Probabilistic Packet Marking with Context and Dictionary based Encoding to Optimize WIMAX Communication

Mangal Sain[1] & Dr. Pawan Kumar[2]
[1]Research Scholar, Mewar University, Chittorgarh, Rajasthan.
[2]Principal, Ganga Technical Campus, Bahadurgarh.

Received: May 17, 2018 Accepted: June 28, 2018

ABSTRACT *The high speed communication is demand of the society. High speed wireless communication with WIMAX is most trending. There are various areas of research in field of communication. Now a day's security is one of the major concern in the area. To improve security in communication encoding data is most recommended method for improving security in communication. This data can be a voice or some digital data. The proposed technique will provide a reliable packet marking in such network. Here proposing the probabilistic packet marking algorithm with the adding of four other approaches are used. i) To decide the transmission path, Random packet marking approach. ii) For identification of visited route, approach to trace back the path iii) For verification of transmitted data, approach of combination of Context based and Dictionary based encoding techniques. iv) A Checksum will be applied to vary the alteration of data. The result will be more reliable transmission on WIMAX using the proposed system.*

Keywords: *WIMAX, PPM, Context based encoding, Dictionary based encoding.*

I. INTRODUCTION

WIMAX provides high bandwidth as compared to WI-FI. With the increased demand in packet transfer a lot of issue raised in the network. In WIMAX, Security is the main concern. In this research, our main concern is on reliable packet transfer. In WIMAX, hybrid Automatic Repeat Request (HARWQ) is used to transfer packet with more reliability. WIMAX provides better performance than existing wireless networks. It helps in providing high throughput along with excellence performance. As there is need to find such a solution which can randomly provide solution with much efficient requirement handling approach. It is proposed that the work can be done on Probabilistic Packet Marking which is used in WIMAX research world.

Some conman names those are much popular are Probabilistic Packet Marking algorithm, A Definite Randomize packet marking approach, an approach to traceback the path, Checksum.

These algorithms are capable to solve the problem that we are facing in existing system but further enhancement of these algorithms are also possible. So, an advanced Probabilistic Packet Marking algorithm will be used. The proposed methodology works on combining the following algorithms for reliable packet transfer.

Probabilistic Packet marking algorithm: In this technique a packet is marked on the basis of probability that's why it is called Probabilistic Packet Marking. For packet marking the packets are chosen on random basis. A marking probability is computed by a router for making a decision for marking a packet or not. If router's computation say to mark a packet than the router mention the IP address on the router and forward the packet and let it to go. By doing so the victim packet gets the intruder data.

In probabilistic packet marking, two procedures are conveyed out specifically packet marking and path reconstruction. After doing packet marking, information regarding packets is stored and carried out by edge sampling procedure. The marked packets are utilized for the path reconstruction. The primary drawback of PPM is for reconstruction the number of packets required is more. The reason is that PPM uses underutilized space in IP packets to send information which is not enough to get information.

Context-based coding: in this we utilize the restricted probabilistic replica to slant the allocation of the information the entropy employed the slanted allocation to instruct the novel information.

Utilize the conditional possibility to slant allocation unrestricted possibility:

P ('h') = 0.05, P(' u') = 0.02.

Conditional probability:

P ('h' |'t') = 0.3, P ('u' | 'q') = 0.99.

Practical issues:

Can utilize lively or stationary facts? By means of higher-level context needs huge possibility table

Solutions:

Adaptive system

By means of context of changeable volumes

Expanding the dictionary with probabilistic variant generator

The substitute to alleviate the difficulty of implying variation is to enlarge all entrance in the dictionary in advance. For illustration, let's have the entry in the dictionary as"EGR-1'', we can enlarge this entrance to the two entries ''EGR-1'' and ''EGR 1." through the prolonged dictionary, we be capable of locating names written in various appearance merely by means of exact-matching algorithms. To do this, we suggested an algorithm that can produce only "likely" spelling modification. Our technique not only generates spelling alternative but also provides every option a generation probability that represents the plausibility of the option. Therefore, one does not need to receive an unaffordable number of needless alternatives by setting a suitable threshold for generation probability.

Probabilistic variant generator

Generation probability:

The generation probability of an option is described as the probability that the alternate can be generated throughout a series of procedures. Every procedure has a procedure probability. High and mighty liberty amongst operation, the generation probability of a variation can be formalized in a recursive manner P (X) / P(Y)

Where P(X) is the generation probability of variant X, P(Y) is the generation probability of variant Y from which variant X is generated, and Pop is the probability of the operation by which Y is transformed into X.

Operation probability: to analyze the generation probabilities in our formalization, we require the possibility for each process. We utilize three types of operations for the generation mechanism:

Substitution: Replace a character with another character.

Deletion: Delete a character.

Insertion: Insert a character.

These types of operations are motivated by the ones used in approximate string matching. We consider character-level contexts in which an operation occurs, and

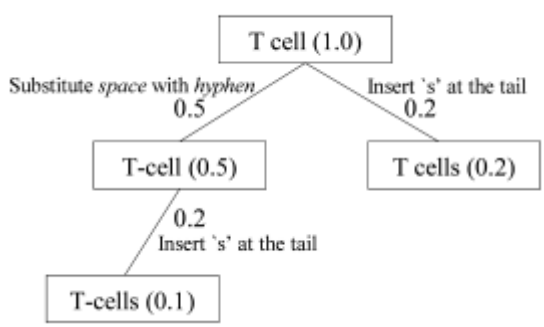


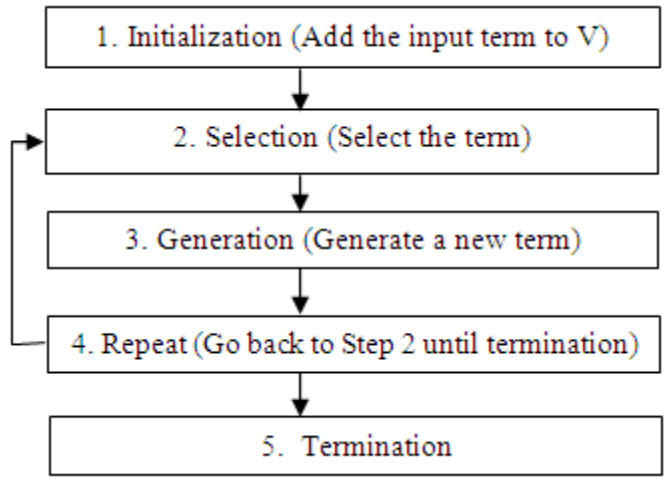
Figure 1: Probabilistic variant generation

The following seven types of contexts are used in this paper. The next step is estimating the probability of each rule. The probability should represent how likely the operation is to occur in a given context. We estimated the operation probabilities from a large number of variant pairs with the following equation:

$$P_{op} = P(\text{operation}|\text{context}) \approx \frac{f(\text{context}, \text{operation}) + 1}{f(\text{context}) + 2},$$

Generation algorithm:

Once the rules and their probabilities are learned, we can generate variants from an input term using those rules. The whole algorithm for variant generation is given below. Note that V represents the set of generated terms.



1. Initialization: Add the input term to V.
2. *Selection:* Select the term and the operation to be applied to it so that the algorithm will generate a new term which has the highest possible probability.
3. *Generation:* Generate a new term using the term and the operation selected in Step 2. Then, add the generated term to V.
4. *Repeat:* Go back to Step 2 until the termination condition is satisfied.

Because this algorithm generates variants in the order of their generation probability, the termination condition can be where that the generation probability for the generated variant is below the predefined threshold or that the number of generated variants exceeds the predefined threshold.

II. PACKET MARKING ALGORITHM RESULTS

Modified Randomize Packet Marking Algorithm:

In IPv4 Header, the stored information is known as marked data. The length of the Identification field is 16 bits. It is split into two parts to store the marking node's identification data (MRK) and the Marked Hop Count (MHC).

The Marked Hop Count (MHC) is used to determine the number of hops between the marking router and the destination. Time to Live (TTL) value depicts the life of the packet on a network in terms of hops. It is known that every router decrements the TTL value of the packet before forwarding the packet to the next router.

Node who marks the packet will be selected by Random number selection algorithm Explained Below:

1. Set Total Nodes N
2. Set MHC=N, TTL=N, MRK=0;
3. For Each Packet
4. Generate a Number between 1 to Max Nodes, X=Random No.
5. If Packet in Not Marked
6. IF PacketID%X + 1 = (MHC-TTL)%X
7. MRK=NodeID,MHC=0;
8. END
9. ELSE
10. MHC=MHC+1;
11. END
12. TTL=TTL-1;
13. END
14. END

Proposed algorithm is implemented in MATLAB and results taken by Evaluation:

We will perform nearly 50 plus experiments to check Random packet marking performance and observe which node will perform marking process by Random behavior. Few experiments are illustrated below:

Packet Marking Algorithm:

```
%set Total Nodes
Nodes=20;
MHC=Nodes; % Marked Hop Count (
TTL=Nodes; %Time to Live
MRK=0;    %Marked node

for i=1:Nodes
   RandomNo=randi([1, Nodes]);
 if((mod(Nodes,RandomNo)+ 1 == mod((MHC-TTL),RandomNo)) && (MRK==0))
    MRK=i;
    MHC=0;
 else
    if(MRK~=0)
    MHC=MHC+1;
    end
end
 TTL=TTL-1;
 A = sprintf('Node %d Status. MHC= %d  TTL= %d  MRK= %d',i,MHC,TTL,MRK);
 disp(A);
end
```

Experiment 1

To Run: packetMarking.m

```
Node 1 Status. MHC= 20  TTL= 19  MRK= 0
Node 2 Status. MHC= 20  TTL= 18  MRK= 0
Node 3 Status. MHC= 20  TTL= 17  MRK= 0
Node 4 Status. MHC= 0  TTL= 16  MRK= 4
Node 5 Status. MHC= 1  TTL= 15  MRK= 4
Node 6 Status. MHC= 2  TTL= 14  MRK= 4
Node 7 Status. MHC= 3  TTL= 13  MRK= 4
Node 8 Status. MHC= 4  TTL= 12  MRK= 4
Node 9 Status. MHC= 5  TTL= 11  MRK= 4
Node 10 Status. MHC= 6  TTL= 10  MRK= 4
Node 11 Status. MHC= 7  TTL= 9  MRK= 4
Node 12 Status. MHC= 8  TTL= 8  MRK= 4
Node 13 Status. MHC= 9  TTL= 7  MRK= 4
Node 14 Status. MHC= 10  TTL= 6  MRK= 4
Node 15 Status. MHC= 11  TTL= 5  MRK= 4
Node 16 Status. MHC= 12  TTL= 4  MRK= 4
Node 17 Status. MHC= 13  TTL= 3  MRK= 4
Node 18 Status. MHC= 14  TTL= 2  MRK= 4
Node 19 Status. MHC= 15  TTL= 1  MRK= 4
Node 20 Status. MHC= 16  TTL= 0  MRK= 4
```

In experiment 1 node 4 is selected by Random Packet Marking Algorithm and it marked Packet with Node ID 4.

The receiver can identify that the router with identification value 4 (MRK = 4) has marked the packet is 16 hops away (MHC = 16). If the packet is not marked by the Router 4 the values of MHC and MRK remain constant all the way. The receiver can identify the hop distance between the sender and the receiver from the difference of MHC and TTL of the unmarked packet.

Experiment 2

To Run: packetMarking.m

```
Node 1 Status. MHC= 20  TTL= 19  MRK= 0
Node 2 Status. MHC= 20  TTL= 18  MRK= 0
Node 3 Status. MHC= 20  TTL= 17  MRK= 0
Node 4 Status. MHC= 20  TTL= 16  MRK= 0
Node 5 Status. MHC= 20  TTL= 15  MRK= 0
Node 6 Status. MHC= 20  TTL= 14  MRK= 0
Node 7 Status. MHC= 20  TTL= 13  MRK= 0
Node 8 Status. MHC= 20  TTL= 12  MRK= 0
Node 9 Status. MHC= 20  TTL= 11  MRK= 0
Node 10 Status. MHC= 20  TTL= 10  MRK= 0
Node 11 Status. MHC= 20  TTL= 9  MRK= 0
Node 12 Status. MHC= 0  TTL= 8  MRK= 12
Node 13 Status. MHC= 1  TTL= 7  MRK= 12
Node 14 Status. MHC= 2  TTL= 6  MRK= 12
Node 15 Status. MHC= 3  TTL= 5  MRK= 12
Node 16 Status. MHC= 4  TTL= 4  MRK= 12
Node 17 Status. MHC= 5  TTL= 3  MRK= 12
Node 18 Status. MHC= 6  TTL= 2  MRK= 12
Node 19 Status. MHC= 7  TTL= 1  MRK= 12
Node 20 Status. MHC= 8  TTL= 0  MRK= 12
```

In experiment 2 node 12 is selected by Random Packet Marking Algorithm and it marked Packet with Node ID 12.

The receiver can identify that the router with identification value 4 (MRK = 12) has marked the packet is 8 hops away (MHC = 8). If the packet is not marked by the Router 4 the values of MHC and MRK remain constant all the way. The receiver can identify the hop distance between the sender and the receiver from the difference of MHC and TTL of the unmarked packet.

Experiment 3

To Run: packetMarking.m

```
Node 1 Status. MHC= 20  TTL= 19  MRK= 0
Node 2 Status. MHC= 20  TTL= 18  MRK= 0
Node 3 Status. MHC= 20  TTL= 17  MRK= 0
Node 4 Status. MHC= 20  TTL= 16  MRK= 0
Node 5 Status. MHC= 20  TTL= 15  MRK= 0
Node 6 Status. MHC= 0  TTL= 14  MRK= 6
Node 7 Status. MHC= 1  TTL= 13  MRK= 6
Node 8 Status. MHC= 2  TTL= 12  MRK= 6
Node 9 Status. MHC= 3  TTL= 11  MRK= 6
Node 10 Status. MHC= 4  TTL= 10  MRK= 6
Node 11 Status. MHC= 5  TTL= 9  MRK= 6
Node 12 Status. MHC= 6  TTL= 8  MRK= 6
Node 13 Status. MHC= 7  TTL= 7  MRK= 6
Node 14 Status. MHC= 8  TTL= 6  MRK= 6
Node 15 Status. MHC= 9  TTL= 5  MRK= 6
Node 16 Status. MHC= 10  TTL= 4  MRK= 6
Node 17 Status. MHC= 11  TTL= 3  MRK= 6
Node 18 Status. MHC= 12  TTL= 2  MRK= 6
Node 19 Status. MHC= 13  TTL= 1  MRK= 6
Node 20 Status. MHC= 14  TTL= 0  MRK= 6
```

In experiment 3 node 6 is selected by Random Packet Marking Algorithm and it marked Packed with Node ID 6.

The receiver can identify that the router with identification value 4 (MRK =6) has marked the packet is 14 hops away (MHC = 14). If the packet is not marked by the Router 4 the values of MHC and MRK remain constant all the way. The receiver can identify the hop distance between the sender and the receiver from the difference of MHC and TTL of the unmarked packet.

Experiment 4

To Run: packetMarking.m

In experiment 4 node 17 is selected by Random Packet Marking Algorithm and it marked Packet with Node ID 17.

The receiver can identify that the router with identification value 4 (MRK =17) has marked the packet is 3 hops away (MHC = 3). If the packet is not marked by the Router 4 the values of MHC and MRK remain constant all the way. The receiver can identify the hop distance between the sender and the receiver from the difference of MHC and TTL of the unmarked packet.

```
>> packetMarking
Node 1 Status. MHC= 20  TTL= 19  MRK= 0
Node 2 Status. MHC= 20  TTL= 18  MRK= 0
Node 3 Status. MHC= 20  TTL= 17  MRK= 0
Node 4 Status. MHC= 20  TTL= 16  MRK= 0
Node 5 Status. MHC= 20  TTL= 15  MRK= 0
Node 6 Status. MHC= 20  TTL= 14  MRK= 0
Node 7 Status. MHC= 20  TTL= 13  MRK= 0
Node 8 Status. MHC= 20  TTL= 12  MRK= 0
Node 9 Status. MHC= 20  TTL= 11  MRK= 0
Node 10 Status. MHC= 20  TTL= 10  MRK= 0
Node 11 Status. MHC= 20  TTL= 9  MRK= 0
Node 12 Status. MHC= 20  TTL= 8  MRK= 0
Node 13 Status. MHC= 20  TTL= 7  MRK= 0
Node 14 Status. MHC= 20  TTL= 6  MRK= 0
Node 15 Status. MHC= 20  TTL= 5  MRK= 0
Node 16 Status. MHC= 20  TTL= 4  MRK= 0
Node 17 Status. MHC= 0  TTL= 3  MRK= 17
Node 18 Status. MHC= 1  TTL= 2  MRK= 17
Node 19 Status. MHC= 2  TTL= 1  MRK= 17
Node 20 Status. MHC= 3  TTL= 0  MRK= 17
```

In experiment 4 node 17 is selected by Random Packet Marking Algorithm and it marked Packed with Node ID 17.

The receiver can identify that the router with identification value 4 (MRK =17) has marked the packet is 3 hops away (MHC = 3). If the packet is not marked by the Router 4 the values of MHC and MRK remain constant all the way. The receiver can identify the hop distance between the sender and the receiver from the difference of MHC and TTL of the unmarked packet.

Experiment 5

To Run: packetMarking.m

```
Node 1 Status. MHC= 20  TTL= 19  MRK= 0
Node 2 Status. MHC= 20  TTL= 18  MRK= 0
Node 3 Status. MHC= 20  TTL= 17  MRK= 0
Node 4 Status. MHC= 20  TTL= 16  MRK= 0
Node 5 Status. MHC= 20  TTL= 15  MRK= 0
Node 6 Status. MHC= 20  TTL= 14  MRK= 0
Node 7 Status. MHC= 20  TTL= 13  MRK= 0
Node 8 Status. MHC= 20  TTL= 12  MRK= 0
Node 9 Status. MHC= 20  TTL= 11  MRK= 0
Node 10 Status. MHC= 20  TTL= 10  MRK= 0
Node 11 Status. MHC= 20  TTL= 9  MRK= 0
Node 12 Status. MHC= 20  TTL= 8  MRK= 0
Node 13 Status. MHC= 20  TTL= 7  MRK= 0
Node 14 Status. MHC= 0  TTL= 6  MRK= 14
Node 15 Status. MHC= 1  TTL= 5  MRK= 14
Node 16 Status. MHC= 2  TTL= 4  MRK= 14
Node 17 Status. MHC= 3  TTL= 3  MRK= 14
Node 18 Status. MHC= 4  TTL= 2  MRK= 14
Node 19 Status. MHC= 5  TTL= 1  MRK= 14
Node 20 Status. MHC= 6  TTL= 0  MRK= 14
```

In experiment 5 node 14 is selected by Random Packet Marking Algorithm and it marked Packed with Node ID 14.

The receiver can identify that the router with identification value 4 (MRK =14) has marked the packet is 6 hops away (MHC = 6). If the packet is not marked by the Router 4 the values of MHC and MRK remain

constant all the way. The receiver can identify the hop distance between the sender and the receiver from the difference of MHC and TTL of the unmarked packet.

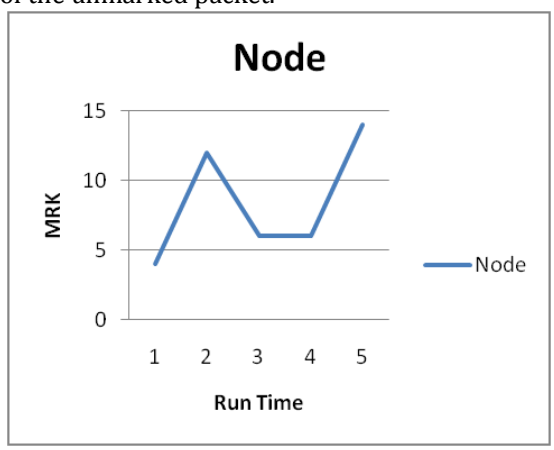


Figure 2: Packet Marking Results

Figure 2 shows the MRK values for different experiment. If the packet is not marked by the Router 4 the values of MHC and MRK remain constant all the way.

The Marked Hop Count (MHC) is used to determine the number of hops between the marking router and the destination. Time to Live (TTL) value depicts the life of the packet on a network in terms of hops. It is known that every router decrements the TTL value of the packet before forwarding the packet to the next router.

III. EXPERIMENTAL WORK

Time Taken for Encryption-Decryption Process

We have performed 8 experiments to get Time consumption in Encode-Decode process and to get accuracy of Process.

To Run: HybridEncode ('01010011')

Output:

```
>> HybridEncode ('01010011')
<0,0,C(0)>
<0,0,C(1)>
<2,2,C(0)>
<3,2,C(1)>
ans =
Context Based Encoded Result:
coded =0000000110000000000011000100010000100011000000011000100011000 1
Checksum of Encoded Data:
csumStart =feb2b52541f6f2561f7150815538731d
Data after Checksum
coded =
0000000110000000000011000100010000100011000000011000100011000 1
Dictionary Encoding Started with Above input data Dictionary Encoded Result:
packed =
  Columns 1 through 6
    48   256   257    48    49    49
  Columns 7 through 12
   258   262   256   260   257   261
  Columns 13 through 18
   264   258   267   259   270   269
  Columns 19 through 21
   270   274   274
Dictionary Decoding Result:
unpacked =0000000110000000000011000100010000100011000000011000100011000 1
Checksum of Decoded Data:
```

csumEnd =feb2b52541f6f2561f7150815538731d
Compare Checksum
checkOK =1
Context Based Decoded Result:decoded =01010011
ans =00000000001111000000000000001110000110000100000110000111000000001110001100011
ok =1
ans =01010011
In the above example we input the data '01010011' and get the following results:

Context based Encoded result:

00000001100000000000110001000100001000110000000110001000110001

Checksum of Encoded data:

00000001100000000000110001000100001000110000000110001000110001

Dictionary encode data result:

Columns 1 through 6

48 256 257 48 49 49

Columns 7 through 12

258 262 256 260 257 261

Columns 13 through 18

264 258 267 259 270 269

Columns 19 through 21

270 274 274

Dictionary Decoding Result:

00000001100000000000110001000100001000110000000110001000110001

Checksum of dictionary decoded result:

feb2b52541f6f2561f7150815538731d

Compare checksum:

Check ok=1

Context Based Decoded Result:

Decoded:

00000000001111000000000000001110000110000100000110000111000000001110001100011

Answer: 01010011

Table 1: Decoding time

S. No.	Input Data	Validation	Time (S)
1	0100100011110	Success	0.0223682
2	Hello I LIVE IN INDIA I am Phd scholar Engineering	Success	0.175915
3	WELCOME TO INDIA	Success	0.087282
4	11101111	Success	0.0045887
5	TESTING	Success	0.069822
6	hybrid technique	Success	0.128475
7	Signal	Success	0.049347
8	Engineering	Success	0.052428

Table 1 and figure 3 shows the decoding time of the few experiments which are encoded by proposed approach. It can be seen in the graph that binary data takes less time to decode.

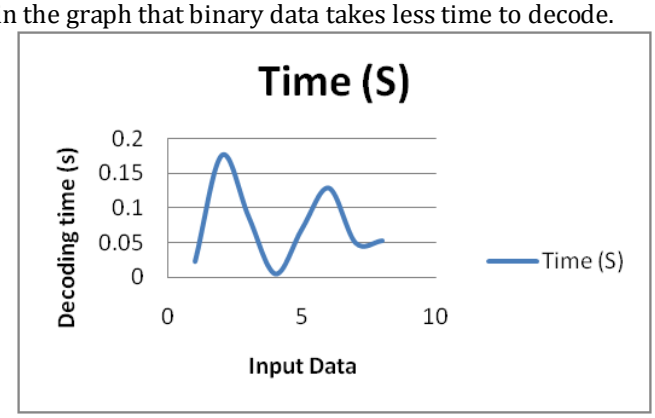


Figure 3: Decode Time

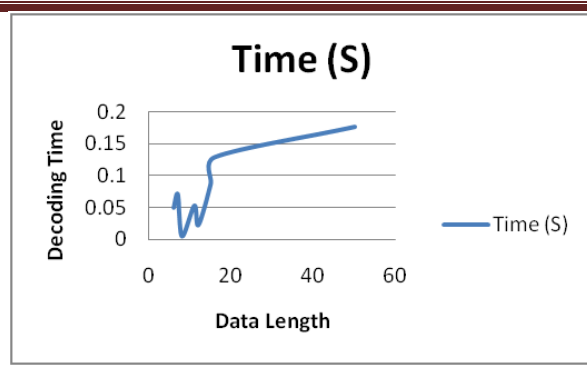


Figure 4: Length Vs Time

As shown in figure 4 the decoding time increases as the length of the data increases, but the binary data takes lesser time to decode.

CONCLUSION

The proposed approach provides a reliable hop based packet marking in such network which is based on Random packet marking approach with algorithm mentioned above. Also A combination of Context based and Dictionary based encoding approach implemented and executed to verify the transmitted data along Checksum to check integrity of data. It can be concluded that the proposed approach is providing a novel, accurate and secure data encoding and decoding technique in data searching and communication.

REFERENCES

[1]. Sukhwinder Singh, "Hybrid Packet Marking IP Traceback Technique over IPv4, IPv6 and Mobile IPv6", International Journal of Engineering Trends and Technology (IJETT) – Volume 46 Number 5 April 2017.
[2]. B. Feng and H. Yusheng, "Improved probabilistic packet marking scheme based on APPM-V6," in In IEEE 7th Joint International Information Technology and Artificial Intelligence Conference (ITAIC), NanChang, China, 2014, pp. 380-386.
[3]. M.Vijayalakshmi, Dr.S.Mercy Shalinie, A.Arun Pragash, "IP traceback system for network and application layer attacks", Proceedings of IEEE Conference on Recent Trends in Information Technology (ICRTIT),2012
[4]. Saurabh, S.; Sairam, A.S.; , "Linear and Remainder Packet Marking for fast IP traceback," Communication Systems and Networks (COMSNETS), 2012 Fourth International Conference on , vol., no., pp.1-8, 3-7 Jan. 2012
[5]. NS Tung, V Kamboj, B Singh, A Bhardwaj, Switch Mode Power Supply An Introductory approach, Switch Mode Power Supply An Introductory approach, May 2012.
[6]. S. Symington, S. Farrell, H. Weiss, P. Lovell, Bundle security protocol specification draft-irtf-dtnrg-bundle-security-12, http://tools.ietf.org/html/draft-irtf-dtnrg-bundle-security-12 (november 2009).
[7]. A. Shikfa, M. Onen, R. Molva, Privacy in context-based and epidemic ¨ forwarding, in: AOC 2009. 3rd IEEE International WoWMoM Workshop on Autonomic and Opportunistic Communications, June 15, 2009, Kos, Greece, 2009.
[8]. A. Lindgren, A. Doria, Probabilistic routing protocol for intermittently connected networks, in: IRTF Internet Draft, draft-irtf-dtnrg-prophet00.txt, 2008.
[9]. A. El Fawal, J.-Y. Le Boudec, K. Salamatian, Self-Limiting Epidemic Forwarding, Tech. rep., EPFL (2006).
[10]. Preet Khandelwal, Surya Prakash Ahirwar, Amit Bhardwaj, Image Processing Based Quality Analyzer and Controller, International Journal of Enhanced Research in Science Technology & Engineering, Volume 2, Issue 7, 2013.
[11]. L. Lilien, Z. Kamal, V. Bhuse, A. Gupta, Opportunistic networks: The concept and research challenges in privacy and security, in: NSF Intl. Workshop on Research Challenges in Security and Privacy for Mobile and Wireless Networks (WSPWN 2006), Miami, 2006.
[12]. D. Boneh, M. Franklin, Identity-based encryption from the weil pairing, in: CRYPTO, 2001, pp. 213–229.
[13]. Vikram Kumar Kamboj, S.K. Bath, J. S. Dhillon, "Multiobjective multiarea unit commitment using hybrid differential evolution algorithm considering import/export and tie-line constraints", Neural Computing and Applications (ISSN: 1433-3058), Vol.28, No.11, 2017, pp. 3521–3536, DOI 10.1007/s00521-016-2240-9.
[14]. T. Spyropoulos, K. Psounis, C. S. Raghavendra, Spray and wait: an efficient routing scheme for intermittently connected mobile networks, in: ACM SIGCOMM workshop on Delay-tolerant networking (WDTN), 2005, pp. 252–259.
[15]. D. Boneh, G. Crescenzo, R. Ostrovsky, G. Persiano, Public-key encryption with keyword search, in: Eurocrypt, 2004.