FACTION OF HASH FUNCTION BASED AUGUMENTING NETWORK SECURITY FOR NETWORK SERVICE SHREWDNESS

Bharanidharan R[1] and Dr.R.Santhosh Kumar [2]
Research Scholar [1, 2], Department of Computer Science and Engineering [1, 2],
Karpagam Academy of Higher Education, Coimbatore.

Abstract - *Providing security becomes more important task due to the increase of network users and cost of network resources. So consider this issue to propose a new group hash function based enhanced and maintain integrity and security of entire network. The hash function maintains various rule set, which contains set of rules with user details, IP address, public and private key, the signature for every user of the network. It manages trust node for various resources to provide security and integrity. The service providence uses a hash function to compute the signature of the network user using the details of users. The user can access any service only by registering in particular trust node which is maintained by the network. When the service request raised by the user, he will be requested for the public and private key; then the signature will be computed using a hash function. The user will be allowed to access the network resource, only after succeeding with the signature computed at request time and the signature generated at the time of registration process. The network generate new rules, which will be used to identify new kind of threats. The proposed system will give security very efficiently and work as a learning system.*

Key words:Group hash function, Security, Enhancing network, trsut node, services.

1.INTRODUCTION

Providing integrity and security becomes more important task due to the increase of network users and cost of network resources [11]. We propose a new group hash function to maintain integrity and security of entire network. The hash function maintains various rule set, which contains set of rules with user details, IP Address, public and private key, the signature for every user of the network. It manages trust node for various resources to provide security and integrity [12-13]. The service providence uses a hash function to compute the signature of the network user using the details of users. The user can access any service only by registering in particular trust node which is maintained by the network. When the service request raised by the user, he will be requested for the public and private key; then the signature will be computed using hash function [14-15]. The user will be allowed to access the network resource, only after succeeding with the signature computed at request time and the signature generated at the time of registration process.

Typically any hash function has two components: a compression function and construction. The compression function is a mapping function that transforms a larger arbitrary-size input to a smaller fixed-size output, and the construction is the method by which the compression function is being repeatedly called to process a variable length message [16-17].

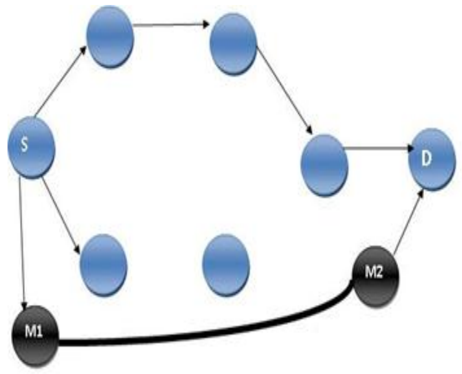


Figure 1 Network service providence path

Traditionally hash functions are being designed without any usage of a key component. However, many a few recent attacks have been successfully implemented on these traditional popular hash functions [18]. As we discussed in the previous section, security of algorithm needs to be proved, most of the newly designed algorithms are based on previously established and accepted designs with few modifications [19].

If established design promises few security aspects, the new design will automatically. In the same line, this algorithm is also based on popular MD5 design principles. Furthermore, integration of key in each round of operation of individual blocks gives more strength to the proposed algorithm against many of the known attacks on MD5 [20]. Currently, there are two methods being used to extend or strengthen the previously existing designs: First, to perform increased number of rounds of operations instead of prescribed number of functions in existing hashing algorithm (for example, instead of four primitive functions use more in case or add some advanced coding or permutation steps (for example, use more scrambling techniques second to increase the total buffer space and use different mixing step in each of the round [21-22]. Building hash functions using block ciphers, as a base, is the most popular and most widely applied method. Hash functions that use this method use a compression function that is like a block-cipher consisting of two inputs- a block of the message and a key. At present, a protocol is considered strong and secure if it requires at least operations to perform an attack on it. But it is definite that in the near future there will be a need for stronger security protocols.

The proposed solution uses integration of keyed symmetric key block encryption algorithm in each step or round of hash compression function [23]. Because symmetric key encryption algorithm works on the use of a single key, both sender and receiver use the same key. This common key may be shared between them using an encrypted link between them by Key Distribution Center (KDC) [24]. It is the responsibility of KDC to send the common session key to both sender and receiver in communication. KDC uses master keys of both parties for this purpose. Because only these two parties carry their corresponding private keys, so no other user in the network may intercept and read the original message and make use of this session key. Except for KDC and both parties, involved in the message transmission, no other user has any idea of the shared secret key [25]. Thus, this method helps in validating the identity of a source as key with sender and receiver is now same.

2.RELATED WORK

Mu Haibing, 2010, et al., The Threshold cryptography in mobile ad hoc networks using stochastic process the attack process and build an attack model firstly [1]. A dynamic evaluation model is the following which can give the proper value of threshold and updating period of sharing a secret the security mechanisms which work well for traditional fixed network are not so effective without the aid of any fixed infrastructure.

Gedare Bloom, 2017, et al., The Controller Area Network along with the recent discovery of vulnerabilities in Controller Area Network based automotive systems some of them demonstrated in practice stimulated a renewed attention to security-oriented enhancements of the Controller Area Network protocol [2].

Yongseung Lee, 2015, et al., The wireless communication technologies, the universalization of cloud services, it has become possible to provide the continuity of the content [3]. It leads to a requirement of mobility management protocols in cloud-based wireless networks, which is composed of connection between the data center and mobile devices.

K. Tamil Selvi, 2014, et al., The security is provided with the help of threshold cryptography technique [4]. The threshold cryptography is to provide security measures by distributing the secret key shares and performing encryption with those shares of secrets.

Zhiguo Ding, 2016, et al, The Non-orthogonal multiple access has been recognized As an important enabling technology to realize the challenging requirements of the fifth generation of mobile Networks multi-user network with mixed multicasting and unicasting traffic, where the base station transmits two types of data streams, one for multicasting and one for unicasting [5].

Sebastian Abt,2016, et al., The IP addresses such that later correlation is still possible without compromising the security of either data sponsoring entity two frequently applied methods are the removal of payload data and IP addresses [6].

Moustafa Ammar, 2016, et al., The integrate network layer with security middle boxes such as intrusion prevention system or Firewall to block attackers at the network edge [7]. A network designed and implemented using the servers and Mini net emulation software where a typical datacenter fat-tree topology is adopted.

Pei-Ling Chiu, 2011, et al., The visual cryptography schemes particularly for large and the development of a systematic and practical approach for threshold challenge. The pixel-expansion- free threshold approach based on an optimization technique is to encrypt binary secret images [8]. The performance metric in the evaluation of the display quality of recovered images.

Alessandro Cilardo, 2011, et al., The Threshold Logic functions directly implementable as primitive gates in the technologies mentioned above, and study their application to the domain of cryptographic computing [9]. A theoretical perspective a study on the computational power of linear threshold functions related to modular reduction and multiplication, the central operations in many cryptosystems such as and Elliptic Curve Cryptography.

Haimabati Dey, 2012, et al., The threshold cryptography gained significant attention for its theoretically proven robustness in securing such self-organized networks with resource-efficient group multicasting technique [10]. The threshold-cryptography requires node-to-node secret sharing and combining them at a later stage, both of which demands significant computational and communicational resources at the nodes.

3. PROPOSED SYSTEM

To provide enhanced security to the network environment, we designed an intelligent intrusion detection system. The Network Service Providence (NSP) maintains its own rule set using which it identifies the malformed request and provide high security-based encryption and decryption process.

3.1 KEY PROVIDENCE FOR SECURITY IN NSP:

The NSP uses many numbers of encryption keys to start the NSP in each network server. Initially, at each node of the network environment, the NSP starts key providence with the group hash function. The hash function module uses the key provided and identifies the threat. Once it identifies the threat, it generates an alert into all client.

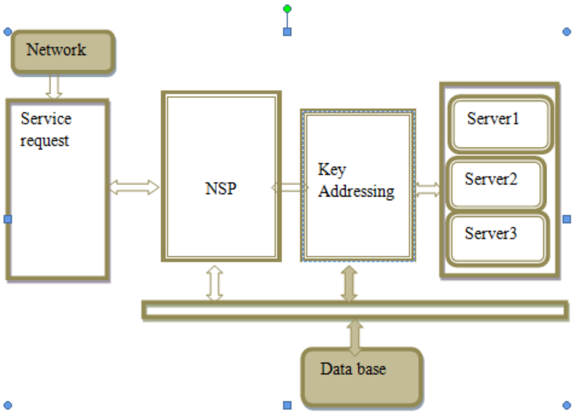


Figure 3.1 Shows the IIDS based Security enhancement

The group hash function uses a specific key agent to fetch the key generated from a various agent of the network servers and analyzes the alerts. The NSP analyses the signature of the request and verifies with the key it maintains. If it identifies any further signature from the produced alert it generates a new key and uses an agent to update the newly generated rule to the rule sets of the network intrusion detection system.

3.2 NETWORK SERVICE PROVIDER BASED ON HASH FUNCTION:

The network service provider generates a service and deploys in a hash function. Meanwhile, it generates set of encryption keys and parameters and attributes for both encryption and decryption keys. It updates the keys and users who are legible to access the service with another user. The user reads the generated keys and user details to stores it in a data base for further usage.

```
Algorithm:
Step1: Initialize service Generation Matrix $K_m$.
Step2: select randomize integer R.
Step3: identify singular matrix $S_m$.
Step4: compute Public key $P_k$ as
    If Dn = true
    $P_k=P_k+ (l× (Dn Ω K_m ))$
    Dn- first diagonal elements in the matrix $K_m$.
Step7: compute Private Key $Pr_k$ as
    $Pr_k=Pr_k+ (l× ( (Dn Ω S_m )))$.
    The size of array M.
    SDn- second diagonal elements in matrix $K_m$.
    Û- Inverse direction location of diagonal elements in matrix $K_m$.
Step8: End.
```

The fundamental concept behind hash functions in cryptography is that a digest is treated as a small representative image of given input string which can be used with an assumption that it is uniquely identifiable with that input string. This small representative image is also called an imprint, digest digital finger print, or simply the message digest. A cryptographic hash function may be taken up as a small fingerprint of the arbitrarily long message or data. If this message or data is fabricated after calculating its corresponding hash value, then this fingerprint will no longer remain valid. Thus, Cryptographic hash functions are mean to assure message integrity and a tool for message authentication too.

3.3 DEFINITIONS AND PROPERTIES OF HASH FUNCTION

The input to hash functions may be a message of any random length, but it always produces a fixed length small output, known as hash code, hash value, digest or hash. A Hash Function HASH maps bit-strings of any given length to n bit fixed length strings. A hash function HASH may be defined as-

1) HASH is a function that contains given both of the properties-

a) Compression- HASH should take the input of any given (arbitrary) length and convert it into the output of fixed and small length.

b) Ease of Computation- It should be easy to compute HASH(X) for any message X.

2) HASH is called weak collision resistant if, for a given message X, it is computationally not feasible to obtain a message X‟ which is not equal to message X: X ≠ X‟ such that HASH(X) = HASH(X‟).

3) HASH is called strong collision resistant if, it is computationally not feasible to obtain two different messages X and X' that is X ≠ X‟ such that there hash matches: HASH(X) = HASH(X‟). Obviously, strong collision resistance implies weak collision resistance too.

4) HASH is known to be one-way if, given a message digest y, it is computationally not feasible to obtain a message X such that HASH(X) = y.

5) HASH can be termed as a cryptographic hash function if it fulfills the given needs

a) To be relatively easy to calculate over any given m.

b) To be one-way.

c) To be strongly collision-resistant.

By the above stated definitions, we may formulate few basic properties of any cryptographic hash function. We assume two inputs p and p" and their respective outputs q and q": According to these properties, a hash function is treated as secure if the message cannot be traced back from its calculate a hash value and if it is weak collision resistant as well as strong collision resistant. Collision resistance property can be achieved if it is not at all possible to obtain two separate messages, which have the identical outputs. Besides these requirements, the hash function should also be able to work and calculate the digest for any input message of any size as input and the hash calculation process should also not be slow or inefficient. There may or may not be the use of a key for designing a hash function. By this criterion, two broad categories may be formalized:

1) Keyed hash functions and,

2) Unkeyed hash functions.

3.3.1 **Keyed hash functions:**

These functions make use of a key in the process of generating a hash value. Therefore, these functions require two specific inputs: (1) a message of arbitrary finite-length, and (2) a key of specific length. The fundamental approach behind this is that, if the adversary does not know the key, he must not be able to forge the message. Such type of hash functions is also known as Message Authentication Codes (MAC). The output of MAC depends on both – the message and the key. As general property of any hash function, the output of keyed hash functions is also of pre-specified length.

Definition-1: (Keyed hash functions)

"The map $HASH :\{0,1\}^* \times\{0,1\}n \rightarrow\{0,1\}m$ is said to be a keyed hash function with *m* -bit output and *n* -bit key if *H* is a deterministic function that takes two inputs, the first of an arbitrary length, the second of *n* -bit length and outputs a binary string of length *m* -bits. Where both *n, m* are positive integers. $\{0,1\}m$ and $\{0,1\}n$ are the sets of all binary strings of length *m* and *n* respectively, and $\{0,1\}^*$ is a set of all finite binary strings. Keyed hash function or MACs are majorly concerned with message integrity and source authentication both".

Algorithm:

Input: Network Trace Nt, Pattern Set Ps

Output: Null

```
Start
    Receive Packet P.
    Identify Source of packet P.
        Saddr = Source-Address(P)
    Retrieve the keyed hash network trace.
    KHNT = Nt(Ni(Loc)).
    Verify the location with the base station Bs.
    If true then
        Retrieve previous time windows pattern pi.
        Pi = Ps(Ni)@$T_{\alpha-1}$
        Compute current windows packet details.
        Tpr = ∑packets(Ni)€Nt(current Time window)
        Compute average payload Apl = (∑payload(Packets€$(Nt@T\alpha))/Tpr$
        Compute Trust Weight Tw = Tpr×Apl.
        If Tw>TTh then //TTH-Trust threshold
            Forward packet.
        end
    Else
        Drop the packet or look for another neighbor.
    End.
Stop.
```

3.3.2 Un-keyed hash functions:

These are the hash functions that do not use any key as input to generate a hash value. Most of the hash functions are un-keyed hash functions. By appending the digest to the message during the transmission, these hash functions are used for error detection. The error can be diagnosed, if the digest of the received message, at the receiving end, is not equal to the received message digest.

This is also known as Modification Detection, and thus such hash functions are also called Manipulation Detection Codes or Modification Detection Codes (MDC) or Message Integrity Codes (MIC). Infect, keyed hash functions can also be used for error detection but the un- keyed hash functions are easier to use for this application because there will not be any problem of secrecy of key used. Un- keyed hash functions are only concerned with message integrity.

```
Algorithm:
Input: Network Trace Nt.
Output: Pattern set Ps.
Start
    Read Network trace Nt.
    $Nt = \sum Logs(Nt) @ T\infty$
    Identify the set of neighbors at the period window T∞.
    Neighbor List Nl = $\sum Neighbors(Ni) @ T\infty$
    For each neighbor Ni from N
        Compute a number of packets has been received.
        $Tpr = \sum Packets€(Nt @ T\alpha)$
        Compute Unkeyed= $(\sum payload(Packets€(Nt @ T\alpha))/Tpr$
        Identify hash key of the node NLoc = Loc(Ni)
        Generate Pattern Pi = { Ni, NLoc, Tpr, Pl}.
        Add to pattern set Ps = ∑patterns(Ps)+Pi.
    End
Stop.
```

Definition-2: (Un- keyed hash functions)

"The map H:{0,1}* →{0,1}m is said to be a un- keyed hash function with m –bit output if H is a deterministic function that takes an arbitrary length message as input and outputs a binary string of length m -bit. The notations m, {0,1}m and {0,1}* are similar as that of used in Definition-1.

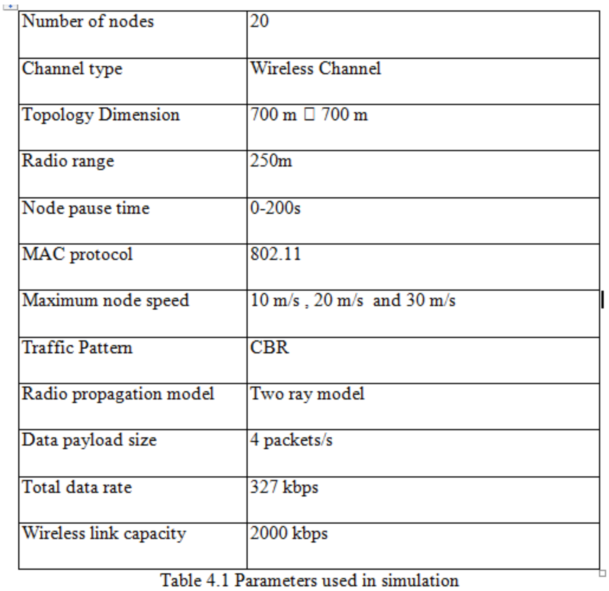
4. RESULTS AND DISCUSSION

Network Simulator 2 (NS2) is used to simulate to compare proposed secure routing algorithm FDR, TC-IP and GHF-NSP over an AODV. In this simulation, an IEEE 802.11 MAC layer and constant-bit rate (CBR) traffic over UDP are used. The simulated field configurations: 20 nodes distributed over 700 m ⍰ 700 m. The initial positions of the nodes were random. Radio propagation model according to the two-ray model. The node transmission range was 250 m. It ran simulations for constant node speeds of 10, 20 and 30 m/s, with pause time fixed at 30 s. The simulated five CBR sessions in each run, with random source and destination pairs. The following parameters are used in NS2 simulation to compare the performance metrics of FDR, TC-IP and GHF-NSP secure routing algorithm over a MANET network.

- Sending time = time consumed to send packets from MAC to the application layer.
- Accessing time = waiting time at MAC layer to access the transmission channel.
- Transmission time = time required to send a packet from the transmitter to the receiver through the physical layer.

  Packet transmission time = Packet size / Bit rate
- Propagation time = the time required for the signal to traverse through a wireless link from the transmitter to the receiver.

  Propagation time = distance / Speed of Light
- Reception time = the time when a packet is received at MAC layer of the receiver side.
- Receive time = the time when a packet is received at the application layer of the receiver side.
- Aggregate throughput: the average of successful packet delivers via a communication link.
- Drop packet: it occurs when packet loss during travelling from the source to destination.
- Efficiency of routing protocol Efficiency = (No. of acknowledged packets / No. of transmitted packets) * 100



Number of nodes	20
Channel type	Wireless Channel
Topology Dimension	700 m □ 700 m
Radio range	250m
Node pause time	0-200s
MAC protocol	802.11
Maximum node speed	10 m/s , 20 m/s and 30 m/s
Traffic Pattern	CBR
Radio propagation model	Two ray model
Data payload size	4 packets/s
Total data rate	327 kbps
Wireless link capacity	2000 kbps

Table 4.1 Parameters used in simulation

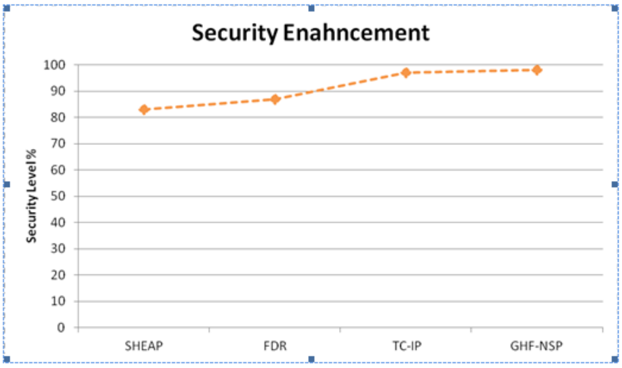


Figure 4.1: Comparison of security enhancement

Figure 4.1 shows the comparison of security enhancement produced by different methods and it shows clearly that the proposed method has provided more accuracy than others.

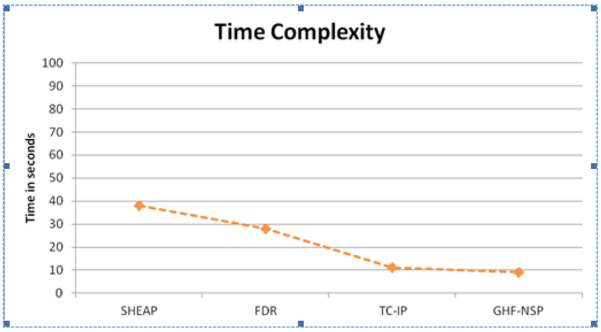


Figure 4. 2: Comparison of time complexity

Figure 4.2 shows the time complexity produced by different methods in performing security of the network and it shows clearly that the proposed method has produced less time complexity than other methods.

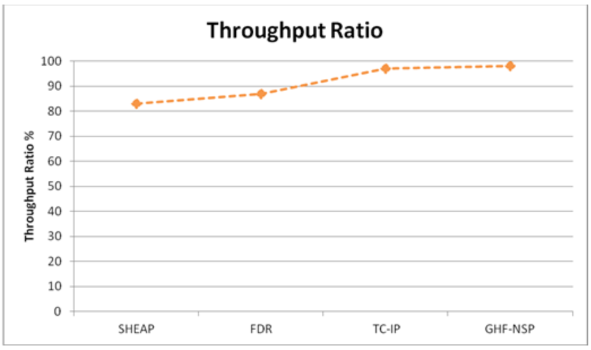


Figure 4.3: Comparison of throughput performance

Figure 4.3 shows the similar result of return ratio formed by different methods and it demonstrations clearly that the planned approach has produced more performance than other methods.

CONCLUSION

The proposed NSP uses the key which will be updated in runtime. The dynamic nature of the key makes the service providence to work efficiently. The dynamically added rule to the key is updated at each location or the network server instantly with the help of key agents. The hash function system works intelligently with the help of encryption and decryption keys. The key set is updated at each time frame or interval, so we will easily enhance the security. Finally, Simulation based experiments were conducted theoretically to further evaluate the performance of the proposed algorithm. The simulation experiments were conducted based on the Network Simulator environment. From the simulation results, it is concluded that the proposed algorithm performs better than all other existing algorithms. Finally, in our proposed system achieved the high security depends on all another factor so automatically increase the overall network performance up to 99.21% as well as delivery ratio will increase in to 98.25% in network.

REFERENCE

(1) Mu Haibing, Zhang Changlun," Security Evaluation Model for Threshold Cryptography Applications in MANET," IEEE, VOl.14, 2010.

(2) Gedare Bloom, Gianluca Cena," Supporting Security Protocols on CAN-Based Networks," IEEE, VOl.12, 2017.

(3) Yongseung Lee, Hyunseung Choo," Network Independent Mobility Management Scheme using Virtual IP Addressing," IEEE, VOl.2, 2015.

(4) K. Tamil Selvi, S.Kuppuswami," Routing Protocol for MANET using Threshold Cryptography Technique," IEEE, VOl.9, 2014.

(5) Zhiguo Ding, Zhongyuan Zhao," On the Spectral Efficiency and Security Enhancements of NOMA Assisted Multicast-Unicast Streaming," IEEE, VOl.8, 2016.

(6) Sebastian Abt,Harald Baier," Correlating Network Events and Transferring Labels in the Presence of IP Address Anonymisation," IEEE, VOl.13, 2016.

(7) Moustafa Ammar, Mohamed Rizk," A Framework for Security Enhancement in SDN-based Datacenters," IEEE, VOl.16, 2016.

(8) Pei-Ling Chiu, Kai-Hui Lee," A Simulated Annealing Algorithm for General Threshold Visual Cryptography Schemes," IEEE, VOl.13, 2011.

(9) Alessandro Cilardo, Exploring the Potential of Threshold Logic for Cryptography-Related Operations," IEEE, VOl.8, 2011.

(10) Haimabati Dey, Raja Datta," Monitoring Threshold Cryptography based Wireless Sensor Networks with Projective Plane," IEEE, VOl.9, 2012.

(11) Sukalyan Goswami, Subarna Laha," Enhancement of GSM Security Using Elliptic Curve Cryptography Algorithm," IEEE, VOl.11, 2012.

(12) Mazen G. Khair, Burak Kantarci," Towards Cellular IP Address Assignment in Wireless Heterogeneous Sensor Networks," IEEE, VOl.3, 2011.

(13) Ken-Ichi Kitayama, Masahide Sasaki," Security in Photonic Networks: Threats and Security Enhancement," IEEE, VOl.23, 2011.

(14) Vidya Krishnamoorthy, Senthilkumar Mathi," Security Enhancement of Handover Key Management Based on Media Access Control Address in 4G LTE Networks," IEEE, VOl.6, 2015.

(15)Nitish Mehta, Piyush Jadhav," Group Authentication Using Paillier Threshold Cryptography," IEEE, VOl.3, 2013.

(16) Zhao Nan, PEI Chang-xing," An Analysis of the Eavesdropping Threshold of Quantum Cryptography Protocol," IEEE, VOl.11, 2011.

(17) Frederique Oggier,Miodrag J.," An Information-Theoretic Security Evaluation of a Class of Randomized Encryption Schemes," IEEE, VOl.9, 2013.

(18) Lalita Priya, Dr. Kakali Chatterjee," A Secure Authentication Scheme in Adhoc Network Using Threshold Cryptography," IEEE, VOl.2, 2015.

(19) Hosnieh Rafiee, Ahmad AlSa'deh," Multicore-Based Auto-Scaling SEcure Neighbor Discovery for Windows Operating Systems," IEEE, VOl.5, 2012.

(20) Natasha Saini, Nitin Pandey," Enhancement of Security in Coginitive Networks," IEEE, VOl.9, 2016.

(21) M. I. Sarkar, T. K. Roy," Security Enhancement in the Receive Diversity with Co-operative Relay for Wireless Networks," IEEE, VOl.12, 2016

(22) Sushil Kr Saroj, Sanjeev Kr Chauhan," Threshold Cryptography Based Data Security in Cloud Computing," IEEE, VOl.3, 2015.

(23) K.S.Seethalakshmi, Usha B A," Security Enhancement in Image Steganography Using Neural Networks and Visual Cryptography," IEEE, VOl.6, 2016.

(24) Himanshu Sharma, Neeraj Kumar," Enhancement of security in Visual Cryptography system using Cover Image share Embedded security algorithm (CISEA)," IEEE, VOl.12, 2011.

(25) Tianhe Shen, Maode Ma," Security Enhancements on Home Area Networks in Smart Grids," IEEE, VOl.8, 2016.