Using Unique Node ID TO Control IPv6 ID Spoofing

Maytham Hakim Ali 1, Saif Al-Alak 2
Department of software, College of Science for Women, University of Babylon, Hillah, Iraq
maytham.ali@student.uobabylon.edu.iq 1, saif.mahmood@uobabylon.edu.iq 2

Abstract: Internet Protocol (IP) has a resent version knowns as (IPv6). Computers on networks could be located and identified via IP. Meanwhile, by monitoring the routing data traffic across internet. Protecting an Identity of IPV6 Packet against ID Spoofing Based on Cryptographic and Steganography techniques are proposed. One of the most considered point is the reliable communication by using security side especially in IPv6 network applications. The faced problems in general cases are DoS attack, IP-Spoofing, and commonly passive attacks types. In this paper an approach is suggested depending on generate an unique identity for each node randomly. In this work, nine experiments are implemented, which are the proposed method based on generate ipv6 address, which is passed to the chaotic logistic map and RSA function with SHA 2. The results show the proposed system provides high randomness for generated ID, and it hides identity of node inside packet.

Keywords: IPv6, Security, SHA2, RSA, IP-Spoofing, Chaotic.

1. Introduction

Information security were started to be an essential issue in digital life Developing new technologies of transmission can forces a particular strategy using for security mechanisms. In special case, for the data communication states [1]. The importance of network security is daily grown as the data size transferred across the Internet. Both of Cryptography and steganography were provide most considerable techniques for information security [2].

IPv6 is considered as the next generation of IP, that be replaced with IPv4. According to a recent article from Ars Technical, if the network moving a head the same current
rate. Which yearly adding 170 million IP for new hosts that connected to the Internet. Therefore, users will exhaust the current space of IPv4 in about 90 months. It worth mentioning that, IPv6 provide IP addresses than people could possibly ever need [3].

Encryption algorithms and chaos maps are one of the methods used for protect information and data from theft and tampering. Several researches have been conducted in this field for the purpose of protecting information through applying a numerous of coding techniques and chaos maps. On the other hand, there are cryptanalysis technologies for breaking the coding techniques for various purposes, such as stealing data for the benefit of certain entities, eavesdropping, changing them for the purpose of harm, achieving special goals and so on. [4]

In recent days, many proposed solutions that collected streams should carefully consider two main characteristics. The first one is security the mean solid end-to-end protection for secret information of the transmitting in addition to the authenticity. The second is efficiency that mathematical processes allowance to be directly applied without confidential information disclosure [5].

There are many research trends related to the proposed system, which is relevant to our topic, Ref [6] Introduce a new protocol. It is called the Identity Dynamic Access Control (IDF) filter. This protocol checks each filter value on every received frame to determine the permissions to enter the system and use system resources.

While in [7] A trueip is utilized as a system to prevent IP spoofing. By using identity-based cryptography is presented. In fact, Trueip is based on a new identity-based signature scheme to allow confirmation of an IP address. Without relying on a certificate or a public key infrastructure.

IPsec encryption is implemented in the tunnel mode between the steganogram sending and receiving gateways [8].

Besides in [9], a new description of network steganography methods. That utilize mechanisms for handling oversized IP packets: IP fragmentation, PMTUD (Path MTU Discovery) and PLPMTUD (Packetization Layer Path MTU Discovery).

As well as, in [10], AES steganography In this method, encryption is used to encode the text (which is now encrypted message), it will be injected into source address covert channel of ipv6 packet.

Also, Secure data communication using protocol steganography in ipv6 as 20 bit flow label field of ipv6 protocol used as covert channel. It’s worth mentioning that RSA
algorithm was employed for data encryption. While, the chaotic method was used for data encoding [11].

Moreover, in ref. [12] A new secure stenographic technique was presented to protect privately transmitted information. In addition, streams distributing them randomly employing a secret key.

Besides in [13], they are presented a network steganography technique. That uses IPv6 packets having zero or more. The extension headers hide secret caring data it from point to point across a network.

2. IPv6
IPv6 is the recent version of the Internet Protocol (IP) defined by the Internet Engineering Task Force (IETF). IPv6 development started in 1991 by the Internet Engineering Task Force (IETF) to deal with the long-anticipated problem of IPv4 address exhaustion. IPv6 uses a 128-bit address, allowing \(2^{128}\) or approximately \(3.4 \times 10^{38}\) addresses, or more than \(7.9 \times 10^{28}\) times as many as IPv4, which uses 32-bit addresses. IPv4 provides about 4.3 billion addresses. IPv6 is a set of specifications from the Internet Engineering Task Force (IETF) that is essentially an upgrade of IP version 4 (IPv4), a category of IP addresses in IPv4-based routing. The basics of IPv6 are similar to those of IPv4 -- devices can use IPv6 as source and destination addresses to pass packets over a network, and tools like ping work for network testing as they do in IPv4, with some slight differences [14].

2.1 IPv6 Architecture
Introducing the IPv6 packet header is easier than its IPv4 counterpart. The length of the IPv6 header increments to 40 bytes (from 20 bytes). This includes two 16-byte addresses (source and destination), preceded by 8 bytes of control information, as shown in Figure 1. [15].
In Figure 1-1 the ipv6 packet format fields as:

- **Vers** - 4-bit IP version number six.
- **Traffic class** - 8-bit traffic class value. For more information, see 1.2.3, “Traffic class” on page 14.
- **Flow label** - 20-bit field. For more information, see 1.2.4, “Flow labels” on page 15.
- **Payload length** - Packet length in bytes (excluding this header) is encoded as 16-bit unsigned integers. If the length is greater than 64 KB, this field is equal to 0 and an option header (jumbo payload) returns the correct length.
- **Next header** - Refers to the type of head immediately following the basic IP head
- **Hop limit** - 8 bits long. This field is similar to the "Time to Live" field of the IPv4 packet and determines the maximum number of hops an IP packet can move. Each device forwarding the packet reduces the field value by 1 percent. If the field value is set to 0, then the packet is discarded.
- **Source Address** - 128 bits long. This field illustrates the address of the packet originator.
- **Destination Address** - 128 bits long. This field displays the address of the packet recipient
- **Data** – specific data to sent from sender to receiver.[15]

### 2.2 IPv6 Spoofing

IP address spoofing could also be a heavy threat to legitimate Internet use. Because it is an IP-level threat that affect the higher layers of the TCP / IP protocol suite.
In IPv6 spoofing, the hacker uses tools to modify the source address in the packet header to give the receiving computer the impression that the packet is from a trusted source, e.g. another pc on a legitimate network. Since this is done at the network level, there's no external evidence of a violation so he will accept it [16].

This kind of attack is a common occurrence in a denial of service (DoS) attack that can affect a traffic computer network. During a DoS attack, hackers use spoofed information processing addresses to flood pc servers with packets of information, preventing them.

Geographically dispersed botnets networks of compromised computers are often utilized to send packets. Each botnet has doubtful thousands of computers capable of spoofing multiple source addresses. As a result, automatic attacks are difficult to discover [17]

**IPv6 spoofing Types:**
IP spoofing detection and prevention can be categorized as :

A- Host based
B- Router based
C- Combinational methods.[18]

Hosts have implemented host-based methods. This allows hosts to identify spoofed packets. They offer the convenience of easily deploying existing infrastructure without any changes. In addition, their response is slow, as a result of fake packets, the host must be reached before it can be detected. Most router-based technologies are built into routers, and counterfeit packets are detected before they reach their destination. Router-based methods are more efficient compared to host-based methods, but the efficiency of the system depends on the overall involvement of routers [18].

### 2.3 Anti-Spoofing Features in IPv6
IPv6 has been designed by IETF to overcome these limitations of IPv4 that surfaced during its use. It has added new features some of which provide more adequate spoofing control mechanisms than those in IPv4 [19]. These include:

A- **Large Address Space:** Internet address space has been extended in IPv6 to 128 bits in comparison to 32 bits in IPv4. This address space provides 2128(i.e. 3.4X1034) unique addresses in comparison to 232(i.e.4.3X109) address space in IPv4. Therefore, address translation techniques such as Network address translation (NAT), Port Address
Translation (PAT), address classes, and Classless Inter-Domain Routing (CIDR) used in IPv4 networks are no longer required. Extremely larger address space makes address scanning difficult in IPv6 networks which considerably reduces the chance of spoofing [19].

B- **Streamlined Header Format:** IPv6 header structure is much less complex and streamlined than IPv4 header. It comprises of eight fields in comparison to thirteen in IPv4. Three header fields namely version, source address, and destination address have not been changed while as five header field namely IHL, identification, flags, fragment offset, and header checksum have been removed. The names of four header fields namely type of service, total length, protocol and time to live have been respectively renamed to traffic class, payload length, next header and hop limit. The position of these fields have also changed. Further, flow label field has been added. IP packets in IPv6 are processed fast, efficiently and securely which requires less time that considerably reduces the chance of IP spoofing extremely [20].

C- **Extension Headers:** All optional fields of IPv4 have been moved to extension field in IPv6. This change allows fast and efficient processing of packets as processing of these optional fields is done in a sequential order only if required. The extension field includes field names Hop-by-Hop, Routing Header, Fragmentation Header, Destination Options Header, Authentication Header (AH), and Encapsulating Security Payload (ESP) headers are all specified from the "Next Header" field of the IPv6 packet. Chances of IP address spoofing can be minimized as Extension Header processing has become fast, efficient and secure using IPsec (AH & ESP)[21].

D- **Efficient Addressing:** IPv6 has efficient address schemes like Unicast, Multicast, and any cast. A packet is routed to an interface that identifies it on a network or subnet using unicast addressing. The packet is delivered to the host in the group for which it is intended and others do not receive it in multicast addressing. In any cast addressing mechanism, a packet is assigned to the nearest group member in the network (Blanchett, 2003). Unlike IPv4, IPv6 does not have a broadcast address where a packet is delivered to all nodes in the network. This considerably reduces the possibility of IP addresses spoofing [22].

E- **Stateless and Stateful Address Configuration:** The rapid growth of Internet demands some mechanism for automatic address configuration. Improved Dynamic Host Control Protocol DHCPv6 makes two types of automatic address configurations namely stateless address auto configuration and tasteful auto-address
configuration available in IPv6. As manual address configuration is not permitted in IPv6, IP related threats are therefore minimized [23].

F- **Better QoS:** Internet protocol does not guarantee delivery of packets at destinations and is thus unreliable but it makes best efforts not only to make the packets delivered fast at destinations. IPv6 and IPv4 both include features for quality of service but in IPv6 two fields namely traffic class and flow label have been set aside to prioritize the delivery of IP packets. These fields prioritize time sensitive packets such as video, voice over IP (VOIP), and teleconferencing packets. Therefore, IPv6 has better quality of service. Due to prioritizing of particular packet flow, IP level threats like IP spoofing can therefore be minimized [24].

G- **Fragmentation at Nodes:** In IPv6, the fragmentation of packets occurs only at the source host, which are reassembled at the destination host. This not only avoids resending of entire packet in case some fragmented packet gets corrupt or lost but also minimizes fragmentation attacks in comparison to that in IPv4 networks [25].

H- **Mobile IPv6 (MIPv6):** MIPv6 has an additional benefit over IPv6 in that it allows for mobile nodes. IPv6 has a large address space and can accommodate the increasing number of mobile devices. IPv6 addresses the handover problem without interrupting the IP level and reduces security problems for mobile devices by using the Neighbour Discovery (ND) protocol [26].

I- **Inbuilt Security:** An important feature of IPv6 is its essential security protocol, IPsec, which protects communications over IP and other upper layers. IPsec is a combination of security protocols and many other components of security. This ensures the privacy, integrity and authenticity of IP packets, thus protecting IP packets from IP address forgery. Data protection is provided through the next header (Kent, CEO, 2006 K Kent, 2005A; Kent, 2005B) IPsec works in two modes: transport mode and tunnel mode. Transport mode encrypts packet payloads whereas tunnel mode encrypts entire packets [27].

J- **Extensibility Features offered by IPv6:** are extensible by addition of new fields to its extension header [28].

3. **The proposed system**

The proposed method based on the unique IPv6 identity, as the process of generate identity unique and suggest hide identity in extension header, the random unique identity generation by using set of transformation IP address node by encryption, and chaotic transformation methods.
The proposed system block diagram explained as follow:

In the first place, the system will generate random address as IPv6 with 16 bytes, as an identity between sender and receiver. Chaotic (Logistic Map) used to scattered address in a chaotic manner and gives random address.

RSA Algorithm used to encrypt the resulted values from Chaotic. While Hash (SHA2) used to provide a unique address which is difficult to alteration.

---

**Table 1: Secure system setting**

| Experiment Number | RSA key size | Hash function |
|-------------------|--------------|---------------|
| 1                 | 512 bit      | MD5 512       |
| 2                 | 1024 bit     | MD5 512       |
| 3                 | 2048 bit     | MD5 512       |
| 4                 | 512 bit      | SHA2 256      |
| 5                 | 1024 bit     | SHA2 256      |
| 6                 | 2048 bit     | SHA2 256      |
| 7                 | 512 bit      | SHA2 512      |
| 8                 | 1024 bit     | SHA2 512      |
| 9                 | 2048 bit     | SHA2 512      |

Extension headers should not be viewed as a special IPv6 feature that will only show in later stages of network and service deployment. Extension headers are associate integral a district of the IPv6 protocol and support some infrastructure and services [29].

The following is a list of circumstances where EHS are commonly used:

**A. Hop-by-Hop:** EH is used to support Jumbo Grams or, with the Router Alert option, which is an integral part of MLD operation. Router notification is an integral part of IPv6 multicast operations for Multicast Listener Discovery (MLD) and Resource Reservation Protocol (RSVP) for IPv6 [29].
B. **Destination EH**: is used in IPv6 Mobility as well as support of certain applications.

C. **Routing EH** is used in IPv6 Mobility and in Source Routing. It may be necessary to disable “IPv6 source routing” on routers to protect against DDoS.

D. **Fragmentation EH** is essential to maintain communication using fragmented packets (in IPv6, the source of traffic must be fragmented; routers do not fragment the packets they send).

E. **Mobility EH** is utilized in support of Mobile IPv6 service [30].

F. **Authentication EH** is similar in format and use to the IPv4 authentication header specified in RFC2402 [31].

G. **Encapsulating Security Payload EH** The IPv4 defined in RFC2406 is similar to the format and use of ESP headers. All information is encrypted after Encapsulation Security Header (ESH) and is therefore not available for intermediate network devices. ESH can be followed by additional destination parameters EH and a top-level datagram [32]. The proposed method showed as in the Figure.

The extension header was introduced in IP version6. The extension header mechanism could be an important part of the IPv6 design. Following field of IPv6 points the primary header to the primary extension header, and this extension header points to the second extension header, and so on.

The proposed method based on hide ipv6 identity in extension header within encapsulation field to carry encrypted data.

Figure 3 show the IPv6 header with next header field transfer from one next header to another one to get extension header one and then extension header two and so on.

![Figure 3: Extension Header transferring from one header to another next header.](image)

| VER | TRAFFIC CLASS | FLOW LABEL |
|-----|---------------|------------|
|     | PAYLOAD LENGTH | NEXT HEADER | HOP LIMIT |
|     | SOURCE ADDRESS |            |           |
|     | DESTINATION ADDRESS |          |           |

![Figure 4: The proposed Extension Header for Hide ipv6 Identity.](image)
4. Results

The results show the state of Fail, Doubt and Safe based on DieHard.

The proposed number of input values as 215 for each experiment, and the best result showed in Experiment 8 with Fail (34) and Safe (114). The RSA key size used between 512 bits to 2048 bits, Hash Function method as MD5 as 512 bits and Hash Function as SHA2 256 bits to 512 bits.

To measure the effectiveness and strength of the secret keys generated by the proposed method, the work calculates randomness. The first test of randomness is performed by using a Diehard statistical test, which consists of 15 tests. The result of statistical tests, called p-values are computed between [0,1) depending on distributing for the random variable. The area divided into three parts (safe, doubt, fail). The p-values in the fail area should diminish, and the p-values should increase in the safe area, to get better randomness and to increase the security.

Table 2: The experiment case study.

| No.Expr | No.Input Value | RSA Key Size | HASH Function | Fail | Doubt | Safe |
|---------|----------------|--------------|---------------|------|-------|------|
| expr1   | 512 bit        | MD5 512      | 46            | 54   | 115   |
| expr2   | 1024 bit       | MD5 512      | 39            | 68   | 108   |
| expr3   | 2048 bit       | MD5 512      | 44            | 62   | 109   |
| expr4   | 512 bit        | SHA2 256     | 43            | 62   | 110   |
| expr5   | 1024 bit       | SHA2 257     | 40            | 64   | 111   |
| expr6   | 2048 bit       | SHA2 258     | 50            | 61   | 104   |
| expr7   | 512 bit        | SHA2 512     | 40            | 66   | 109   |
| expr8   | 1024 bit       | SHA2 512     | 34            | 67   | 114   |
| expr9   | 2048 bit       | SHA2 512     | 43            | 61   | 111   |

Besides, the Figure 5, showed the proposed 9 experiments and based on the three cases as Fail, Doubt and Safe.
While the results of Randomness Test explained as the ID would be produced by executing a chaotic and PUBLIC KEY encryption in Java programming language. The total size of generated IDs should be 11-12 MB to be tested by DieHard. DieHard is producing 255 p-values between (0,1]. The randomness of an algorithm's performance is one of the most crucial factors in determining its security. The diehard tests are carried out by the quest. Diehard is a collection of statistical tests created by Marsaglia to measure the quality of a random number generator. It consists of 15 statistical tests. These tests use a p-value to break the set-down into three categories: safe, doubt, and failure. The following regions can be used to describe these areas: In the region of Doubt, there are (0.1 p-values 0.25 or 0.75 p-value > 0.9). (0 < p-value ≤0.1 or 0.9 ≤ p-value ≤ 1) in the failure area. In a safe area, a p-value of 0.25 to 0.75.[5].

The best result shows in experiment 8 as showed in figure 6.
Figure 6: Randomness of IPv6.

Besides the Information Entropy explained as: The entropy $H(m)$ of a message $m$ can be calculated as follows.

$$H(m) = \sum_{i=1}^{2^n} p(m_i) \log_2 \left( \frac{1}{p(m_i)} \right)$$

Where $n$ is the number of message bits $m$, $2^n$ represents all possible symbols, $p(m_i)$ represents the probability $m_i$ [14].

While the Entropy of each experiment value

| Number of Experiment | Entropy        |
|----------------------|---------------|
| expr1                | 7.999983594  |
| expr2                | 7.999982477  |
| expr3                | 7.999985109  |
| expr4                | 7.999982994  |
| expr5                | 7.999981262  |
| expr6                | 7.99998451   |
| expr7                | 7.999983194  |
| expr8                | 7.999983     |
| expr9                | 7.999980717  |

While the Figure below show the table of the Entropy values.
Figure 7: Entropy results.
While the best result of Histogram values of Experiment 8 explained as:

| expr1 | expr2 | expr3 | expr4 | expr5 | expr6 | expr7 | expr8 | expr9 |
|-------|-------|-------|-------|-------|-------|-------|-------|-------|
| 7.999978 | 7.999979 | 7.999980 | 7.999981 | 7.999982 | 7.999983 | 7.999984 | 7.999985 | 7.999986 |

- Repeated Hexa
- ASCII of Hexa values
- Result of Experiment 1
Result of Experiment 3

Result of Experiment 4

Result of Experiment 5

Result of Experiment 6

Result of Experiment 7

Result of Experiment 8
5. Conclusion

The contributions of the work can be summarized by the following points: Implementing SHA2 Hash algorithm and RSA with chaotic. Also, using RSA key size from 512 to 2048 and Hash function MD5 512. The ID would be produced by executing a chaotic and PUBLIC KEY encryption in Java programming language. Enhancement the security based on the Randomness Test. As, attackers are using many different ways to inject their forgery packets inside a network to achieve DoS attack. Receiver nodes are using many techniques to distinguish forgery packets from real packets to detect a DoS attack. The proposed system implements with Java tool kit (Netbeans 8.2), Diehard to measure the quality of a random number generator and MATLAB to get Entropy and Histogram values.

References

[1] Levi, M., & Wall, D. S. (2004). Technologies, security, and privacy in the post- 9/11 European information society. Journal of law and society, 31(2), 194-220.
[2] Abdullah, A. M., & Aziz, R. H. H. (2016). New approaches to encrypt and decrypt data in image using cryptography and steganography algorithm. International Journal of Computer Applications, 143(4), 11-17.
[3] Bambauer, D. (2011). Conundrum. Minn. L. Rev., 96, 584.
[4] Hurrah, N. N., Parah, S. A., Loan, N. A., Sheikh, J. A., Elhoseny, M., & Muhammad, K. (2019). Dual watermarking framework for privacy protection and content Authentication of multimedia. Future Generation Computer Systems, 94, 654-673.
[5] Naeem, M. M., Hussain, I., & Missen, M. M. S. (2020). A survey on registration hijacking attack consequences and protection for Session Initiation Protocol (SIP). Computer Networks, 175, 107250.
[6] Wang, C. C., Wu, C. H., & Irwin, J. D. (2004, March). Using an identity-based dynamic access control filter (IDF) to defend against DoS attacks. In 2004 IEEE Wireless Communications and Networking Conference (IEEE Cat. No. 04TH8733) (Vol.1, pp. 639-645). IEEE.

[7] Schridde, C., Smith, M., & Freisleben, B. (2009, October). TrueIP: prevention of IP spoofing attacks using identity-based cryptography. In Proceedings of the 2nd International Conference on Security of Information and Networks (pp. 128-137).

[8] Shehab, M. A., & Korany, N. O. (2012, May). New Steganographic Method for Data Hiding in the IP ID Field. In The International Conference on Electrical Engineering (Vol. 8, No. 8th International Conference on Electrical Engineering ICEENG 2012, pp. 1-14). Military Technical College.

[9] Dhokate, M. D. D., & Ghorpade, V. R. Data Hiding With Multiple Network Protocol Usage.

[10] Cabaj, K., Caviglione, L., Mazurczyk, W., Wendzel, S., Woodward, A., & Zander, S. (2018). The new threats of information hiding: The road ahead. IT professional, 20(3), 31-39.

[11] Tian, J., Xiong, G., Li, Z., & Gou, G. (2020). A Survey of Key Technologies for Constructing Network Covert Channel. Security and Communication Networks, 2020.

[12] Özçelik, İ., & Brooks, R. (2020). Distributed denial of service attacks: Real- world detection and mitigation. CRC Press.

[13] Bedi, P., & Dua, A. (2020, May). Network Steganography Using Extension Headers in IPv6. In International Conference on Information, Communication and Computing Technology (pp. 98-110). Springer, Singapore.

[14] Thaler, D., Draves, R., Matsumoto, A., & Chown, T. (2012). Default address selection for internet protocol version 6 (IPv6). RFC6724, IETF.

[15] Ludovici, A., Calveras, A., Catalan, M., Gómez, C., & Paradells, J. (2009, September). Implementation and evaluation of the enhanced header compression (IPHC) for 6LoWPAN. In Meeting of the European Network of Universities and Companies in Information and Communication Engineering (pp. 168-177). Springer, Berlin, Heidelberg.

[16] Banday, M. T., & Mathangi, R. A. (2015). Control of IP Address Spoofing-A Comparative Study of IPv4 and IPv6 Networks.

[17] Gupta, B. B., & Badve, O. P. (2017). Taxonomy of DoS and DDoS attacks and desirable defense mechanism in a cloud computing environment. Neural Computing and Applications, 28(12), 3655-3682.
[18] Park, K., & Lee, H. (2001). On the effectiveness of route-based packet filtering for distributed DoS attack prevention in power-law internets. ACM SIGCOMM computer communication review, 31(4), 15-26.

[19] Banday, M. T., & Mathangi, R. A. (2015). Control of IP Address Spoofing-A Comparative Study of IPv4 and IPv6 Networks.

[20] Lee, H. W., Yun, S. H., Kim, J. S., Oh, N. H., & Kim, D. H. (2005, May). IPv6/IPsec conformance test management system with formal description technique. In International Conference on Computational Science and Its Applications (pp. 401-410). Springer, Berlin, Heidelberg.

[21] Kent, S., & Atkinson, R. (1998). IP authentication header.

[22] Metz, C. (2002). IP anycast point-to-(any) point communication. IEEE Internet computing, 6(2), 94-98.

[23] Berko, I. S. (2014). An Analysis of the Risk Exposure of Adopting IPv6 in Enterprise Networks (Doctoral dissertation, Rhodes University).

[24] Xiao, X., & Ni, L. M. (1999). Internet QoS: A big picture. IEEE network, 13(2), 8-18.

[25] Jankiewicz, E., Loughney, J., & Narten, T. (2011). Ipv6 node requirements. IETF Request for Comment, 6434.

[26] Al-Surmi, I., Othman, M., & Ali, B. M. (2012). Mobility management for IP-based next generation mobile networks: Review, challenge and perspective. Journal of Network and computer Applications, 35(1), 295-315.

[27] Keoh, S. L., Kumar, S. S., & Tschofenig, H. (2014). Securing the internet of things: A standardization perspective. IEEE Internet of things Journal, 1(3), 265-275.

[28] Risso, F., & Baldi, M. (2006). NetPDL: an extensible XML-based language for packet header description. Computer Networks, 50(5), 688-706.

[29] McClain, J. W. (2014). IPv6 is More Than Addresses.

[30] Hoang, T. D. (2015). Deployment IPv6 over IPv4 network infrastructure.

[31] Kent, S., & Atkinson, R. (1998). IP authentication header.

[32] Amoss, J. J., & Minoli, D. (2007). Handbook of IPv4 to IPv6 transition: Methodologies for institutional and corporate networks. CRC Press.