human Thinking Particle Swarm Optimization (HTPSO)”, “Human Disease Particle Swarm Optimization (HDPSO)” respectively. Results are explained in Section 13. Section 14 gives Conclusions.

2 Particle Swarm Optimization

Particle Swarm Optimization (PSO) was proposed by Kennedy and Eberhart in 1995. PSO is based on Artificial Birds. It has been applied to solve complex optimization problems.

In PSO, first we initialize all particles as shown below. Two variables $pbest_i$ and gbest are maintained. $pbest_i$ is the best fitness value achieved by i^{th} particle so far and gbest is the best fitness value achieved by all particles so far. Lines 4 to 11 in the below text helps in maintaining particle best and global best. Then the velocity is updated by rule shown in line no. 14. Line 15 updates position of i^{th} particle. Line 19 increments the number of iterations and then the control goes back to line 4. This process of a particle moving towards its local best and also moving towards global best of particles is continued until termination criteria will be reached.

Procedure: Particle Swarm Optimization (PSO)

```
1) Initialize all particles
2) iterations = 0
3) do
4)      for each particle i do
5)          If ( f( $x_i$ ) < f( $pbest_i$ ) ) then
6)              $pbest_i = x_i$
7)          end if
8)          if ( f( $pbest_i$ ) < f( gbest ) ) then
9)              gbest = $pbest_i$
10)         end if
11)     end for
12)     for each particle i do
13)         for each dimension d do
14)             $v_{i,d} = w*v_{i,d} +$
                    $C_1*Random(0,1)*(pbest_{i,d} – x_{i,d})$
                  $+ C_2*Random(0,1)*(gbest_d – x_{i,d})$
15)             $x_{i,d} = x_{i,d} + v_{i,d}$
17)         end for
18)     end for
19)     iterations = iterations + 1
20) while ( termination condition is false)
```

3 Human Bhagavad Gita Particle Swarm Optimization

Bhagavad Gita is a Hindu sacred text. There are no Hybrid PSO algorithms based on Bhagavad Gita till date. According to Bhagavad Gita “He who is successful is not ideal. He who failed is not ideal. Only he is ideal and revered who irrespective of success or failure stands steadfast in the pursuit of his mission”. Human Bhagavad Gita Particle Swarm Optimization (HBGPSO) is designed based on this fact.

The population consists of ideal and non ideal candidates. Based on random number generated and IdealCandidateProbability, the human is classified into either ideal or non ideal candidate. Ideal candidate is not affected by success or failure and he moves in search space without any halt. So velocity and position are always updated as shown in line number 15 and 16 irrespective of anything. But this is not the case for non ideal candidate. Based on random number generated and SuccessProbability, non-ideal candidate is classified to facing either success or failure. Non ideal candidate will not update velocity and position and moves into halted state when he faces failure as shown in line number 25. He updates velocity and position when he faces success as shown in line number 21 and 22. Hence failure or success is not a matter for ideal candidate. But non ideal candidate will stop progress when he faces failure.

Procedure: Human Bhagavad Gita Particle Swarm Optimization (HBGPSO)

```
1) Initialize all particles
2) iterations = 0
3) do
4)      for each particle i do
5)          If ( f( $x_i$ ) < f( $pbest_i$ ) ) then
6)              $pbest_i = x_i$
7)          end if
8)          if ( f( $pbest_i$ ) < f( gbest ) ) then
9)              gbest = $pbest_i$
10)         end if
11)     end for
12)     for each particle i do
13)         if ( random(0,1) < IdealCandidateProbability ) then // ideal candidate
14)             for each dimension d do
15)                 $v_{i,d} = w*v_{i,d} +$
                    $C_1*Random(0,1)*(pbest_{i,d} – x_{i,d})$
                    $+ C_2*Random(0,1)*(gbest_d – x_{i,d})$
16)                 $x_{i,d} = x_{i,d} + v_{i,d}$
17)             end for
18)         else // non ideal candidate
19)             if ( random(0,1) < SuccessProbability) then
20)                 for each dimension d do
21)                     $v_{i,d} = w*v_{i,d} +$
                        $C_1*Random(0,1)*(pbest_{i,d} – x_{i,d})$
                        $+ C_2*Random(0,1)*(gbest_d – x_{i,d})$
22)                     $x_{i,d} = x_{i,d} + v_{i,d}$
23)                 end for
24)             else // non ideal candidate with failure
25)                 // non ideal candidate with failure doesnot update position and velocity
26)             end if
27)         end if
28)     end for
29)     iterations = iterations + 1
30) while ( termination condition is false)
```

4 Human Poverty Particle Swarm Optimization

There are no Hybrid PSO algorithms based on Human Poverty till date. The population consists of Rich Humans and Poor Humans. Based on random number generated and RichCandidateProbability, the human is classified into either Rich or Poor. Rich Humans have enough money to move in the search space without any halt. So velocity and position are always updated as shown in line number 15 and 16 irrespective of anything. But this is not the case for poor Humans. Based on random number generated and DonationsProbability, Poor Human is classified to having enough money to move in the search space or having insufficient money. Poor Human will not update velocity and position and moves into halted state when he doesn't have enough money as shown in line number 25. He updates velocity and position when he gets donations and has enough money to travel in search space as shown in line number 21 and 22. Hence money is not a matter for Rich Human. But Poor candidate will stop progress when he did not get sufficient money to travel in search space.

Procedure: Human Poverty Particle Swarm Optimization (HPPSO)

```
1) Initialize all particles
2) iterations = 0
3) do
4)      for each particle i do
5)          If ( f( $x_i$ ) < f( $pbest_i$ ) ) then
6)              $pbest_i = x_i$
7)          end if
8)          if ( f( $pbest_i$ ) < f( gbest ) ) then
9)              gbest = $pbest_i$
10)         end if
11)     end for
12)     for each particle i do
13)         if ( random(0,1) < RichCandidateProbability ) then // rich candidate
14)             for each dimension d do
15)                 $v_{i,d} = w*v_{i,d} +$
                    $C_1*Random(0,1)*(pbest_{i,d} – x_{i,d})$
                    $+ C_2*Random(0,1)*(gbest_d – x_{i,d})$
16)                 $x_{i,d} = x_{i,d} + v_{i,d}$
17)             end for
18)         else // poor candidate
19)             if ( random(0,1) < DonationsProbability) then // poor candidate gets donations
20)                 for each dimension d do
21)                     $v_{i,d} = w*v_{i,d} +$
                        $C_1*Random(0,1)*(pbest_{i,d} – x_{i,d})$
                        $+ C_2*Random(0,1)*(gbest_d – x_{i,d})$
22)                     $x_{i,d} = x_{i,d} + v_{i,d}$
23)                 end for
24)             else
25)                 // poor candidate with no donations doesnot update position and velocity
26)             end if
27)         end if
28)     end for
```

```
29)     iterations = iterations + 1
30) while ( termination condition is false)
```

5 Human Dedication Particle Swarm Optimization

There are no Hybrid PSO algorithms based on Human Dedication till date. Based on random number generated and HumanDedicationProbability, Human is classified into either Dedicated Human or Non Dedicated Human. Dedicated Humans move faster in search space by having a high dedication factor of 0.9 as shown in line number 16. But Non Dedicated Humans have a low dedication factor of 0.1 and move slower in search space than Dedicated Humans as shown in line number 21.

Procedure: Human Dedication Particle Swarm Optimization (HuDePSO)

```
1) Initialize all particles
2) iterations = 0
3) do
4)      for each particle i do
5)          If ( f( $x_i$ ) < f( $pbest_i$ ) ) then
6)              $pbest_i = x_i$
7)          end if
8)          if ( f( $pbest_i$ ) < f( gbest ) ) then
9)              gbest = $pbest_i$
10)         end if
11)     end for
12)     for each particle i do
13)         if ( rand(0,1) < HumanDedicationProbability) // dedicated humans
14)             for each dimension d do
15)                 $v_{i,d} = w*v_{i,d} +$
                        $C_1*Random(0,1)*(pbest_{i,d} – x_{i,d})$
                        $+ C_2*Random(0,1)*(gbest_d – x_{i,d})$
16)                 $x_{i,d} = x_{i,d} + 0.9 * v_{i,d}$
17)             end for
18)         else // non-dedicated humans
19)             for each dimension d do
20)                 $v_{i,d} = w*v_{i,d} +$
                        $C_1*Random(0,1)*(pbest_{i,d} – x_{i,d})$
                        $+ C_2*Random(0,1)*(gbest_d – x_{i,d})$
21)                 $x_{i,d} = x_{i,d} + 0.1 * v_{i,d}$
22)             end for
23)         end if
24)     end for
25)     iterations = iterations + 1
26) while ( termination condition is false)
```

6 Human Selection Particle Swarm Optimization

There are no Hybrid PSO algorithms based on Human Selection till date. There are 2 options to select from for Humans. Either Humans move towards local best position or they move towards global best position. Based on random number generated and HumanSelectionProbability, Humans select from 2 options available. If random number generated is less than HumanSelectionProbability then Human move towards local best as shown in line number 15. Otherwise, Human move towards global best position as shown in line number 20.

Procedure: Human Selection Particle Swarm Optimization (HuSePSO)

```
1) Initialize all particles
2) iterations = 0
3) do
4)      for each particle i do
5)           If ( $f(x_i) < f(pbest_i)$ ) then
6)                $pbest_i = x_i$
7)           end if
8)           if ( $f(pbest_i) < f(gbest)$ ) then
9)                $gbest = pbest_i$
10)          end if
11)     end for
12)     for each particle i do
13)          if ( rand(0,1) < HumanSelectionProbability) // moves towards local best
14)               for each dimension d do
15)                    $v_{i,d} = w*v_{i,d} +$
                            $C_1*Random(0,1)*(pbest_{i,d} – x_{i,d})$
16)                    $x_{i,d} = x_{i,d} + v_{i,d}$
17)               end for
18)          else // moves towards global best
19)               for each dimension d do
20)                    $v_{i,d} = w*v_{i,d} +$
                            $C_2*Random(0,1)*(gbest_d – x_{i,d})$
21)                    $x_{i,d} = x_{i,d} + v_{i,d}$
22)               end for
23)          end if
24)     end for
25)     iterations = iterations + 1
26) while ( termination condition is false)
```

7 Human Safety Particle Swarm Optimization

Please see [25], to understand Human Safety Particle Swarm Optimization (HuSaPSO). The code for HuSaPSO is shown below.

Procedure: Human Safety Particle Swarm Optimization (HuSaPSO)

```
1) Initialize all particles
2) iterations = 0
3) do
4)      for each particle i do
5)           If ( $f(x_i) < f(pbest_i)$ ) then
6)                $pbest_i = x_i$
7)           end if
8)           if ( $f(pbest_i) < f(gbest)$ ) then
9)                $gbest = pbest_i$
10)          end if
```

```
    end for
    for each particle i do
        for each dimension d do
            $v_{i,d} = w*v_{i,d} +$
              $C_1*Random(0,1)*( x_{i,d} - pworst_{i,d})$
             $+ C_2*Random(0,1)*( x_{i,d} - gworst_d)$
            $x_{i,d} = x_{i,d} + v_{i,d}$
        end for
    end for
    iterations = iterations + 1
while ( termination condition is false)
```

8 Human Kindness Particle Swarm Optimization

Please see [25], to understand Human Kindness Particle Swarm Optimization (HKPSO). The code for HKPSO is shown below.

Procedure: Human Kindness Particle Swarm Optimization (HKPSO)

```
Initialize all particles
iterations = 0
do
    for each particle i do
        If ( f( $x_i$ ) < f( $pbest_i$ ) ) then
            $pbest_i = x_i$
        end if
        if ( f( $pbest_i$ ) < f( gbest ) ) then
            gbest = $pbest_i$
        end if
    end for
    for each particle i do
        for each dimension d do
            $v_{i,d} = w*v_{i,d} +$
              $C_1*Random(0,1)*(pbest_{i,d} - x_{i,d})$
             $+ C_2*Random(0,1)*(gbest_d - x_{i,d})$
            $x_{i,d} = x_{i,d} + KindnessFactor_i * v_{i,d}$
        end for
    end for
    iterations = iterations + 1
while ( termination condition is false)
```

9 Human Relaxation Particle Swarm Optimization

Please see [25], to understand Human Relaxation Particle Swarm Optimization (HRPSO). The code for HRPSO is shown below.

Procedure: Human Relaxation Particle Swarm Optimization (HRPSO)

```
Initialize all particles
Initialize RelaxationProbability
iterations = 0
do
    for each particle i do
```

```
        If ( f( $x_i$ ) < f( $pbest_i$ ) ) then
            $pbest_i = x_i$
        end if
        if ( f( $pbest_i$ ) < f( gbest ) ) then
            gbest = $pbest_i$
        end if
    end for
    for each particle i do
        if  Random(0,1) < = RelaxationProbability
            continue   // continues to next particle
        end if
        for each dimension d do
            $v_{i,d} = w*v_{i,d} +$
                $C_1$*Random(0,1)*($pbest_{i,d} - x_{i,d}$)
                + $C_2$*Random(0,1)*($gbest_d - x_{i,d}$)
            $x_{i,d} = x_{i,d} + v_{i,d}$
        end for
    end for
    iterations = iterations + 1
while ( termination condition is false)
```

10 Multiple Strategy Human Particle Swarm Optimization

Please see [25], to understand Multiple Strategy Human Particle Swarm Optimization (MSHPSO). The code for MSHPSO is shown below.

Procedure: Multiple Strategy Human Particle Swarm Optimization (MSHPSO)

```
Initialize all particles
iterations = 0
do
    for each particle i do
        If ( f( $x_i$ ) < f( $pbest_i$ ) ) then
            $pbest_i = x_i$
        end if
        if ( f( $pbest_i$ ) < f( gbest ) ) then
            gbest = $pbest_i$
        end if
        If ( f( $x_i$ ) > f( $pworst_i$ ) ) then
            $pworst_i = x_i$
        end if
        if ( f( $pworst_i$ ) > f( gworst ) ) then
            gworst = $pworst_i$
        end if
    end for
    If ((iterations == 0) || (iterations%2==0)) then
          // for starting and even iterations
        for each particle i do
            for each dimension d do
                $v_{i,d} = w*v_{i,d} +$
                    $C_1$*Random(0,1)*($pbest_{i,d} - x_{i,d}$)
                    +$C_2$*Random(0,1)*($gbest_d - x_{i,d}$)
                $x_{i,d} = x_{i,d} + v_{i,d}$
            end for
        end for
    else // for odd iterations
        for each particle i do
            for each dimension d do
                $v_{i,d} = w*v_{i,d} +$
                    $C_1*Random(0,1)*( x_{i,d} - pworst_{i,d} )$
                    $+ C_2*Random(0,1)*( x_{i,d} - gworst_d)$
                $x_{i,d} = x_{i,d} + v_{i,d}$
            end for
        end for
    end if
    iterations = iterations + 1
while ( termination condition is false)
```

11 Human Thinking Particle Swarm Optimization

Please see [25], to understand Human Thinking Particle Swarm Optimization (HTPSO). The code for HTPSO is shown below.

Procedure: Human Thinking Particle Swarm Optimization (HTPSO)

```
Initialize all particles
iterations = 0
do
    for each particle i do
        If ( f( $x_i$ ) < f( $pbest_i$ ) ) then
            $pbest_i = x_i$
        end if
        if ( f( $pbest_i$ ) < f( gbest ) ) then
            gbest = $pbest_i$
        end if
        If ( f( $x_i$ ) > f( $pworst_i$ ) ) then
            $pworst_i = x_i$
        end if
        if ( f( $pworst_i$ ) > f( gworst ) ) then
            gworst = $pworst_i$
        end if
    end for
    for each particle i do
        for each dimension d do
            $v_{i,d} = w*v_{i,d} + Random(0,1)*(pbest_{i,d} – x_{i,d}) + Random(0,1)*(gbest_d – x_{i,d})$
            $v_{i,d} = v_{i,d} + Random(0,1)*( x_{i,d} - pworst_{i,d} ) + Random(0,1)*( x_{i,d} - gworst_d)$
            $x_{i,d} = x_{i,d} + v_{i,d}$
        end for
    end for
    iterations = iterations + 1
```

```
while (termination condition is false)
```

12 Human Disease Particle Swarm Optimization

Please see [25], to understand Human Disease Particle Swarm Optimization (HDPSO). The code for HDPSO is shown below.

Procedure: Human Disease Particle Swarm Optimization (HDPSO)

```
Initialize all particles
iterations = 0
do
    for each particle i do
        If ( f( $x_i$ ) < f( $pbest_i$ ) ) then
            $pbest_i = x_i$
        end if
        if ( f( $pbest_i$ ) < f( gbest ) ) then
            gbest = $pbest_i$
        end if
    end for

    If ((iterations == 0) || (iterations%2==0)) then
          // for starting and even iterations
        for each particle i do
            for each dimension d do
              $v_{i,d} = w*v_{i,d} +$
                $C_1*Random(0,1)*(pbest_{i,d} – x_{i,d})$
                $+C_2*Random(0,1)*(gbest_d – x_{i,d})$
              $x_{i,d} = x_{i,d} + v_{i,d}$
            end for
        end for
    else // for odd iterations
        for each particle i do
            for each dimension d do
              $v_{i,d} = w*v_{i,d} +$
                $C_1*Random(0,1)*( x_{i,d} - pbest_{i,d} )$
                $+ C_2*Random(0,1)*( x_{i,d} - gbest_d )$
              $x_{i,d} = x_{i,d} + v_{i,d}$
            end for
        end for
    end if
    iterations = iterations + 1
while ( termination condition is false)
```

13 Results

Ten Artificial Human Optimization methods titled “Human Bhagavad Gita Particle Swarm Optimization (HBGPSO)”, “Human Poverty Particle Swarm Optimization (HPPSO)”, “Human Dedication Particle Swarm Optimization (HuDePSO)”, “Human Selection Particle Swarm Optimization (HuSePSO)”, “Human Safety Particle Swarm Optimization (HuSaPSO)”, “Human Kindness Particle Swarm Optimization (HKPSO)”, “Human Relaxation Particle Swarm Optimization (HRPSO)”, “Multiple Strategy Human Particle Swarm Optimization (MSHPSO)”, “Human Thinking Particle Swarm Optimization (HTPSO)”, “Human Disease

Particle Swarm Optimization (HDPSO)” are applied on Ackley, Beale, Bohachevsky, Booth and Three-Hump Camel Benchmark Functions and results obtained are shown in this section. The Figures of benchmark functions are taken from [26].

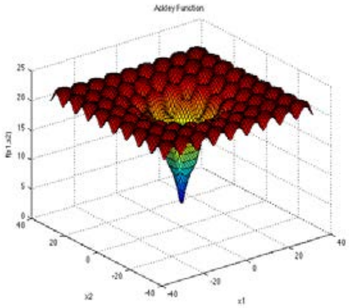


Figure 1. Ackley Function

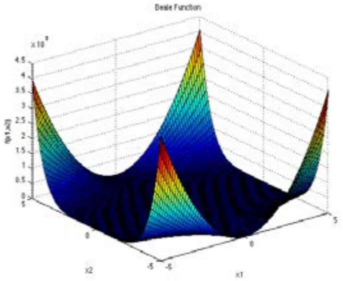


Figure 2. Beale Function

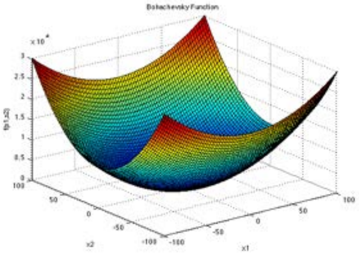


Figure 3. Bohachevsky Function

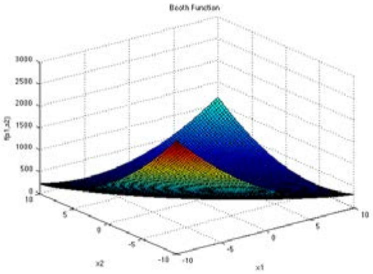


Figure 4. Booth Function

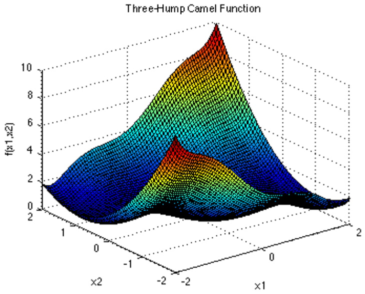
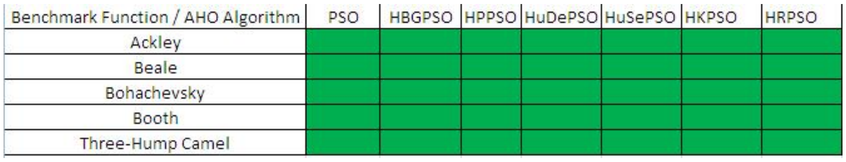
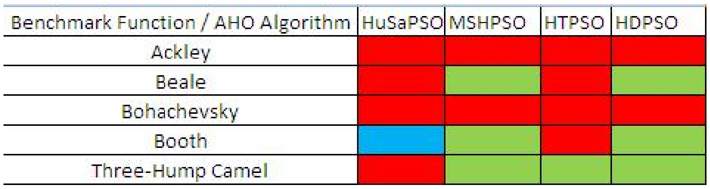


Figure 5. Three-Hump Camel Function



Benchmark Function / AHO Algorithm	PSO	HBGPSO	HPPSO	HuDePSO	HuSePSO	HKPSO	HRPSO
Ackley	🟩	🟩	🟩	🟩	🟩	🟩	🟩
Beale	🟩	🟩	🟩	🟩	🟩	🟩	🟩
Bohachevsky	🟩	🟩	🟩	🟩	🟩	🟩	🟩
Booth	🟩	🟩	🟩	🟩	🟩	🟩	🟩
Three-Hump Camel	🟩	🟩	🟩	🟩	🟩	🟩	🟩

Figure 6. Overall Result Part One



Benchmark Function / AHO Algorithm	HuSaPSO	MSHPSO	HTPSO	HDPSO
Ackley	🟥	🟥	🟥	🟥
Beale	🟥	🟩	🟥	🟩
Bohachevsky	🟥	🟥	🟥	🟥
Booth	🟦	🟩	🟥	🟩
Three-Hump Camel	🟥	🟩	🟩	🟩

Figure 7. Overall Result Part Two

In Figure 6 and Figure 7, first row shows AHO algorithms and first column shows benchmark functions. Green represents “Performed Well”. Red represents “Didn’t Performed Well”. Blue represents “Performed Between Well and Not Well”.

From Figure 6 it is clear that HBGPSO, HPPSO, HuDePSO, HuSePSO, HKPSO, HRPSO and PSO Performed Well for all benchmark functions.

From Figure 7 it can be observed that HuSaPSO didn’t perform well even on single benchmark function. MSHPSO and HDPSO performed well on three benchmark functions. HTPSO performed well on only single benchmark function.

14 Conclusions

Artificial Human Optimization Algorithms (AHO Algorithms) inspired by Bhagavad Gita (HBGPSO), Human Poverty (HPPSO), Human Dedication (HuDePSO) and Human Selection (HuSePSO) are proposed in this work. Ten AHO algorithms are applied on 5 benchmark functions and results obtained are shown in this work. Six AHO algorithms performed as good as PSO algorithm where as remaining four AHO algorithms didn’t performed as good as PSO. HuSaPSO performed worst among all algorithms used in this work. All algorithms designed in this work performed as good as PSO. A general misunderstanding among people is that algorithms inspired by Humans will perform better than other algorithms inspired by other beings. For example, let algorithm A is inspired by Birds and Algorithm B is inspired by Humans. Then because of misunderstanding, it will lead to conclusion that Algorithm B performs better than Algorithm A because Humans are best beings and most intelligent beings on this planet. In this work, we have found that HuSaPSO inspired by Humans did not performed well even on single benchmark function where as PSO inspired by birds performed well on all benchmark functions. Our future work is to design “Human Cricket Particle Swarm Optimization (HCPSO)”, “Human Farming Particle Swarm Optimization (HFPSO)” inspired by Human Cricket game and Human Farming respectively. Artificial Human Optimization Algorithms designed from scratch will also be part of our future work.

ACKNOWLEDGEMENTS

Authors would like to thank the following editorial members of TMLAI for accepting innovative works under Artificial Human Optimization Field:

Professor Er Meng Joo, School of Electrical and Electronic Engineeringt, Nanyang Technological University, Singapore

Professor Djamel Bouchaffra, Department of Mathematics and Computer Science, Grambling State University, Louisiana., United States

Prof Bhavani Thuraisingham, Department of Computer Science, Erik Jonsson School of Engineering and Computer Science, The University of Texas at Dallas, United States

Professor Dong-Hee Shin, Department of Interaction Science, Social Computing Institute, Sungkyunkwan University, Seoul, Korea, Republic of

Professor Filippo Neri, Professor of Computer Information Systems, Faculty of Information & Communication Technology, Dar Guzeppi Zahra, University of Malta, Malta

REFERENCES

[1] Saptarshi Sengupta, Sanchita Basak, Richard Alan Peters II. Particle Swarm Optimization: A survey of historical and recent developments with hybridization perspectives. https://arxiv.org/abs/1804.05319, 2018.

[2] Yudong Zhang, Shuihua Wang, and Genlin Ji, "A Comprehensive Survey on Particle Swarm Optimization Algorithm and Its Applications," Mathematical Problems in Engineering, vol. 2015, Article ID 931256, 38 pages, 2015. https://doi.org/10.1155/2015/931256.

[3] M. R. AlRashidi, M. E. El-Hawary. A Survey of Particle Swarm Optimization Applications in Electric Power Systems. IEEE Transactions on Evolutionary Computation. Volume 13, Issue 4, August 2009.

[4] Sharandeep Singh. A Review on Particle Swarm Optimization Algorithm. International Journal of Scientific & Engineering Research, Volume 5, Issue 4, April-2014.

[5] T. Saravanan and V. Srinivasan. Overview of Particle Swarm Optimization. Indian Journal of Science and Technology, Vol 8(32), November 2015.

[6] Muhammad Imran, Rathiah Hashim, Noor Elaiza Abd Khalid.An Overview of Particle Swarm Optimization Variants. Procedia Engineering. Elsevier.Volume 53, Pages 491-496, 2013.

[7] Riccardo Poli, James Kennedy, Tim Blackwell. Particle swarm optimization - An overview. Swarm Intelligence. Volume 1, Issue 1, pp 33–57, Springer, 2007.

[8] Liu H, Xu G, Ding GY, Sun YB, "Human behavior-based particle swarm optimization", The Scientific World Journal, 2014.

[9] Ruo-Li Tang, Yan-Jun Fang, "Modification of particle swarm optimization with human simulated property", Neurocomputing, Volume 153, Pages 319–331, 2015.

[10] Muhammad Rizwan Tanweer, Suresh Sundaram, "Human cognition inspired particle swarm optimization algorithm", 2014 IEEE Ninth International Conference on Intelligent Sensors, Sensor Networks and Information Processing (ISSNIP), 2014.

[11] M.R. Tanweer, S. Suresh, N. Sundararajan, "Self regulating particle swarm optimization algorithm", Information Sciences: an International Journal, Volume 294, Issue C, Pages 182-202, 2015.

[12] M. R. Tanweer, S. Suresh, N. Sundararajan, "Improved SRPSO algorithm for solving CEC 2015 computationally expensive numerical optimization problems", 2015 IEEE Congress on Evolutionary Computation (CEC), pp. 1943-1949, 2015.

[13] Satish Gajawada. "POSTDOC : The Human Optimization", Computer Science & Information Technology (CS & IT), CSCP, pp. 183-187, 2013.

[14] Satish Gajawada. "CEO: Different Reviews on PhD in Artificial Intelligence", Global Journal of Advanced Research, vol. 1, no.2, pp. 155-158, 2014.

[15] Satish Gajawada. "Entrepreneur: Artificial Human Optimization". Transactions on Machine Learning and Artificial Intelligence, Volume 4 No 6 December (2016); pp: 64-70

[16] Satish Gajawada. “Artificial Human Optimization – An Introduction”, Transactions on Machine Learning and Artificial Intelligence, Volume 6, No 2, pp: 1-9, April 2018

[17] Satish Gajawada. “An Ocean of Opportunities in Artificial Human Optimization Field”, Transactions on Machine Learning and Artificial Intelligence, Volume 6, No 3, June 2018

[18] Satish Gajawada. “25 Reviews on Artificial Human Optimization Field for the First Time in Research Industry”, International Journal of Research Publications, Vol. 5, no. 2, United Kingdom.

[19] Satish Gajawada and Hassan M. H. Mustafa, “Collection of Abstracts in Artificial Human Optimization Field”, International Journal of Research Publications, Volume 7, No 1, United Kingdom, 2018.

[20] Satish Gajawada, Hassan M. H. Mustafa, HIDE : Human Inspired Differential Evolution - An Algorithm under Artificial Human Optimization Field , International Journal of Research Publications (Volume: 7, Issue: 1), http://ijrp.org/paper-detail/264

[21] Satish Gajawada, Hassan M. H. Mustafa , Artificial Human Optimization – An Overview. Transactions on Machine Learning and Artificial Intelligence, Volume 6, No 4, August 2018.

[22] Satish Gajawada, Hassan M. H. Mustafa, Testing Multiple Strategy Human Optimization based Artificial Human Optimization Algorithms, Computer Reviews Journal, vol. 1, no.2, 2018.

[23] Satish Gajawada, Hassan M. H. Mustafa. Hybridization Concepts of Artificial Human Optimization Field Algorithms Incorporated into Particle Swarm Optimization. *International Journal of Computer Applications* 181(19):10-14, September 2018.

[24] Satish Gajawada, Hassan M. H. Mustafa (2018). An Artificial Human Optimization Algorithm Titled Human Thinking Particle Swarm Optimization. *International Journal of Mathematical Research*, 7(1): 18-25. DOI: 10.18488/journal.24.2018.71.18.25

[25] Satish Gajawada, Hassan Mustafa: Novel Artificial Human Optimization Field Algorithms - The Beginning. CoRR abs/1903.12011(2019)

[26] https://www.sfu.ca/~ssurjano/optimization.html

SOCIETY FOR SCIENCE AND EDUCATION
UNITED KINGDOM
TMLAI TRANSACTIONS ON
MACHINE LEARNING AND ARTIFICIAL INTELLIGENCE
Volume 7 No 3
ISSN 2054-7390

Two Factor Authentication Framework Using OTP-SMS Based on Blockchain

[1] Eman T Alharbi, [2] Daniyal Alghazzawi
[1,2] Department of Information System, Faculty of Computing and information technology, King Abdulaziz University, Jeddah, Saudi Arabia;
Etalharbi0125@stu.kau.edu.sa; dghazzawi@kau.edu.sa

ABSTRACT

The authentication process is the main step which should be used to confirm that the user is the legitimate one and give the access only for him. Recently, Two Factor Authentication (2FA) schemes have been used by most of the applications to add an extra layer of security on the login process and solve the vulnerabilities of using only one factor for authentication. OTP-SMS is one of the most common methods which has been used in 2FA. However, attackers found a way to attack this method and gain an access to the user's account without their permission. In this paper, we proposed a new 2FA framework for OTP-SMS method to prevent different attacks, mainly Man In The Middle (MITM) attack and third party attack. The proposed framework is based on the use of Blockchain technology, which add more security and better environment for authentication process. The proposed framework uses an encrypted OTP, which generated by smart contract and uses also its hash value to send it to the application/website to complete the authentication process. We introduced a comparison between our proposed framework and other two frameworks which uses Blockchain to secure OTP-SMS. Our framework found to be secure against MITM and third party attacks and the computation time and complexity are less than other frameworks.

Keywords: Two Factor Authentication, One Time Password, Blockchain, Smart Contract, Ethereum, Man in the Middle Attack, Third Party.

1 Introduction

Authentication is a method and technique that used to construct an association among two parties. This association depends on confidence and certainty that the two parties are the authentic parties to establish the association (connection). The most common authentication method is based on the using of password, which is used on various services, like on social networking, bank accounts, and different website and applications. However, there are many ways to hack the secret password, and the easy ones can be attacked without the need for extensive computation. The best way to prevent password attacks is to add more security and make the authentication process more complex.

One of the most common approaches which used to increase the security of authentication is the use of two factor instead of using only one. Two factor Authentication (2FA) schemes was introduced to overcome the weakness of single password authentication scheme and strength the security side by deploying a second authentication factor. There are several different methods that are applicable to be used in 2FA. The main categories of authentication are [1]:

DOI: 10.14738/tmlai.73.6524
Publication Date: 30th June, 2019
URL: http://dx.doi.org/10.14738/tmlai.73.6524

1. Something you are (user's biometric like fingerprint, voice recognition, retina scanning)
2. Something you know (Password and PIN codes)
3. Something you have (mobile phone, ID card, or an Electronic card)

2FA method requires proving two instances of a knowledge factor (e.g., password, inherent biometric features or generating One Time Password). Using messages based on One Time Password (OTP-SMS) is the most common method of second factor which used in 2FA scheme, as shown in Figure.1. OTP-SMS has been widely deployed in many applications which need an extra layer of security, for example, web based banking and login verification in social media applications [2].

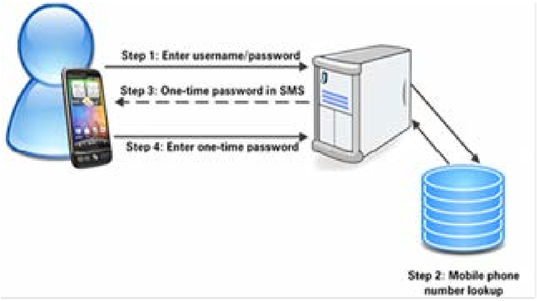

Step 1: Enter username/password
Step 3: One-time password in SMS
Step 4: Enter one-time password
Step 2: Mobile phone number lookup

Fig.1. OTP-SMS as Second Factor of 2FA [3]

There are so many advantages of 2FA method, but attackers were working on breaking this method and they found many ways to hack it and reveal the sensitive information of the users. Breaking 2FA requires the attacker to execute only a single type of malicious action, but multiple times in more contexts – for example, extracting a password (e.g., by a keylogger) and extracting a private token of an application generating OTPs (e.g., by malware). We thus see a need for research on more secure 2FA scheme, specially OTP-SMS, that can withstand today's sophisticated adversary models. In this paper, we explore authentication framework that use Blockchain as a second authentication process instead of the generation of OTP by the third parties. Such approach could eliminate the inherent weaknesses of existing OTP-SMS schemes and preventing the attacks which could reveal the authentication process.

The remaining of this paper is organized as the following: Section II introduces a discussion of the attacks on 2FA scheme, Section III discuss the background and preliminaries, section IV introduce the related work, Section V introduces the proposed framework, Section VI introduces a discussion and finally section VII introduce a conclusion of the work.

2 Attacks on Two Factor Authentication Schemas

Most two-factor authentication (2FA) methods are adopted with online applications or website services, where one-time password (OTP) is created when clients sign in with their username and password. A client gets the OTP by means of a SMS on their enlisted phone number and enters it on the site to finish the login step. While 2FA is a positive enhancement for plain password authentication, it isn't trustworthy [4]. There are many attacks can be occur on 2FA scenario and break down the authentication process.

Jesudoss and Subramaniam [5] introduced an extensive study that investigate and analyze different possible attacks on authentication aspects of security and they placed about 11 possible attack which can reveal a password for attacker . In addition, Certic [6] introduced another study to present forensic evidences that there is a serious breach in the 2FA authentication model, and he confirmed 4 of the attacks that referred by [5]. Moreover, Dmitrienko et.al [2] introduced a study that investigate the security vulnerabilities of the mobile 2FA of many service providers including Dropbox, Google authenticator and twitter. They show that the used mobile 2FA schema has many weakness and attacker can bypass the authentication process simply by intercepting the OTP or capturing the cookies session which can be used for regeneration OTP.

The following is a list of the most common attacks that can reveal 2FA scheme and release the user's credentials:

2.1 Man in the middle attack

A man in the middle (MITM) attack is a general term when an attacker eavesdrops or impersonates one of the parties by positioning himself between two hosts, i.e. website/application and user to steal personal information (e.g. login credential, credit card information). The communication appears as a normal exchange of information, but all the communication between them goes only through the attacker, as shown in Figure.2. So attackers can change, copy or erase the whole or a part of the data traffic between parties. MITM might be used to simply monitor the data (passive attack) or modify it (active attack) [7].

Typically, MITM attack targets the users of financial or e-commerce sites, which require logging in information. 2FA can be revealed by MITM attack, which can tricke the user to visit a fake website, which exactly looks like the legitimate one. The user enters his login information into the fake site, then the attacker get these information and enter them to the legitimate site, which at that point sends an OTP to the user. The user does not have any idea about this movement and he will enters the OTP in the fake site and the attacker sends them to the legitimate site, which allow him to gain full access to the account without anyone's knowledge.

Secure Socket layer (SSL) is one of the main solutions for MITM, which encrypt the traffic and make it impossible to tamper or modify any of the transferred information between two parties [8]. However, using SSL is not enough because there are ways to fake it (by proxy servers), so that the user think that he have a secure connection while he navigated to a non-SSL site. To overcome any revealing or altering in user information, Blockchain technology can be used and an encryption by using the use's public key for OTP should applied. Moreover, the hashed value of OTP can be sent instead of the real value. If the attacker alter the data, then the received hash will be different and the authentication will be failed.

2.2 Session Hijacking

Session Hijacking attack is the abuse of user session, which acquired from his site, to steal his critical information. This attack can occur between a Web server and a Web browser by exploiting the cookies of TCP session. This TCP session contains tokens (in http request header), which including a sign for authentication that sent by the web server to the browser. The attacker can gain an unauthorized access by using this stolen tokens [10]. This attack is common in Web applications. However, even by using 2FA the attacker still able to perform this kind of attack. To overcome this problem, SSL Secure protocol combined with cookie management system should be used.

2.3 Third party

In the two-factor authentication systems, the generation and verification of the second factor tokens is done by the third party, which considered as a part of the authentication scheme. Any third-party authentication mechanism is based on the security of the vendors or carriers who generate the second factor token. OTP-SMS authentication process is based on the mobile carrier's practices which assign and reuse phone numbers. If the mobile phone is lost or the attackers convince the carrier that they are the true user and they their phone has been lost, they can intercept phone calls and SMS messages, and get access to the OTP tokens [11]. Nowadays, some applications have been requested to stop using OTP-SMS as a second factor in the authentication process. To overcome this problem, the generation of the second factor should be managed through a decentralized authority which can be implemented securely by using Blockchain technology.

2.4 Account recovery

The attacker is searching for the weakest point in the authentication system to attack. When the user loses the first factor of authentication (or if an attacker pretends to), i.e. password, the two-factor authentication process will be temporarily disabled. In this case, the attacker might be able to social engineer the account recovery process to get access to the account. Moreover, the knowledge-based authentication which used in the account recovery process to ask user for secret question provide much worse security and makes the attacking easier as these answers are often very easy to guess.

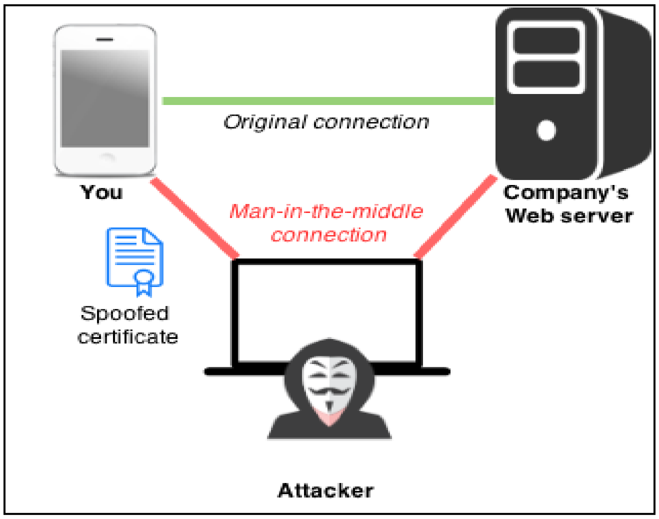


Fig. 2. Man In The Middle Attack Scenario [9]

3 Background and Preliminaries

In order to understand how blockchain can solve the vulnerabilities of 2FA, we have to understand what is Blockchain, how it works and what are its characteristics.

3.1 Blockchain Definition

A blockchain is a distributed database that uses the technology of distributed ledger that preventing the forgery of data records by arbitrary manipulation. Blockchain is a special instance of Distributed Ledger Technologies (DLTs) that records transactions of any value or asset securely. The transaction can be for any type of value between independent parties using a peer-to-peer network, without a central administrator.

3.2 How Blockchain Works

In a blockchain, blocks are linked using a cryptographic hash function, which called Merkle tree, and each new block has to be agreed upon by special participant's node called miners which running a consensus protocol. Each block contains various transactions, which are the interactions between client and Blockchain. These transactions may contain either orders transferring crypto-tokens or calls of smart contract functions, and each one linked with the sender's signature and receiver's public key. The smart contract is a written code for special applications and can encode arbitrary processing logic (e.g., agreements) written in a supported language. All transactions sent to a blockchain are validated by miners who maintain a replicated state of the blockchain. To incentivize miners, blockchain platforms introduce reward and fee schemes. The way how Blockchain is working is displayed and tagged in Figure.3.

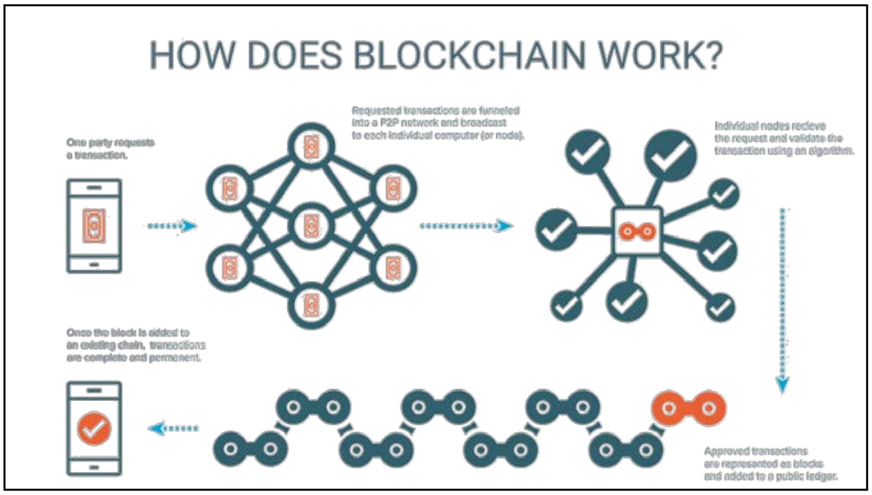

HOW DOES BLOCKCHAIN WORK?
One party requests a transaction.
Requested transactions are funneled into a P2P network and broadcast to each individual computer (or node).
Individual nodes recieve the request and validate the transaction using an algorithm.
Approved transactions are represented as blocks and added to a public ledger.
Once the block is added to an existing chain, transactions are complete and permanent.

Fig.3. The way of how Blockchain is working [12]

3.3 Different functionality of nodes in Blockchain

Blockchain is composed of many nodes which create the network itself. These nodes are different and each one has its own functionality. Here we briefly discuss the types of nodes and what are the functions of each type:

- Routing (minimum functionality)
    - Used to discover and connect to other peers in the network, validate and propagate transactions and blocks).
    - Its purpose is to keep the network alive and passing information through the network.
- Storage (full functionality)
    - Store local copy of the blockchain database.
    - Can autonomously and authoritatively verify any transactions without any external references.
- Mining (minor)
    - Runs special mining software to solve a cryptography puzzle to win mining reward.
    - Its purpose is adding the verified transactions to the blockchain.
    - Doesn't necessary to have local copy from the database, they depend on a pool server to get the required information.
- Wallet (simplified payment verification)

- Good for devices with limited storage, security, and power.
- Rely on other trustworthy full node to provide necessary information.

3.4 The Advantages of Blockchain

The blockchain has a number of advantages compared to a traditional centralized system. These advantages including transparency, security, efficiency, and resilience [1], [13].

- Transparency: sharing the resources between all the participated nodes in Blockchain is done in a straightforward fashion and the use of these resources is open by default.
- Security: hacker intrusions can cause catastrophic damage in the centralized data management. However, the case in Blockchain is entirely unexpected and data falsification is almost impossible because hackers need to control all the nodes which contains the distributed data to change any information.
- Efficiency: It is easy to follow the data blocks and get its information in Blockchain. Even if many nodes were participated, the complex processes of system integration can be bypassed.
- Resilience: Centralized data management have a single point of failure (SPOF), while Blockchain does not have SPOF as its devices are decentralized and all data is shared equally between the participated nodes. It is unlikely to receive malicious threats in Blockchain, even if some nodes subject to execution corruption or mistakes.

3.5 Ethereum and Smart Contracts

Ethereum is a platform that provides a customized blockchain to build applications in a distributed environment. It connects each party directly to reach zero-dependency and better transparency. It works on the client-server model and located in the middle of decentralizing computer system.

Smart contracts are programs which created to perform a specific execution. They can be encoded on any blockchain system, Ethereum is the most favoured choice since it gives adaptable handling abilities and allow the programmers to edit and code them as they need [1]. Smart contracts can be used to do the following: managing agreements between users, triggering a claim automatically if certain events occur, and store application's data like health data record.

4 Related Work

Blockchain is an emerging technology that has been used in widely in resent researches. The use of Blockchain in authentication process become an active area and there are many researchers proposed special frameworks to show how this technology can adopted and changes the authentication models to be better than the existed ones. Lin et.al [14] proposed a framework for smart factory which used Blockchain to authenticate the employees in the factory before allowing them to use any device. Ethereum smart contract had been used to request transaction which signed by the employee's private key. The transaction is validated by decrypting it, using public key for employee, and then allow him to use the device. The proposed framework provides the security that guarantee confidentiality, auditability, and authenticated access to each device. The proposed framework was evaluated, and its security were proved.

In addition, Homoliak et.al [15] proposed 2FA framework which based on the use of a smart-contract cryptocurrency wallet. It consists of three components (i.e., an authenticator, a client, and a smart contract). The proposed framework provides a secure, usable, and flexible way of managing crypto-tokens in a self-sovereign fashion. The authentication process performed by generating one-time passwords (OTPs) by pseudo random function and then aggregate it by a Merkle tree. They proved that this framework is secure against the man-in-machine and quantum cryptanalysis attacks.

Moreover, Park et.al [16] propose 2FA framework to solve the problem of the private Blockchain which is hyperledger. The proposed framework based on the use of TOTP (time based one-time password) which generates a password using the current time information and the secret key shared by a TOTP server and a user. This OTP is generated by the membership function, which is a part of the private Blockchain, based on the user authority. The application will provide the authentication and access for the user when receive the OTP, which is sent to the application rather than send it directly to the user, which guarantee a high level of authentication.

The use of Blockchain with IoT infrastructure can address the issues that confronting the advancement of IoT engineering and security. Wu et.al [17] proposed 2FA framework for out-of-band IoT devices based on Blockchain infrastructure. The implementation of the framework integrates the Blockchain system with multiple devices to simulate IoT infrastructure. All the devices were registered in the Blockchain and each device is connected with the nearest device that able to authenticate each other based on the relationship which stored in the Blockchain nodes. The request for authentication is sent from a devise to the related device which checks in the Blockchain if this device is related and has the ability to authenticate it. This scheme was able to prevent the attack of external malicious devices, even if the adversary was able to steel the first token.

These related works are summarized with their strategies and the problems which solved in Table 1.

Table 1. The Related Work with Their Strategy and Solved Problems

Framework	Strategy	Solved problem
BSeIn: Blockchain for Authentication and Access control for Smart Factory [14]	Authenticate users of factory devices and guarantee secure transactions by using private key to sign the request. The Blockchain smart contract used for authentication process to and to keep tracing of records and connect various factories together.	Secure mutual authentication and provide fine-grained access control.
Smart-contract cryptocurrency wallet framework [15]	Managing crypto-tokens in a secure and flexible way using 2FA based on Blockchain. OTP is generated by the authenticator and aggregated by Merkle tree of Blockchain.	Secure against the man-in-machine and quantum cryptanalysis attacks
OTP Authentication Scheme for Hyperledger Fabric Blockchain [16]	Using 2FA based on Blockchain which generate OTP by the membership function of Hyperledger Blockchain. OTP token is sent to the application rather than directly to the user and then used to access the desired service and make it available to the user.	Prevent third party attack.
An Out-of-band Authentication Scheme for Internet of Things Using Blockchain Technology [17]	2FA based on Blockchain for devices in IoT network. The authentication steps are: checking the related device in the nearest node then send a verification code to activate the device. Blockchain were used to store the relationships between devices and give access to the related device only.	Preventing single point of failure, and provide secure, reliable and flexible access to the devices of IoT network.

5 The Proposed Framework

The OTP-SMS security and management have turned out to be critical with the recent rise of cyber-attacks. We propose OTP-SMS for 2FA framework based on Blockchain smart-contract to overcome the vulnerabilities of using original OTP which based on using a central authority. The proposed framework gives a flexible, usable, and secure way of generating and validating SMS-OTP which is encrypted and secured against most of the common attacks, which are MITM and third party attacks. The components of our proposed framework are including web application, user, and Ethereum smart contract. The authentication is performed in two stages: the first by providing the username and password to the desired application/website, and the second is by decrypting the OTP which is generated and sent via a smart contract which requested by web application to authorize the user, where the blocks of records are stored in an ever-growing public distributed ledger called a blockchain, which is resistant by design against modifications.

The following steps are descrying how this framework works, as shown in Figure.4:

1. User logs into application/website with the combination of username-password.
2. The application/website asks the user to send a transaction to their Ethereum 2FA contract. The user should be at least a wallet node in the used Blockchain to be able to send contracts and encrypt/decrypt any message. A reasonable waiting time is set for an authenticated event, then login is rejected if no authenticated event is heard for this user's Ethereum address or if the timeout.
3. User sends a transaction to the Ethereum 2FA contract.
4. a. Ethereum checks the validity of the user request through checking the integrity of his transaction with the website/application.

   b. If the request is valid, Ethereum 2FA contract generate OTP.

   c. Ethereum 2FA contract encrypts OTP by user's public key then send it to the user.

   d. Ethereum 2FA contract computes the hash value of OTP and sent it to the website/application (H1).
5. a. User decrypt the OTP and compute its hash (H2), and send the hash value to the website/application.

   b. Website/application compare the received hash values (H1 form smart contract and H2 form user) to ensure integrity of the user and there is no any alteration on the OTP. If the two values are equal and the process still within the waiting time, Website/application provide the access to the user.

6 Discussion

We proposed a novel framework to provide two factor authentication which based on the use of OTP-SMS. The proposed framework is introducing a solution for the greatest attack which thread the OTP-SMS two factor authentication scheme, mainly the Man In The Middle Attack (MITM) and third party attack. The encapsulation of the OTP message through encrypt it using user's public key makes such attack impossible and keep the data save. Moreover, the using of hash value by the website/application to authenticate the users instead of the original OTP is s novel method which has not been exposed in researches to our knowledge.

In this section we will compare our proposed framework with the frameworks which introduced by Homoliak et.al in [15] and Park et.al [16]. The comparison is summarized in Table 2.

Homoliak et.al in [15] framework was based on the use of pseudo random function to generate the OTP at the authenticator side (which is the website/application), and send it in plain text to the smart contract in the Blockchain. This step makes it possible for attacker to perform his MITM attack as the OTP is not encrypted while send it through network. Moreover, the computation of the root value, which used later for authentication process, is complex and consuming long time, as multiple OTPs should be generated from the original one, then compute their hash values, and aggregate these values to compute the root value to send it to the user for authentication purpose. The use of hashed value make it impossible for altering the OTP, but in the first place sending the OTP as plain text make this framework still vulnerable for attacks.

Similarly, Park et.al [16] framework solved the problem of third authority attack by generating the OTP via membership function of the Blockchain. However, the OTP is sent as pain text which make it vulnerable to MITM attack. In addition to this attack, there is no any mean to ensure that the OTP is the same generated one and no alteration is performed on it, which considered as another vulnerability in that framework.

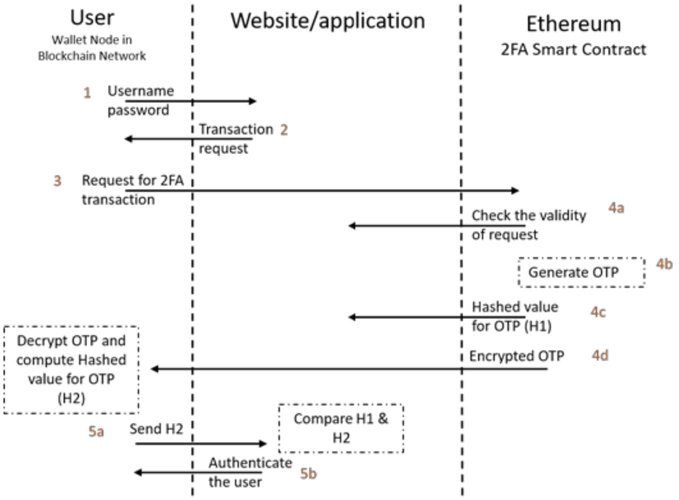

User
Wallet Node in Blockchain Network
Website/application
Ethereum
2FA Smart Contract
1 Username password
Transaction 2 request
3 Request for 2FA transaction
Check the validity of request 4a
Generate OTP 4b
Hashed value for OTP (H1) 4c
Decrypt OTP and compute Hashed value for OTP (H2)
Encrypted OTP 4d
5a Send H2
Compare H1 & H2
Authenticate the user 5b

Fig. 4. The proposed 2FA based on Blockchain Framework

Table 2. Comparison between the Proposed Framework and other two frameworks.

Attribute	Our Proposed Framework	Homoliak et.al [15]	Park et.al [16]
Used authentication factor	OTP	OTP	OTP
Complexity of computation	Easy	Complex	Easy
Time of computation	Low	High	Low
MITM attack	Secure	Not Secure	Not Secure
Third party attack	Secure	Secure	Secure
Alteration on OTP	Secure	Secure	Not Secure

7 Conclusion

In this paper, we introduced OTP-SMS framework as a second factor of the authentication process. Our framework based on using the Blockchain technology to add extra layer of security and solve the vulnerabilities in the login process. We used Ethereum smart contract to generate OTP instead of a third party, and encrypt this OTP with the public key of the user, meanwhile, it sends the hash value to the requested website/application. The user will decrypt the received OTP by his private key and then compute the hash value and send it to the website/ application. The website/ application will authenticate the user after comparing the received hash values from both entities. These processes are preventing MITM attack from getting access to the OTP or altering its value. Moreover, the Blockchain solve the problem of third party attack as well. Our framework provides more security for users in less time and low computation power. For future work, we plan to implement this framework with real applications and prove its ability to preventing different attacks and measure the exact time which required for authentication.

REFERENCES

[1]. R. Gupta, Hands-on cybersecurity with blockchain: implement DDoS protection, PKI-based identity, 2FA, and DNS security using blockchain. 2018.

[2]. A. Dmitrienko, C. Liebchen, C. Rossow, and A.-R. Sadeghi, “Security Analysis of Mobile Two-Factor Authentication Schemes,” vol. 18, no. 4, p. 24, 2014.

[3]. “Setup two-factor authentication with OTP sent as SMS.” [Online]. Available: http://www.sms-integration.com/setup-two-factor-authentication-with-otp-sent-as-sms-80.html. [Accessed: 30-Mar-2019].

[4]. “Do two-factor authentication vulnerabilities outweigh the benefits?,” SearchSecurity. [Online]. Available: https://searchsecurity.techtarget.com/answer/Do-two-factor-authentication-vulnerabilities-outweigh-the-benefits. [Accessed: 18-Mar-2019].

[5]. A. Jesudoss and N. P. Subramaniam, “A Survey on Authentication Attacks and Countermeasures in A Distributed Environment,” Indian J. Comput. Sci. Eng. IJCSE, vol. 5, no. 2, pp. 71–77, 2014.

[6]. S. Certic, “Two-Factor Authentication Vulnerabilities,” SSRN Electron. J., 2018.

[7]. “What is MITM (Man in the Middle) Attack.” [Online]. Available: https://www.incapsula.com/web-application-security/man-in-the-middle-mitm.html. [Accessed: 19-Mar-2019].

[8]. C. Onwubiko and A. P. Lenaghan, “Managing Security Threats and Vulnerabilities for Small to Medium Enterprises,” in 2007 IEEE Intelligence and Security Informatics, 2007, pp. 244–249.

[9]. “Man in the Middle Attack | How Can You Prevent MITM Attack?,” Comodo Securebox. [Online]. Available: https://securebox.comodo.com/ssl-sniffing/man-in-the-middle-attack. [Accessed: 30-Mar-2019].

[10]. I. Dacosta, S. Chakradeo, M. Ahamad, and P. Traynor, “One-Time Cookies: Preventing Session Hijacking Attacks with Disposable Credentials,” Georgia Institute of Technology, Technical Report, 2011.

[11]. “Five Most Common Security Attacks on Two-Factor Authentication.” [Online]. Available: https://www.itbusinessedge.com/slideshows/five-most-common-security-attacks-on-two-factor-authentication.html. [Accessed: 18-Mar-2019].

[12]. S. Shankland, “Why should you care about blockchain? It’s the ultimate trust builder,” CNET. [Online]. Available: https://www.cnet.com/news/blockchain-explained-builds-trust-when-you-need-it-most/. [Accessed: 30-Mar-2019].

[13]. Z. Gao et al., “Blockchain-based Identity Management with Mobile Device,” in Proceedings of the 1st Workshop on Cryptocurrencies and Blockchains for Distributed Systems - CryBlock’18, Munich, Germany, 2018, pp. 66–70.

[14]. C. Lin, D. He, X. Huang, K.-K. R. Choo, and A. V. Vasilakos, “BSeIn: A blockchain-based secure mutual authentication with fine-grained access control system for industry 4.0,” J. Netw. Comput. Appl., vol. 116, pp. 42–52, Aug. 2018.

[15]. I. Homoliak, D. Breitenbacher, A. Binder, and P. Szalachowski, “An Air-Gapped 2-Factor Authentication for Smart-Contract Wallets,” ArXiv181203598 Cs, Dec. 2018.

[16]. W.-S. Park, D.-Y. Hwang, and K.-H. Kim, “A TOTP-Based Two Factor Authentication Scheme for Hyperledger Fabric Blockchain,” in 2018 Tenth International Conference on Ubiquitous and Future Networks (ICUFN), Prague, 2018, pp. 817–819.

[17]. L. Wu, X. Du, W. Wang, and B. Lin, “An Out-of-band Authentication Scheme for Internet of Things Using Blockchain Technology,” in 2018 International Conference on Computing, Networking and Communications (ICNC), Maui, HI, 2018, pp. 769–773.

SOCIETY FOR SCIENCE AND EDUCATION
UNITED KINGDOM

TMLAI TRANSACTIONS ON
MACHINE LEARNING AND ARTIFICIAL INTELLIGENCE

Volume 7 No 3
ISSN 2054-7390

On Finding Geodesic Equation of Two Parameters Binomial Distribution

William W.S. Chen
Department of Statistics, The George Washington University
Washington D.C. 20013
williamwschen@gmail.com

ABSTRACT

The purpose of this paper is to find a general form of the geodesic equation of the binomial distribution. Using Darboux's theory we will set up a second order partial differential equation. Then we will apply the chain rule to transform the variable and rotate the axis to remove the interaction term, which will lead us to find the geodesic equation of binomial distribution. To illustrate how we can find such a geodesic equation in practice, we demonstrate by an example.

SOME KEY WORDS AND PHRASES: Bernoulli Trial, binomial distribution, Darboux Theory, differential geometry, geodesic equation, digamma function, Rotation axis, second order partial differential equation, trigamma function.

1 Introduction

A Bernoulli experiment is a random experiment, the outcome of which can be classified in but one of two mutually exclusive and exhaustive ways: success or failure. A sequence of Bernoulli trials occurs when a Bernoulli experiment is performed several independent times so that the probability of success, p, remains the same from trial to trial. We may let p denote the probability of success on each trial and let

q=1-p denote the probability of failure. In a sequence of Bernoulli trials, we are often interested in the total number of successes and are not interested in the order of this occurrence. If we let the random variable x equal the number of observed success in n Bernoulli trial, then n-x failure occur. The number of ways of selecting x positions for the x successes in the n trials is $\begin{pmatrix} n \\ x \end{pmatrix} = \frac{\text{n!}}{\text{x!(n-x)!}}$, and the probability of each of these ways is $\text{p}^{\text{x}}(1\text{-p})^{\text{n-x}}$ Thus, the probability density function of x is the sum of the probability of these $\begin{pmatrix} n \\ x \end{pmatrix}$ mutually exclusive events; $\text{f(x)} = \begin{pmatrix} n \\ \text{x} \end{pmatrix} \text{p}^{x}(1\text{-p})^{\text{n-x}},\ \text{x=0,1,...n}$ The random variable x is said to have binomial distribution. The constants n and p are called the parameters of the binomial distribution. "Are we alone in the galaxy?" The existence of life on Earth does not mean that the probability of life emerging once is equal to 1. When we roll a die and get a 6, the probability of getting

DOI: 10.14738/tmlai.73.6696
Publication Date: 30th June, 2019
URL: http://dx.doi.org/10.14738/tmlai.73.6696

the 6 does not change to 1, it remains 1/6. However, we do know that the probability of life emerging on a habitable planet is at least greater than zero. The binomial distribution tells us the probability of x=k successes in a series of Bernoulli trials. So, for n habitable planets, we can calculate the probability that x=k of these planets will host life, $\mathrm{f(x)}=\begin{pmatrix} n \\ \mathrm{x} \end{pmatrix}\mathrm{p}^{x}\mathrm{(1\text{-}p)^{n\text{-}x}}$ for k=0, we get $\mathrm{f(k{=}0)}=(1-p)^{n}$. The probability that life exists on at least one planet, $\mathrm{P(k\geq 0)}$ or $\mathrm{P(k\neq 0)}$, is equal to 1 minus the probability that life exists on zero planets, $\mathrm{P(k\neq 0){=}1\text{-}(1\text{-}p)^{n}}$.

To answer the question “are we alone?” What we really want to know is the probability that life exists on at least two planets; $\mathrm{P(k\geq 2){=}1\text{-}P(k{=}0)\text{-}P(k{=}1){=}1\text{-}(1\text{-}p)^{n}}-np(1-p)^{n-1}$. The probability

tells us, given n and p, the probability that two or more planets will host life. In this paper, we give out another useful result: geodesic equation.

2 List the Fundamental Tensor

The standard form of the two parameters binomial distribution has the probability density function given by,

$$\mathrm{f(x)}=\begin{pmatrix} n \\ \mathrm{x} \end{pmatrix}\mathrm{p}^{x}\mathrm{(1\text{-}p)^{n\text{-}x}}=\frac{\mathrm{n!}}{\mathrm{x!(n\text{-}x)!}}\mathrm{p^{x}(1\text{-}p)^{n\text{-}x}}$$

$$=\frac{\Gamma(n+1)}{\Gamma(x+1)\Gamma(n-x+1)}\mathrm{p}^{x}\mathrm{(1\text{-}p)^{n\text{-}x}} \qquad 0<\mathrm{p}<1,\quad \mathrm{x}=0,1,2,..\mathrm{n}$$

$$\ln \mathrm{f(x)}=\ln\Gamma(n+1)-\ln\Gamma(x+1)-\ln\Gamma(n-x+1)+x\ln p\ +\mathrm{(n\text{-}x)ln(1\text{-}p)} \qquad (2.1)$$

From the equation (2.1) above, we derive the basic metric tensor components for this distribution as follows,

$$\frac{\partial \ln f(x)}{\partial n}=\frac{\Gamma'(n+1)}{\Gamma(n+1)}\text{ - }\frac{\Gamma'(n-x+1)}{\Gamma(n-x+1)}+\mathrm{ln(1\text{-}p)}=\Psi\mathrm{(n{+}1)\text{-}}\Psi\mathrm{(n\text{-}x{+}1)}+\mathrm{ln(1\text{-}p)}$$

$$\frac{\partial^2 \ln f(x)}{\partial n^2}=\Psi'\mathrm{(n{+}1)\text{-}}\Psi'\mathrm{(n\text{-}x{+}1)} \qquad (2.2)$$

$$\frac{\partial^2 \ln f(x)}{\partial p\partial n}=\frac{-1}{1-p}; \qquad \frac{\partial \mathrm{lnf(x)}}{\partial \mathrm{p}}=\frac{x}{p}-\frac{n-x}{1-p} \qquad (2.3)$$

$$\frac{\partial^2\mathrm{lnf(x)}}{\partial \mathrm{p}^2}=\frac{-x}{p^2}-\frac{n-x}{(1-p)^2} \qquad (2.4)$$

Taking the negative expectation of equations (2.2),(2.3) and (2.4), we define the coefficient of the first fundamental form E, F, and G as follows:

$$E = -E(\frac{\partial^2 \ln f(x)}{\partial n^2}) = -\Psi^{'}(\text{n+1}) + \text{E}(\Psi^{'}(\text{n-}x+1)) = \lambda_x(\text{n,p}) \qquad (2.5)$$

$$\text{where } \lambda_{\text{x}}(n,p) = -\Psi^{'}(\text{n+1}) + \sum_{\text{x=0}}^{\text{n}} \Psi^{'}(\text{n-}x+1)\begin{pmatrix}\text{n}\\ \text{x}\end{pmatrix} p^x(1-p)^{n-x}$$

$$F = -E(\frac{\partial^2 \ln f(x)}{\partial p \partial n}) = \frac{1}{1-p}; \qquad (2.6)$$

$$\text{G} = -\text{E}(\frac{\partial^2 \ln f(\text{x})}{\partial p^2}) = \frac{np}{p^2} + \frac{n-np}{(1-p)^2} = \frac{n}{\text{p}(1-p)} \qquad (27)$$

Equations (2.5), (2.6) and (2.7) will be used to set up the partial differential equation in the next section.

3 The Geodesic Equation

In this section, we will find the geodesic equation of the binomial distribution by solving a second order partial differential equation. This idea originated from Darboux's**,** theory. We can set up $\nabla Z = 1$ as follows:

$$\frac{\text{EZ}_{\text{p}}^2 - 2FZ_nZ_p + GZ_n^2}{EG - F^2} = 1$$

$$\lambda_{\text{x}}(\text{n,p})\ \text{Z}_{\text{p}}^2\ - \frac{2}{1-p}\text{Z}_n\text{Z}_{\text{p}} + \frac{n}{\text{p}(1-p)}\text{Z}_n^2 \ = \ \frac{n\lambda_x(n,p)(1-p)-p}{\text{p}(1-p)^2} \qquad (3.1)$$

To solve the partial differential equation (3.1) above, we would consider the polar coordinate transformation. Let $\text{n} = \text{r}\cos\theta$, *and*

$\text{p} = \text{r}\sin\theta$, we should be aware of the fact that Z is a function (n, p) while both (n, p) are also functions of (r, θ). In calculus, we learn that the chain rule will give us the following results:

$$Z_r = \frac{\partial \text{Z}}{\partial \text{n}}\frac{\partial \text{n}}{\partial r} + \frac{\partial \text{Z}}{\partial \text{p}}\frac{\partial \text{p}}{\partial r} = Z_n\cos\theta + Z_p\sin\theta,$$

$$Z_\theta = \frac{\partial \text{Z}}{\partial \text{n}}\frac{\partial \text{n}}{\partial \theta} + \frac{\partial \text{Z}}{\partial \text{p}}\frac{\partial \text{p}}{\partial \theta} = Z_n(-r\sin\theta) + Z_p r\cos\theta, \qquad (3.2)$$

Using the Cramer Rule in equation (3.2), we can solve reversely for Z_{n} *and* Z_{p} as a function of Z_r *and* Z_θ as follows:

$$Z_n = \frac{\begin{vmatrix} Z_r & \sin\theta \\ Z_\theta & r\cos\theta \end{vmatrix}}{\begin{vmatrix} \cos\theta & \sin\theta \\ -r\sin\theta & r\cos\theta \end{vmatrix}} = \frac{r\cos\theta Z_r - \sin\theta Z_\theta}{r\cos^2\theta + r\sin^2\theta} = \cos\theta Z_r - \frac{1}{r}\sin\theta Z_\theta$$

$$Z_p = \frac{\begin{vmatrix} \cos\theta & Z_r \\ -r\sin\theta & Z_\theta \end{vmatrix}}{\begin{vmatrix} \cos\theta & \sin\theta \\ -r\sin\theta & r\cos\theta \end{vmatrix}} = \frac{\cos\theta Z_\theta + r\sin\theta Z_r}{r\cos^2\theta + r\sin^2\theta} = \sin\theta Z_r + \frac{1}{r}\cos\theta Z_\theta \qquad (3.3)$$

Substitute (3.3) into (3.1), we get:

$$\lambda_x(n,p)(\sin\theta\, Z_r + \frac{1}{r}\cos\theta\, Z_\theta)^2 - \frac{2}{1-p}(\sin\theta\, Z_r + \frac{1}{r}\cos\theta\, Z_\theta)(\cos\theta\, Z_r - \frac{1}{r}\sin\theta\, Z_\theta)$$

$$+\frac{n}{p(1-p)}(\cos\theta Z_r - \frac{1}{r}\sin\theta Z_\theta)^2 = \frac{n\lambda_x(n,p)(1-p)-p}{p(1-p)^2} \qquad (3.4)$$

To calculate the coefficient of $Z_r Z_\theta$:

$$\frac{\lambda_x(n,p)}{r} 2\sin\theta\cos\theta - \frac{2}{1-p}(\frac{\cos^2\theta}{r} - \frac{\sin^2\theta}{r}) - \frac{n}{p(1-p)}\frac{2}{r}\sin\theta\cos\theta = 0$$

$$(\lambda_x(n,p)p(1-p)-n)\tan 2\theta = 2p$$

$$2\theta = \tan^{-1}\ \frac{2p}{\lambda_x(n,p)p(1-p)-n} = \tan^{-1}\lambda_2(n,p) \qquad (3.5)$$

To calculate the coefficient of Z_r^2 :

$$\lambda_3(n,p) = \lambda_x(n,p)\sin^2\theta - \frac{1}{1-p}\sin 2\theta + \frac{n\cos^2\theta}{p(1-p)} \qquad (3.6),$$

To calculate the coefficient of Z_θ^2 :

$$r^2\lambda_4(n,p) = \lambda_x(n,p)\cos^2\theta + \frac{\sin 2\theta}{1-p} + \frac{n\sin^2\theta}{p(1-p)} \qquad (3.7),$$

and constant term $C_0 = \frac{n\lambda_x(n,p)(1-p)-p}{p(1-p)^2}$.

After rotating to a proper angle, the new partial differential equation (3.4) becomes

$$\lambda_3(n,p)Z_r^2 + r^2\lambda_4(n,p)Z_\theta^2 = C_0$$

$$\lambda_3(n,p)Z_r^2 = \mathrm{C}_0\text{-}\ r^2\lambda_4(n,p)Z_\theta^2\ = \mathrm{A}^2 \qquad (3.8)$$

where $\lambda_3(n,p)$, and $\lambda_4(n,p)$ defined the same as equation (3.6) and (3.7).

Now, we can break the above equation (3.8) into two separate parts, and let them equal the same constant, say A^2,

part 1,

$$Z_r^2 = \frac{A^2}{\lambda_3(n,p)}; \quad Z_r = \pm\frac{A}{\sqrt{\lambda_3(n,p)}} \quad Z = \pm\frac{Ar}{\sqrt{\lambda_3(n,p)}} \qquad (3.9)$$

part 2,

$$C_0 - r^2\lambda_4(n,p)Z_\theta^2 = A^2; \quad Z_\theta^2 = \frac{C_0 - A^2}{r^2\lambda_4(n,p)}; \; Z = \pm\sqrt{\frac{C_0 - A^2}{r^2\lambda_4(n,p)}}\;\theta; \qquad (3.10)$$

Put equations (3.9) and (3.10) together to arrive at the general solution of equation (3.8),

$$Z = \pm\frac{Ar}{\sqrt{\lambda_3(n,p)}} \pm\sqrt{\frac{C_0 - A^2}{r^2\lambda_4(n,p)}}\;\theta; \qquad (3.11)$$

Applying the Darboux Theory, we find that the geodesic equation of binomial distribution is given by, $\frac{\partial Z}{\partial A} = B$;

$$\pm\frac{r}{\sqrt{\lambda_3(n,p)}} \pm\frac{A\theta}{\sqrt{(C_0 - A^2)\lambda_4(n,p)r^2}} = B \qquad (3.12)$$

From previously defined relations, we know that (r,θ) and (n,p) are related to $\mathrm{n} = \mathrm{rcos}\theta,\ \mathrm{p} = \mathrm{rsin}\theta,$

$$r^2 = n^2 + p^2 \quad \text{and} \quad \tan\theta = \frac{\mathrm{p}}{n};$$

$$or\ \ \mathrm{r} = \pm\sqrt{n^2 + p^2} \quad \text{and} \quad \theta = \tan^{-1}\frac{\mathrm{p}}{n} \qquad (3.13)$$

hence after substituting the relation (3.13) into equation (3.12) we find our geodesic equation of binomial distribution as:

$$\pm\frac{\sqrt{n^2 + p^2}}{\sqrt{\lambda_3(n,p)}} \pm\frac{A\tan^{-1}\frac{\mathrm{p}}{n}}{\sqrt{(C_0 - A^2)(n^2 + p^2)\lambda_4(n,p)}} = B \qquad (3.14)$$

where C_0, $\lambda_3(n,p)$ and $\lambda_4(n,p)$ are defined the same as before,
and A, B are arbitrary constants.

4 Example

In this section we choose two values for the parameters $n = 10$ *and* $p = 0.5$. Later we will calculate five constants to specify a unique fixed binomial distribution. We list these five constants as follows:

$$\lambda_{\text{x}}(n,p) = -\Psi^{'}(\text{n+1}) + \sum_{\text{x=0}}^{\text{n}} \Psi^{'}(\text{n-}x+1)\binom{\text{n}}{\text{x}} p^{x}(1-p)^{n-x}$$

$$\lambda_2(n,p) = \frac{2p}{\lambda_x(n,p)p(1-p)-n};$$

$$\tan 2\theta = \lambda_2(n,p); \quad \theta = \frac{1}{2}\tan^{-1}\lambda_2(n,p)$$

$$\lambda_3(n,p) = \lambda_x(n,p)\sin^2\theta - \frac{\sin 2\theta}{1-p} + \frac{n\cos^2\theta}{p(1-p)};$$

$$r^2\lambda_4(n,p) = \lambda_x(n,p)\cos^2\theta + \frac{\sin 2\theta}{1-p} + \frac{n\sin^2\theta}{p(1-p)};$$

$$C_0 = \frac{n\lambda_x(n,p)(1-p)-p}{p(1-p)^2}$$

We translate the equation of $\lambda_{\text{x}}(n,p)$ directly from R-package language as follows:

$\lambda_{\text{x}}(10,0.5)$ <- -trigamma(11)+sum(trigamma(10+1-(0:10))*

choose(10,0:10)*0.5^10) (4.1)

We tabulate our computation results as follows:

$\lambda_{\text{x}}(10,0.5) = 0.10674$, $\lambda_2(10,0.5) = -0.1002676$, $\theta = -0.04996678$,

$\lambda_3(10,0.5) = 40.10002$, $r^2\lambda_4(10,0.5) = 0.006723169$, $C0 = 0.2695992$

So the geodesic equation for $n = 10$ and $\text{p} = 0.5$ is given by

$$\pm\frac{\sqrt{n^2+p^2}}{\sqrt{40.10002}} \pm \frac{A\tan^{-1}\frac{\text{p}}{n}}{\sqrt{0.006723169(0.2695992-A^2)}} = B$$

where A and B are arbitrary constants, α and p are some parameters

5 Concluding Remarks

Among the five constants, we realize that the first constant, $\lambda_x(n,p)$, is the most critically important one, because the remaining four constants are dependent on its value. We suggested two methods to compute this constant. Method one as we demonstrated in section 4 by the R-Package. Alternatively, one can use Chen (1982) coded in Fortran IV computer program that can compute the digamma psi functions. It is important to aware of the fact that a finite sum of binomial series converge quickly. However, negative binomial distribution is an infinite series sum, and has no promise of converging. This finite sum may be viewed as a weighted mean of binomial distribution plus some constant. After we find the first constant, $\lambda_x(n,p)$, it would be a straightforward matter to compute the remaining four parameters. Give us a proper angle to rotate, and an interaction term will disappear. Then a specified binomial distribution geodesic equation can be defined.

REFERENCES

[1] Apostol T.M.(1974) Mathematical Analysis. Addison-Wesley Publishing Company. Second Edition.

[2] Balakrishnan N. and Nevzorov V.B.(2003) A Primer on Statistical Distributions. John Wiley & Sons, Inc.

[3] Chen W.W.S (1982) Evaluation of the first 12 derivatives of the digamma psi functions with applications . Proceeding of Statistical Computing Section, 1982, pp293-298.

[4] Chen W.W.S. (2017) On Finding Geodesic Equation of Student T Distribution. Journal of Mathematics Research. Vol. 9. No. 2, April 2017, pp32-37.

[5] Crawley M.J.(2007) The R Book. John Wiley & Sons Ltd. The Atrium, Southern Gate, Chichester, West Sussex PO198SQ, England.

[6] Darboux, G.(2nd ed, 1914) Lecons sur la theorie generale des surfaces. 4 vols, Gauthier-Villars, Paris. I, 1887, 513pp. ;II,1889,522pp.; III,1894,512pp.; IV,1896, 548pp.

[7] Grey A.(1993) Modern differential geometry of curves andsurfaces. CRC Press, Inc. Boca Raton.

[8] Kass, R.E, and Vos, P.W.(1997) Geometrical foundations of asymptotic inference. John Wiley & Sons, Inc. New York. https://doi.org/10.1002/9781118165980

[9] Struik, D.J.(1961) Lectures on classical differential geometry. Second Edition. Dover Publications, Inc.