DOI 10.12694/scpe.v20i1.1481
Scalable Computing: Practice and Experience ISSN 1895-1767
Volume 20, Number 1, pp. 83–92. http://www.scpe.org

NODE AUTHENTICATION USING NTRU ALGORITHM IN OPPORTUNISTIC NETWORK

MUSAEED ABOUAROEK* AND KHALEEL AHMAD †

Abstract. The demand for using wireless paradigms for performing various information and communication operations has been exploded. The opportunistic networks is a special type of delay tolerant networks proposed to operate in an emergency manner to facilitate mobile connectivity between the nodes when there is no connectivity. These emergencies are caused either by human-made or natural disasters. Opportunistic Networks depend on mobile phones and other mobile devices that carry wireless technology. This paper is an attempt to expand the opportunistic network through the authentication nodes. We propose an NTRU algorithm for node authentication in opportunistic networks .NTRU algorithm is an asymmetric post-quantum cryptosystem. This algorithm is unbreakable and robust compared to RSA and ECC cryptosystem.

Key words: Node Authentication, Packet Integrity, Sybil Attack, NTRU Algorithm, Post-Quantum Cryptography

AMS subject classifications. 68M12

1. Introduction. The opportunistic network is a subclass of mobile ad hoc network (MANET) that has been proposed to operate in an emergency manner where no network exists. OppNets are used to communicate between the nodes which may be mobiles or other devices having Wi-Fi or Bluetooth using personal laptops, cameras, sensors. OppNets may connect to other heterogeneous networks among the cellular base station, sensor networks, IoT devices, and other networks which connected through WI-FI [1, 2, 3, 4]. In this network the nodes act to each other as a router that causes Opportunistic networks to be more adaptable than Delay Tolerant Network (DTN) as shown in Fig. 1.1. OppNets use store-carry and forward mechanism to connect and extend the network because the path between the source and destination does not exist [5, 6, 7].

An OppNets grows from heterogeneous nodes and extend through authenticated nodes . The helper nodes need to join to opportunistic networks will check and verify to prevent and secure the network from the malicious node[7]. These nodes have self-configure and free to join/leave the OppNets. The use of OppNets is very suitable for disasters and emergency scenarios as they are infrastructure less or unavailable while the nodes can store - carry and forward the messages and the routes from the source to the destination are built dynamically [8, 9, 10]. The nodes in OppNets usually have high mobility, low density, limited power, short radio range, and often subject to different kinds of attacks by malicious nodes. Due to these characteristics, OppNets have gained significant research attention due to the security and authentication challenges that have emerged [11]. OppNets are very challenging network and the main challenging is to develop security solutions or discovering new algorithms to improve the connectivity between the nodes in a secure manner. Authentication is an important feature which must be implemented in each every network. Different researchers have done various efforts to explain authentication goals, node authentication, and packet authentication features in opportunistic networks [12, 13, 14].

2. Related Work. In 2018, Ahmed et al.presented a technique that allows nodes to authenticate packets as they receive them by constructing hash trees, also referred to as Merkle trees. Merkle trees are used to check and authenticate all the packets. As a result the direct trust is formed. Direct trust is updated based on the authenticity of the packets and the encounter rate of the node. As nodes come into contact with each other during the packet transmission period, they share feedback on how much they trust other nodes [11].

In 2018, Mehra et al. proposed codeword authenticated scheme in which the authentication between the entities takes place using three factor namely codeword, password and OTP. This protocol efficiently validates the entities preserving perfect forward secrecy and thwarting reply attack, DoS attack and man in the middle attack in hostile environment [15].

In 2017, Kumar et al. researchers proposed a security algorithm for opportunistic networks. The proposed algorithm utilizes dynamic IDs for key exchange mechanism and RSA for the message encryption

*Department of Computer Science and IT, Maulana Azad National Urdu University, India (musaeednaji@gmail.com)
†Department of Computer Science and IT, Maulana Azad National Urdu University, India (khaleelamna@gmail.com)

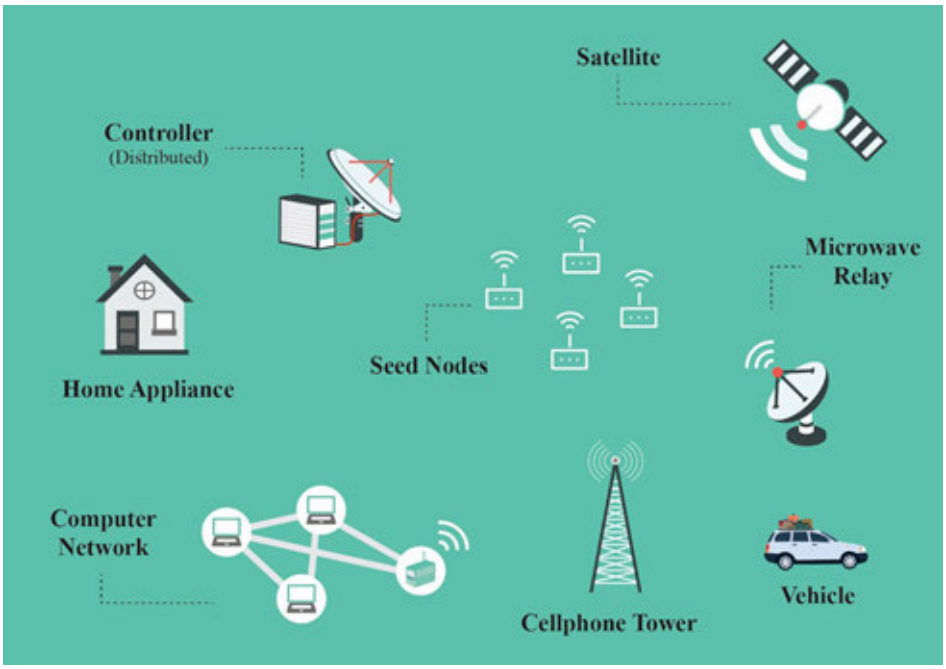

FIG. 1.1. *Heterogeneous nodes in an OppNet*

purposes and maintains the privacy of data as well as user privacy. In addition to this message integrity is also preserved. Results showed the proposed algorithm that fulfills the security requirements of opportunistic networks and perform well under various performance metrics [5] .

In 2017, Singh et al. proposed an authentication mechanism that uses a trust framework for opportunistic networks. They proposed some trust framework which provides trust of authenticated nodes to supernode, so that it can be an authentic node to register new node,as same as super node does. This mechanism is applied for the short-term and limited wireless network environment. They used a separate node to manage node registration and provide authorization to other authenticated nodes to register unauthentic nodes [16].

Wu et al. 2015 discussed a security architecture of opportunistic network where it is divided into five modules as authentication, access control, secure routing, trust management, cooperation and application user privacy [17].

In 2015, Guo et al. researchers proposed an authentication mechanism with privacy protection for opportunistic networks. It is applied for the short-term and limited-time wireless network environment, and a supernode is also set to manage node registration. The proposal implements some encryption and security technologies against security threats and attacks. In this analysis, the proposed mechanism finishes the authentication with less data, and provides anonymity and user privacy in the network. The present study proposes an OppNet-specific authentication scheme for preventing malicious node attacks and protecting personal privacy [18].

In 2014, Kuo et al. proposed an efficient and secure anonymous roaming authentication scheme for mobility networks. In order to maintain secure advantages, researchers proposed a scheme that utilizes hash functions and point operations instead of the asymmetric or symmetric system. Comparing security and performance, researchers proposed a scheme which not only has more security properties in comparison with previous schemes, but also enhances performance during the roaming authentication phase for mobility networks [19].

In 2010 Ma et al. proposed threshold secret sharing and identity- based cryptography were employed to facilitate opportunistic node authentication to secure data communication over intermittently connected mobile ad hoc networks(ICMANs). To avoid the key escrow problem and the single point of failure problem, the master private key of IBC was cooperatively generated and shared by n distributed PKGs, while each authenticating node has to encounter t-out-of-n PKGs to recover its own private key [20].

In 2014 Soleimani and Kahvand presented a dynamic trust model that used a trust to defend ad hoc networks from packet dropping attacks. At the initial stage of the network, a node trusted its surrounding nodes and updated the trust value according to their behavior. Behavior that decreased the trust value of a node included: dropping a packet, not forwarding a packet to the destination, not starting a route discovery phase. The trust value of a node increased when it forwarded the packets in a route targeting the destination. The nodes in the model do not propagate the trust values of the nodes in the network [21].

In 2015, Niaz and Saake present a deterministic method to protect the integrity of outsourced data using Merkle Hash Trees authentication. The method aims to deal with saving and loading the authenticated data from and to cloud service providers. The authors are aware of the difficulties faced with traditional databases to increased communication and computation overhead that result from adding and removing records, and aim to addresses in their ongoing work [22].

In 2007, Asokan et al. analyzed the applicability of IBC in this context and conclude that for authentication and integrity, IBC has no significant advantage over traditional cryptography, but it can indeed enable better ways of providing confidentiality. Additionally, the author showed a way of bootstrapping the needed security associations for IBC use from an existing authentication infrastructure [23].

3. Preliminaries. NTRU stands for Nth Degree Truncated Ring Units.NTRU encrypt is a public-key cryptosystem developed by three mathematicians named Hoffstein, Pipher and Silverman in 1998. NTRU is a ring-based cryptosystem. It has a ring R that consists of all truncated polynomials of degree N-1 having integer coefficients: a = $a_0 + a_1X + a_2X^2 + a_3X^3 + \ldots + a_{N-2}X^{N-2} + a_{N-1}X^{N-1}$. Polynomials are added in the usual way. They are also multiplied more-or-less as usual, except that X^N is replaced by 1, X^{N+1} is replaced by X, X^{N+2} is replaced by X^2, and so on [24, 25, 26, 27].

Notations:. P : Defines the highest degree of polynomial to be truncated.
q : q takes as a large modulus, usually, the coefficients of the truncated polynomials will be reduced mod q.
p : p is a small modulus. As the final step in decryption, the coefficients of the message are reduced mod p.
f(x): f(x) is a small polynomial and it is the part of the private key.
f_p : fp is the inverse of f(x) mod p and it is the part of the private key.
f_q : fq is the inverse of f(x) mod q.
g(x) : g(x) is a small polynomial, it is used to generate the public key.
P_U : P_U denotes the public key;P_k= p * (fq * g(x)) (mod q)
P_R : P_R denotes the private key.
m(x) : m(x) denotes the message, it takes as a small polynomial.
r(x) : r(x) denotes the random blind value, it is used during the encryption.
C : C denotes the ciphertext (encrypted message).
P_1 : The partially decrypted message P_1 = (f(x) * C) mod q.
P_2 : The partially decrypted message $P_2 = P_1$(mod p).
N_s : Seed Nodes (Authenticated Nodes)
N_h : Helper Node
N_{source} : Source Node (Sender)
N_d : Destination Node (Receiver)
D_R : Delivery Ratio
$M_{created}$: Messages created or generated by the sender
$M_{broadcast}$: Messages broadcast
$M_{received}$: Messages received by the receiver
$T_{created}$: Messages created or generated time
$T_{received}$: Messages received time

Set up of NTRU Algorithm.

i. **Key Generation**

- Choose two random polynomial f(x) and g(x) that is invertible by (mod p) and (mod q)
- Choose two random polynomial f(x) and g(x) that is invertible by (mod p) and (mod q)
- Choose two random polynomial f(x) and g(x) that is invertible by (mod p) and (mod q)

- Compute the inverse of f(x) mod p = fpand f(x) mod q= fq such that f(x) * f(x)-1 = 1 (mod p, q)
- The private key (PR) is the pair (f(x), fp)
- The public key (PU)= p * (fq * g(x)) (mod q)

ii. Encryption
- Choose a random polynomial r(x)
- Choose a message m(x).
- Compute the ciphertext (C)= r(x) * P_U + m(x) (mod q).

iii. Decryption
- Compute a polynomial using private key f(x) as P1 = f(x) * C(mod q)
- Compute a polynomial as P2 = P1 (mod p) and lessen the coefficients between p/2 and p/2.

4. System Model. In OppNets, the malicious node may modify or change the content of the messages [28, 29, 30]. To secure an opportunistic network from such type of attacks, we proposed an NTRU algorithm that shall eradicate the malicious nodes and useful in secure message communication. To perform this work, we purposed the NTRU algorithm which will provide an authentication to the node and the packet. The authenticated nodes (seed nodes) in an OppNet will generate the unique ID for each node to recognize them and generates the key to encrypt and decrypt messages to protect against advisory during transmission. Authenticated nodes will check the helper node which needs to join the network. If the node has an assigned ID then the authenticated node (seed node) will verify the ID but if the helper node is new then the seed node will generate the ID and authenticate it to join the network. In addition with, the seed node also broadcast the public key of helper node to update the public key list of each node. After ID allocation and verification the node is ready to carry and forward the messages as shown in Fig. 4.1.

4.1. Authenticated nodes. These are the main nodes on which opportunistic network based on and to ensure the security of the network where the authenticated nodes (seed nodes) register the new node to become an authenticated node. Its the backbone of the opportunistic network which generates ID to new node to authorize and connects to the network. After receiving the authorized ID for granted to enter the opportunistic networks and only authenticated nodes can carry and forward the messages to other nodes. Authenticated nodes can be generated and verify ID for new nodes which need to join the opportunistic network as a helper as shown in Fig. 4.2.

4.2. Unauthenticated nodes. These are the nodes which want to join to the opportunistic network without getting the registration ID or complete registration process, so these nodes are not authorized by authenticated nodes (seed nodes).

4.3. Mutual Node Identification and Authentication. When a new node needs to join the opportunistic network, it has to get the permission from the seed nodes or authenticated nodes. First, the authenticated node will receive a request from the node which needs to join, then will check and verify to know the node id is authorized or not, if node id is available in the public list of ids which is store in every authenticated node then will allow the node to join the opportunistic network. Second, if the node does not have any id so will send ACK to the authenticated node to register and response with new ID to join OppNets and broadcast new id to all authenticated nodes (seed nodes) to update the id list periodically. Now, this node is ready to join and communicate with any authenticated nodes and can generate an ID for new nodes. This is the main advantage to extend and grow the Opportunistic network.

4.4. Packet Authentication. The message, authenticated node, encrypts function and helper node must be in IDs list which must be authenticated, so these are the requirements to authorize the packet. When node n has the message for transmission, so it has to follow these steps to send the packet:

- Authenticated node or seed node will use the encrypt function by NTRU algorithm and generate two keys public key and private key to secure the packet
- Next node also called helper node will receive packet contents of destination id, keys of packet and message to carry and forward in an authenticated situation.
- Receiving node will receive the encrypted message and if its the destination node then will use the decryption function and forward the message to the next node till reach the destination.

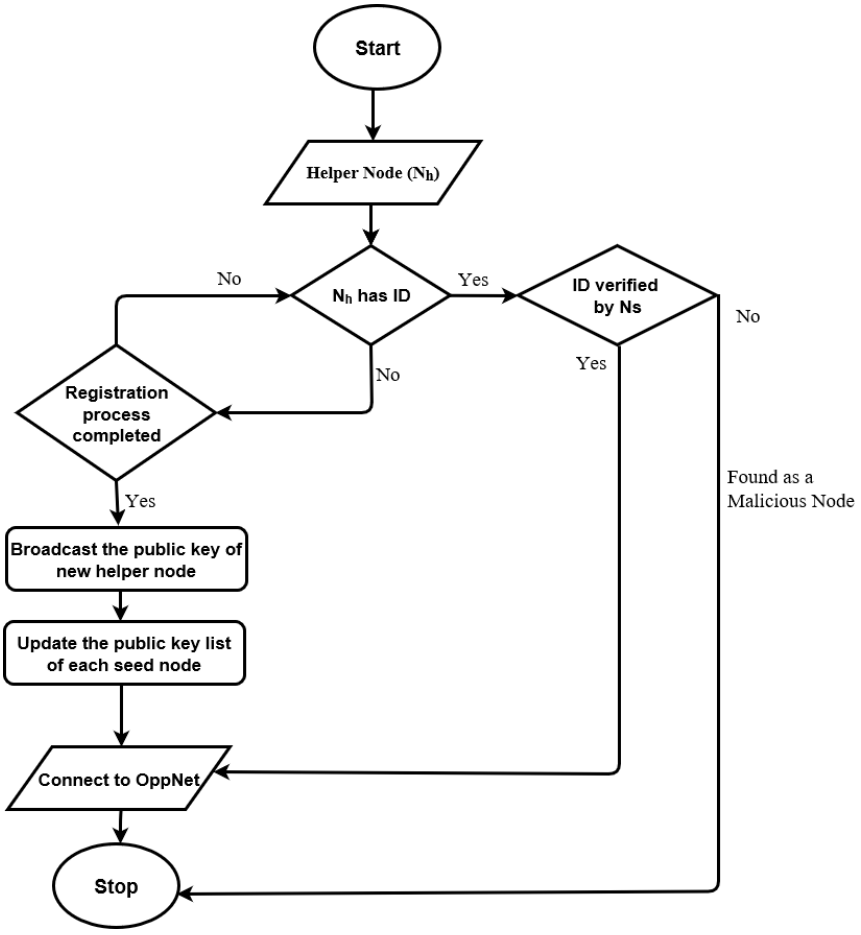

FIG. 4.1. *Flow Chart of Node Authentication Process*

4.5. Algorithm for Node Authentication Process.

```
BEGIN
  Nh is interested to join in OppNet, it sends a registration request to Ns
  If Nh has already an ID
        // If helper node is already registered in OppNet
        // then helper node has ID
       If ID is verified as authenticated by Ns // ID is verified by seed nodes.
           Connect to OppNets
       Else
           Authentication failed// Node found as a malicious.
       End If
  Else
      If the registration process is successfully completed by Ns
         Ns broadcast Public key (PU) of  Nh
         Update the public key list of each Ns
         Connect to  OppNets
```

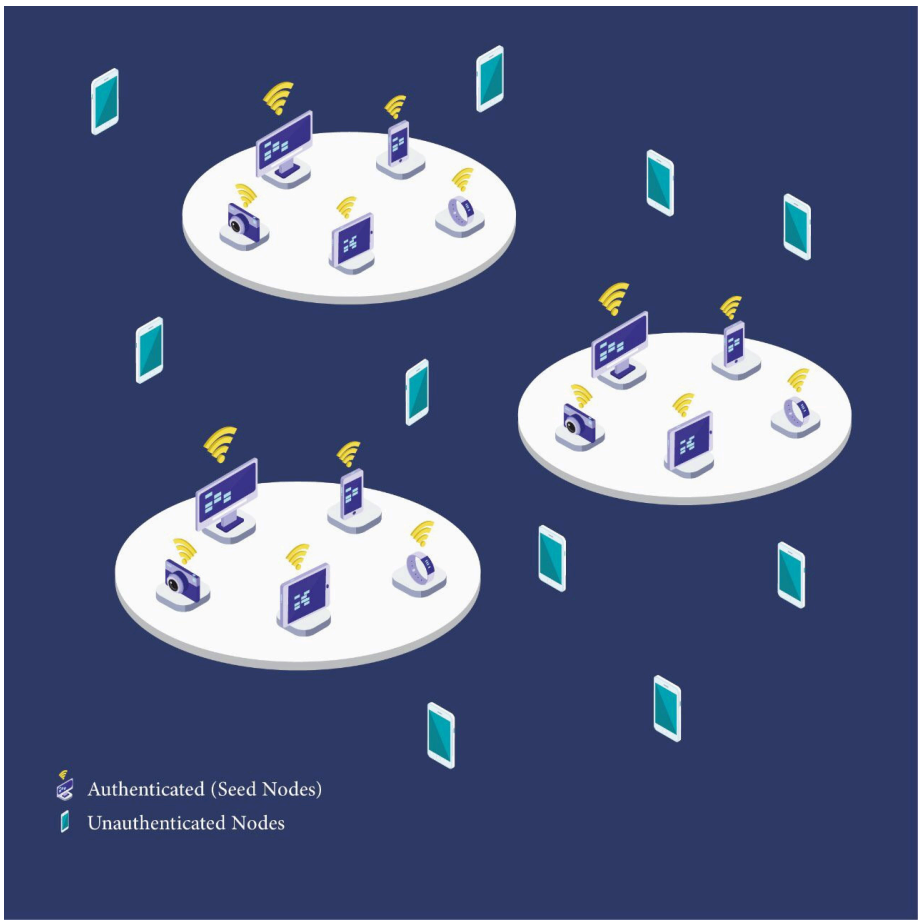

FIG. 4.2. *Node Authentication in Opportunistic Networks*

```
14       Else
15           Go to step 2 // re-initiate the process until the registration complete
16       End If
17   End If
17 END
```

4.6. Simulation of NTRU Algorithm. Suppose a node (N_{source}) wishes to send a message to a destination (Nd),N_{source} will encrypts the messages using receivers public key (P_U).

Consider the following Public Key Parameters values: $N = 11, p = 3$ and $q = 32$.

Choose the two polynomials randomly:

$f(x) = -1 + x + x^2 - x^4 + x^6 + x^9 - x^{10}$, $g(x) = -1 + x^2 + x^3 + x^5 - x^8 - x^{10}$

Consider the message which is in binary form 01001011 which is equivalent to $x^6 + x^3 + x^1 + 1$ in polynomial form: message $m(x) = 1 + x^1 + x^3 + x^6$

I. **Key Generation Process** Compute the inverse f_p of (f mod p)and the inverse $f_q$of (f mod q).

- $f_p = f(x)^{-1}(\text{mod p}) = (-1 + x + x^2 - x^4 + x^6 + x^9 - x^{10})^{-1}(\text{mod } 3)$

```
In[7]:= fp = -1 + x + x^2 - x^4 + x^6 + x^9 - x^10;
        PolynomialMod[Algebra`PolynomialPowerMod`PolynomialPowerMod[fp, -1, x, x^11 - 1], 3]

Out[8]= 1 + 2 x + 2 x^3 + 2 x^4 + x^5 + 2 x^7 + x^8 + 2 x^9
```

$f_p = 1 + 2x + 2x^3 + 2x^4 + x^5 + 2x^7 + x^8 + 2x^9$

- $f_q = f(x)^{-1} (\text{mod q}) = (-1 + x + x^2 - x^4 + x^6 + x^9 - x^{10})^{-1} \ (\text{mod } 32)$

```
In[9]:= fq = -1 + x + x^2 - x^4 + x^6 + x^9 - x^10;
        PolynomialMod[Algebra`PolynomialPowerMod`PolynomialPowerMod[fq, -1, x, x^11 - 1], 32]

Out[10]= 5 + 9 x + 6 x^2 + 16 x^3 + 4 x^4 + 15 x^5 + 16 x^6 + 22 x^7 + 20 x^8 + 18 x^9 + 30 x^10
```

$f_q = 5 + 9x + 6x^2 + 16x^3 + 4x^4 + 15x^5 + 16x^6 + 22x^7 + 20x^8 + 18x^9 + 30x^{10}$

- Public Key (P_U)= p * (fq * g(x)) (mod q) Now, compute f_q * g(x) and apply the truncated concept:
  f_q* g(x)= $(5 + 9x + 6x^2 + 16x^3 + 4x^4 + 15x^5 + 16x^6 + 22x^7 + 20x^8 + 18x^9 + 30x^{10}) * (-1 + x^2 + x^3 + x^5 - x^8 - x^{10})$
  $= -5 - 9x - x^2 - 2x^3 + 11x^4 + 12x^5 + 13x^6 + 3x^7 + 22x^8 + 15x^9 + 16x^{10} + 29x^{11} + 60x^{12} + 19x^{13} - 2x^{14} - 7x^{15} - 36x^{16} - 40x^{17} - 50x^{18} - 18x^{19} - 30x^{20}$
  $= -5 - 9x - x^2 - 2x^3 + 11x^4 + 12x^5 + 13x^6 + 3x^7 + 22x^8 + 15x^9 + 16x^{10} + x^{11}(29 + 60x + 19x^2 - 2x^3 - 7x^4 - 36x^5 - 40x^6 - 50x^7 - 18x^8 - 30x^9)$
  $= 24 + 51x + 18x^2 - 4x^3 + 4x^4 - 24x^5 - 27x^6 - 47x^7 + 4x^8 - 15x^9 + 16x^{10}$
  $p * (f_q * g(x))$
  $= 3 * (24 + 51x + 18x^2 - 4x^3 + 4x^4 - 24x^5 - 27x^6 - 47x^7 + 4x^8 - 15x^9 + 16x^{10})$
  $= 72 + 153x + 54x^2 - 12x72x^5 - 81x^6 - 141x^7 + 12x^8 - 45x^9 + 48x^{10}$

```
In[24]:= PolynomialMod[72 + 153 x + 54 x^2 - 12 x^3 + 12 x^4 - 72 x^5 - 81 x^6 - 141 x^7 + 12 x^8 - 45 x^9 + 48 x^10, 32]

Out[24]= 8 + 25 x + 22 x^2 + 20 x^3 + 12 x^4 + 24 x^5 + 15 x^6 + 19 x^7 + 12 x^8 + 19 x^9 + 16 x^10
```

- Public Key (P_U) = $8 + 25x + 22x^2 + 20x^3 + 12x^4 + 24x^5 + 15x^6 + 19x^7 + 12x^8 + 19x^9 + 16x^{10}$
- Private Key (P_R): f(x) = $-1 + x + x^2 - x^4 + x^6 + x^9 - x^{10}$
  f_p=$1 + 2x + 2x^3 + 2x^4 + x^5 + 2x^7 + x^8 + 2x^9$

II. **Message Encryption Process** Now, sender computes the ciphertext (C) using receivers public key:
Message m(x) =$1 + x^1 + x^3 + x^6$
Choose Random Polynomial r(x) = $-1 + x^2 + x^3 + x^4 - x^5 - x^7$
$P_U = 8 + 25x + 22x^2 + 20x^3 + 12x^4 + 24x^5 + 15x^6 + 19x^7 + 12x^8 + 19x^9 + 16x^{10}$
q = 32

- C= r(x) * P_U+ m(x) (mod q)
  Compute r(x) * P_U and apply the truncated concept: r(x) * P_U =$(-1 + x^2 + x^3 + x^4 - x^5 - x^7) * (8 + 25x + 22x^2 + 20x^3 + 12x^4 + 24x^5 + 15x^6 + 19x^7 + 12x^8 + 19x^9 + 16x^{10})$

```
>> conv([-1 0 1 1 1 -1 0 -1 0 0 0],[8 25 22 20 12 24 15 19 12 19 16])

ans =

    -8   -25   -14    13    43    35    14     7    -6     5   -14    23     4     8   -22   -28   -19   -16     0     0
```

$= -8 - 25x - 14x^2 + 13x^3 + 43x^4 + 35x^5 + 14x^6 + 7x^7 - 6x^8 + 5x^9 - 14x^{10} + 23x^{11} + 4x^{12} + 8x^{13} - 22x^{14} - 28x^{15} - 19x^{16} - 16x^{17}$
$= -8 - 25x - 14x^2 + 13x^3 + 43x^4 + 35x^5 + 14x^6 + 7x^7 - 6x^8 + 5x^9 - 14x^{10} + x^{11}(23 + 4x + 8x^2 - 22x^3 - 28x^4 - 19x^5 - 16x^6)$
$= 15 - 21x - 6x^2 - 9x^3 + 15x^4 + 16x^5 - 2x^6 + 7x^7 - 6x^8 + 5x^9 - 14x^{10}$
r(x) *P_U+ m(x)
$= (15 - 21x - 6x^2 - 9x^3 + 15x^4 + 16x^5 - 2x^6 + 7x^7 - 6x^8 + 5x^9 - 14x^{10}) + (1 + x^1 + x^3 + x^6$
$= 16 - 20x - 6x^2 - 8x^3 + 15x^4 + 16x^5 - x^6 + 7x^7 - 6x^8 + 5x^9 - 14x^{10}$
r(x) * P_U+ m(x) (mod 32)
$16 - 20x - 6x^2 - 8x^3 + 15x^4 + 16x^5 - x^6 + 7x^7 - 6x^8 + 5x^9 - 14x^{10} (\text{mod } 32)$
$= 16 + 12x + 26x^2 + 24x^3 + 15x^4 + 16x^5 + 31x^6 + 7x^7 + 26x^8 + 5x^9 + 18x^{10}$

After encryption process, the ciphertext (C) is:

- $C = 16 + 12x + 26x^2 + 24x^3 + 15x^4 + 16x^5 + 31x^6 + 7x^7 + 26x^8 + 5x^9 + 18x^{10}$

III. **Message Decryption Process** The receiver (N_d) received the message (m) in an unreadable form which is known as ciphertext (C). Now, the receiver (N_d) decrypts the message using own private key (P_R):
$C = 16 + 12x + 26x^2 + 24x^3 + 15x^4 + 16x^5 + 31x^6 + 7x^7 + 26x^8 + 5x^9 + 18x^{10}$
Private Key (P_R):
f(x) $= -1 + x + x^2 - x^4 + x^6 + x^9 - x^{10}$
$f_p = 1 + 2x + 2x^3 + 2x^4 + x^5 + 2x^7 + x^8 + 2x^9$
q = 32
p = 3

- P_1 = f(x) * C(mod q)
  Firstly computes f(x) * C and apply the truncated concept:
  f(x) * C= $(-1 + x + x^2 - x^4 + x^6 + x^9 - x^{10}) * (16 + 12x + 26x^2 + 24x^3 + 15x^4 + 16x^5 + 31x^6 + 7x^7 + 26x^8 + 5x^9 + 18x^{10})$

```
>> conv([-1 1 1 0 -1 0 1 0 0 1 -1],[16 12 26 24 15 16 31 7 26 5 18])

ans =

   -16     4     2    14    19    11   -10    28    23    52    -7    46    21    -7     9    20    -6    19   -21    13
```

$= -16 + 4x + 2x^2 + 14x^3 + 19x^4 + 11x^5 - 10x^6 + 28x^7 + 23x^8 + 52x^9 - 7x^{10} + 46x^{11} + 21x^{12} - 7x^{13} + 9x^{14} + 20x^{15} - 6x^{16} + 19x^{17} - 21x^{18} + 13x^{19} - 18x^{20}$
$= -16 + 4x + 2x^2 + 14x^3 + 19x^4 + 11x^5 - 10x^6 + 28x^7 + 23x^8 + 52x^9 - 7x^{10} + x^{11}(46 + 21x - 7x^2 + 9x^3 + 20x^4 - 6x^5 + 19x^6 - 21x^7 + 13x^8 - 18x^9)$
$= 30 + 25x - 5x^2 + 23x^3 + 39x^4 + 5x^5 + 9x^6 + 7x^7 + 36x^8 + 34x^9 - 7x^{10}$
f(x) * C(mod q), to reduce the coefficients between -q/2 and q/2:
$= (30 + 25x - 5x^2 + 23x^3 + 39x^4 + 5x^5 + 9x^6 + 7x^7 + 36x^8 + 34x^9 - 7x^{10})$ (mod 32)
$= 30 + 25x + 27x^2 + 23x^3 + 7x^4 + 5x^5 + 9x^6 + 7x^7 + 4x^8 + 2x^9 + 25x^{10}$
Choose the values lying between -q/2 and q/2 or between [-16,15].
$P_1 = -2 - 7x - 5x^2 - 9x^3 + 7x^4 + 5x^5 + 9x^6 + 7x^7 + 4x^8 + 2x^9 - 7x^{10}$

- $P_2 = P_1$(mod p)
  P_1(mod p), to reduce the coefficients between -p/2 and p/2:
  $= (-2 - 7x - 5x^2 - 9x^3 + 7x^4 + 5x^5 + 9x^6 + 7x^7 + 4x^8 + 2x^9 - 7x^{10})$(mod 3)
  $= 1 + 2x + x^2 + 0 + x^4 + 2x^5 + 0 + x^7 + x^8 + 2x^9 + 2x^{10}$
  $= 1 - x + x^2 + x^4 - x^5 + x^7 + x^8 - x^9 - x^{10}$
  $P_2 = 1 - x + x^2 + x^4 - x^5 + x^7 + x^8 - x^9 - x^{10}$

- Original Message m(x) = $f_p * P_2$(mod p)
  Now, compute$f_p * P_2$ and apply the truncated concept:
  $f_p * P_2$
  $= (1 + 2x + 2x^3 + 2x^4 + x^5 + 2x^7 + x^8 + 2x^9) * (1 - x + x^2 + x^4 - x^5 + x^7 + x^8 - x^9 - x^{10}) = 1 + x - x^2 + 4x^3 + x^4 + 2x^5 - x^6 + 6x^7 + 2x^8 + 3x^9 - 3x^{10} + 6x^{11} + 0x^{12} - 2x^{13} - 3x^{14} + 2x^{15} + x^{16} - x^{17} - 3x^{18} - 2x^{19}$
  $= 1 + x - x^2 + 4x^3 + x^4 + 2x^5 - x^6 + 6x^7 + 2x^8 + 3x^9 - 3x^10 + x^{11}(6 - 2x^2 - 3x^3 + 2x^4 + x^5 - x^6 - 3x^7 - 2x^8)$
  $= (7 + x - 3x^2 + x^3 + 6x^4 + 3x^5 - 2x^6 + 3x^7 + 3x^9 - 3x^{10})$

m(x) = $f_p * P_2$ (modp)
$= (7 + x - 3x^2 + x^3 + 6x^4 + 3x^5 - 2x^6 + 3x^7 + 3x^9 - 3x^{10})$(mod 3)
$= 1 + x - 0 + x^3 + 0 + 0 + x^6 + 0 + 0 + 0$
$= 1 + x + x^3 + x^6$
$= x^6 + x^3 + x + 1$

Finally, the receiver (N_d) received the original Message:
$m(x) = x^6 + x^3 + x + 1 = 01001011$
$m(x) = 01001011$

5. Security Analysis. In this part of the paper, we analyze the security of our proposed algorithm, so the proposed algorithm is able to fulfill the security requirements.

Identification and Authentication. Before joining the network, any node has to check by authenticated nodes to verifying ID to join the Opportunistic Networks. Without unique I, the node is not able to join the OppNets and can't satisfy the identification. Before accepted any node to join or carried the message needs to apply the authentication technique, in which each authenticated node will check the ID before giving the task to transmit it, if ID is found in public list of IDs that mean the node is authenticated.

Confidentiality. During the registration process of each node to ensure that nodes are not a malicious node to protect the message transferred from source to destination are only based on authorized nodes. To protect the packet confidentiality would be encryption using cryptography to ensure that only authenticated nodes can know the key and carry the message.

Integrity. Before forwarding the message to the next node, the encryption techniques generates two keys, one public key and second private key to prevent any unauthorized nodes to modify or change the message. The integrity of the message refers to protect the packet from a malicious node or unauthorized nodes

Sybil Attack. In the case of a Sybil attack, the masquerade node tries to act as an authenticated node and create the multiple fake IDs which congest the network or stealing the confidential information. The proposed approach will check the ID of every helper node which comes into the network, if helper nodes have an ID then the proposed approach will check the ID that helper node is authentic or malicious. If a helper node does not have the ID then the approach will register the new helper node and allocate the unique ID. After successful registration, the seed node will broadcast the public key (PU) of a new helper node so that every seed node could recognize the helper node. The proposed approach prevents the Sybil attack.

6. Performance Analysis. To evaluate the performance of the proposed algorithm on the basis of the following three metrics:

Delivery Ratio (D_R):. It is the ratio of the number of messages received by the receiver in respect of the number of messages created (generated) at the sender side.

$$D_R = \frac{m_{received}}{m_{created}}$$

Latency. Latency is the average end-to-end delay between sender and receiver. The low latency depicts the better performance with respect to saving the network resources.

$$Latency = \frac{T_{received} - T_{created}}{Totalofm_{created}}$$

Routing Overhead. It is the ratio between the number of messages broadcast and the number of messages received. The ample routing overhead implies the more resources utilized.

$$RoutingOverhead = \frac{m_{broadcast}}{m_{received}}$$

7. Conclusion and Future Work. In this paper, we presented the security algorithm for opportunistic networks which provides node authentication to protect and prevent from Sybil attack, malicious and unauthorized nodes. This algorithm helps and improve authentication to extend opportunistic network from heterogeneous nodes, when new node needs to join it has to contact the seed nodes, then will check the node, if it has ID then will check and compare with public list which keep all nodes ID, if found then node become authorized, if ID not found then the seed nodes will generate new ID and broadcast it to update the public list periodically, so node can join after authorized. This algorithm features enhanced authentication in Opportunistic network environments, the proposed algorithm can prevent the Sybil attack and other nodes which are not authenticated. In the future, the authors will implement the proposed algorithm in the opportunistic environment on ONE simulator.

REFERENCES

[1] M. Goyal and M. Chaudhary, *Ensuring Privacy in opportunistic Network,* IOSR J. Comput. Eng. 13 (2), 74–82, 2013.

[2] J. Solis, P. Ginzboorg, and N. Asokan,*Best-Effort Authentication for Opportunistic Networks,* 2011.

[3] Y. Ma and A. Jamalipour, *Opportunistic node authentication in intermittently connected mobile ad hoc networks,* in 2010 16th Asia-Pacific Conference on Communications, APCC 2010, 2010, 453–457

[4] A. Seth and S. Keshav, *Practical security for disconnected nodes,* 2005 First Work. Secur. Netw. Protoc. NPSec, held conjunction with ICNP 2005 13th IEEE Int. Conf. Netw. Protoc., vol. 2005, 31–36, 2005.

[5] P. Kumar, N. Chauhan, and N. Chand, *Authentication with Privacy Preservation in Opportunistic Networks,* in International Conference on Inventive Communication and Computational Technologies, 2017, no. Icicct, 183–188

[6] J. L. Tsai and N. W. Lo, *Provably secure anonymous authentication with batch verification for mobile roaming services,* Ad Hoc Networks, vol. 44, 19–31, 2016.

[7] A. Albeshri, S. A. Chaudhry, and S. Kumari, *Cryptanalysis and improvement of a Multi-server Authentication protocol by,* vol. 12, no. 1, 523–549, 2018.

[8] P. Kumar, N. Chauhan, and N. Chand, *Progress in Intelligent Computing Techniques: Theory, Practice, and Applications,* vol. 519, 465–471, 2018.

[9] R. Miller and W. Trappe, *ACE - Authenticating the Channel Estimation Process in Wireless Communication Systems,* 91–96.

[10] M. A. Shah, Sijing Zhang, C. Maple, and O. Shah,*A novel symmetric key cryptographic authentication for cooperative communication in cognitive radio networks,* 19th Int. Conf. Autom. Comput. (ICAC), 2013, no. September, 1–5, 2013.

[11] A. Ahmad, R. Doss, M. Alajeely, S. F. Al Rubeaai, and D. Ahmad, *Packet integrity defense mechanism in OppNets,* Comput. Secur., vol. 74, 71–93, 2018

[12] P. Raveneau, E. Chaput, R. Dhaou, and A. L. Beylot, *A multi-level FREAK DTN: Taking care of disconnected nodes in the IoT,* in 2016 7th International Conference on the Network of the Future, NOF 2016, 2017.

[13] A. T. A. Forwarding and S. M. Traces,*Data Forwarding In Opportunistic Network Using Mobile Traces,* In Data Forwarding In Opportunistic Network Using Mobile Traces, 2012, 425–430.

[14] S. Aluvala, K. Raja Sekhar, and D. Vodnala,*A novel technique for node authentication in mobile ad hoc networks,* Perspect. Sci., vol. 8, 680–682, 2016.

[15] P. S. Mehra, M. N. Doja, and B. Alam, *Codeword Authenticated Key Exchange (CAKE) light weight secure routing protocol for WSN*, International Journal of Communication Systems, 32 (2018).

[16] U. P. Singh and N. Chauhan, *Authentication using Trust Framework in Opportunistic Networks,* 2017.

[17] Y. Wu, Y. Zhao, M. Riguidel, G. Wang, and P. Yi, *Security and trust management in opportunistic networks: a survey,* Security and Communication Networks, vol. 8, no. 9, 1812–1827, 2015.

[18] M. Guo, H. Liaw, M. Chiu, and L. Tsai, *Authenticating with Privacy Protection in Opportunistic Networks Ming-Huang,* in EAI International Conference on Heterogeneous Networking for Quality, Reliability, Security and Robustness (QSHINE 2015), 2015, no. Qshine, 375–380.

[19] W. C. Kuo, H. J. Wei, and J. C. Cheng, *An efficient and secure anonymous mobility network authentication scheme,* J. Inf. Secur. Appl., vol. 19, no. 1, 18–24, 2014.

[20] Y. Ma and A. Jamalipour,*Opportunistic node authentication in intermittently connected mobile ad hoc networks,* in 16th Asia-Pacific Conference on Communications (APCC). IEEE, 2010, 453–457.

[21] Soleimani M, Kahvand M.*Defending packet dropping attacks based on dynamic trust model in wireless ad hoc networks.* In: Seventeenth IEEE Mediterranean Electrotechnical Conference (MELECON). 2014. p. 362–6.

[22] Niaz M, Saake G. Merkle*hash tree based techniques for data integrity of outsourced data.* In: The twenty seventh GI-workshop on foundations of databases. 2015. p. 66–71

[23] N. Asokan, K. Kostiainen, P. Ginzboorg, J. Ott, and C. Luo, *Applicability of identity-based cryptography for disruption-tolerant networking,* in Procs. 1st international MobiSys workshop on Mobile opportunistic networking. ACM, 2007, 52–56.

[24] S. Bu and H. Zhang *"Research on the method of choosing parameters for NTRU,* 1st Int. Conf. Multimed. Inf. Netw. Secur. MINES 2009, vol. 2, no. 2, 334–337, 2009.

[25] R. Jha and A. Saini *A Comparative Analysis & Enhancement of NTRU Algorithm for Network Security and Performance Improvement* Commun. Syst. Netw. , 80–84, 2011.

[26] N. Zhao and S. Su,*An improvement and a new design of algorithms for seeking the inverse of an NTRU polynomial,* Proc. - 2011 7th Int. Conf. Comput. Intell. Secur. CIS 2011, 891–895, 2011.

[27] B. N. Hien,*An Overview of the NTRU Cryptographic System. 2014.*

[28] C. M. Huang, K. C. Lan, and C. Z. Tsai,*A survey of opportunistic networks,* in Proceedings - International Conference on Advanced Information Networking and Applications, AINA, 2008, 1672–1677.

[29] M. Alajeely, R. Doss, and A. Ahmad,*Security and Trust in Opportunistic Networks – A Survey,* IETE Tech. Rev., vol. 33, no. 3, 256–268, 2016.

[30] R. M. Chaudhari, *A Survey on Attack Detection Techniques In Delay,* pp. 101–109.

Edited by: Rosilah Hassan
Received: Nov 25, 2018
Accepted: Jan 27, 2019