**Research Article**

# A New Mechanism for Generating an Ipv6 Address in IoT Context

**Ali EL KSIMI\* and Cherkaoui LEGHRIS**

*University Hassan II, Casablanca, Morocco*

**\*Corresponding author:** Ali El Ksimi, L@M, RTM team, FST Mohammedia, University Hassan II, Casablanca, Morocco

## Abstract

As objects connected to the Internet multiply, it is likely that the stateless IPv6 autoconfiguration service will finally be used on a large scale. Autoconfiguration aims to reduce the efforts of integrating machines into the local network to connect them to the internet. It is based on the mechanism of neighbour discovery (NDP: Neighbour Discovery Protocol) and does not require any administrative management of the assigned addresses. In this sense, one of the methods used to generate an IPv6 address is based on the physical address of the machine. However, this has resulted in privacy issues for many users. The latter are concerned that it is possible to go back to the physical computer by analysing the packets. Several approaches are proposed in the literature. In this paper, we propose a new mechanism for generating an IPv6 address using ID tag RFID. The results of our method show the better performance in terms of time complexity.

## Introduction

The IoT technologies are going to transform the entire society, including ourselves. With the emergence of many Internet connected objects, we have indeed a new dimension of our presence in the world: we find out, work, play, eat and are conducting a number of different activities on the net. This digital life is characterized by its immediacy, density information, omnipresence, in contrast to the world of things; it's a new real world. Given that in the coming years, all objects will be connected to the internet, it is recommended to use a technology that will be the best solution to ad-dress them. In this paper, we focused on RFID technology to this fact. It is based on the exchange of information carried by electromagnetic waves between a label, or rated "tag", and a reader. Today, there are thousands in the number of applications which include RFID. Transforming the identifier tag in IPv6 address will enable small objects to communicate via internet. The main point of having IoT (internet of things) devices is that they can interconnect, and communicate with one another or with the Internet. IoT devices are thus typically equipped with one (or more) network interfaces [1]. In this paper, we propose a new mechanism to generate an IPv6 address the IPv6 address using the RFID tag ID. The rest of this paper is organized as follows: In section 2, we present a related work to our research field. In section 3, we study an overview of

IPv6 autoconfiguration while in section 4; we show our proposed algorithm. In section 5, we show the implementation and results evaluation. A conclusion and perspectives are provided in last section.

## Related Work

Many objects used in our life don't have microprocessors and therefore, cannot join a computer network. Using RFID technology and tag integration in objects, this communication will be possible. The Internet of Things includes many technologies, some of which were invented many years ago and others of which are modern. Among the enabling technologies and protocols IoT, we quote: Wireless sensor networks (WSN), Radio frequency identification (RFID) [2], Wi-Fi type wireless network [3], routing protocol for low power and low loss networks (RPL) [4,5], 6LowPAN [6-9], IEEE 802.15.4 [10], Bluetooth Low-Energy (BLE) [11-13]. Gyanendra [14] have presented a survey of IPv6 challenges and they show a comparison of IPv6 addressing schemes in IoT context. The authors of [15] have provide a survey on subjecting Electronic Product Code and non-ID objects to IP identification for IoT devices. The solution proposed by the authors of [16] is based on the idea of generating a unique virtual 48-bit MAC address based on the identifier of the RFID tag. The generated address can be used by the DHCP server

to dynamically assign IP addresses to RFID tags. However, it is not clear that this mechanism supports all the different EPC classes. Consequently, the scalability and adaptability of this mechanism remain low. The authors in [17] provided a new method based on EPC [18] mapping to produce an IPv6 addressing mechanism for objects. They first used EUI-64 B and then replaced the EUI with 64-bit EPC to obtain a hierarchical method; they merged the 64-bit network prefix with 64-bit EPC to produce an IPv6 (128-bit) address. However, one of the biggest disadvantages of this method is that it only works with 64-bit EPC and does not support different sizes of EPC.

Another addressing method based on cryptographically generated addresses (CGA) was introduced in [19]. This method uses the EPC code EM1400 as host ID and combines it with 64 bits of Net ID. Three scenarios can occur during EPC mapping. When the mapped EPC is less than 64 bits, the mechanism adds zeros paddings. Otherwise, if it is equal to 64 bits, it will be used without any manipulation. Finally, if it is larger than 64 bits, the mechanism uses compression strategies. This method supports RFID tags for addressing, and it is also a hierarchical addressing method. In addition, it is simple and there is no need for additional hardware for implementation. However, the reason for categorizing this method in the CGA group is that the mechanism uses hash functions to compress long EPCs. The use of hash functions results in additional computation costs and increases the process time for mapping and allocating creation time of the IPv6 address. In Aljosha Judmayer [20], the authors have proposed a novel algorithm for IoT devices addressing. It is lightweight in operation, requires minimal administration overhead, and defends against reconnaissance attacks; address based correlation as well as denial-of-service attacks. The integration of RFID with the mobile phone was presented in [21]. The purpose of this work is to avoid wasted time in the servers by using the mobile phone as a reader. Regarding the mechanism, the mobile phone reads the tag identifier and the data from the memory in order to find the IPv6 in the tag. It recognizes

the global EPC in case of existence of IPv6. But if there were no IPv6, the mobile phone would build the IPv6 format using 64 bits of Net ID and 64 bits of host, and deliver the generated IPv6 address to the RFID tag. However, in this method, the mobile phone must support the IPv6 format, which reduces the adaptability of this mechanism.

The authors of [22] proposed an IPv6 addressing method, supported by mobile communications. This method uses MIPv6 (Mobile IPv6) on the reader side. MIPv6 [23] needs a manager called home agent (HA) for addresses. HA stores the reader subnet prefix, which is derived from the tag ID. Then HA provides the subnet prefix to the corresponding node (CN). CN sends IP address to reader via message. Then the reader passes the message to the tag, so that it begins to create an IPv6 address. Finally, the IPv6 address obtained will be sent back to CN in the form of an acknowledgment message. However, we can conclude from the different studied works that the generation of IPv6 address requires either extra nodes in the network to construct network addresses or additional functionalities to RFID readers residing at the network edge, and increases the process time for mapping and allocating generation time of the IPv6 address. In our paper, we used another different method that could generate easily the IPv6 address which minimizes the time complexity of algorithm.

## RFID Technology and Ipv6 Autoconfiguration

### RFID technology

Radiofrequency identification (RFID) [24] technology has gained a lot of attention in recent years. RFID is an automatic system that stores/retrieves data in/from devices called RFID tags. RFID tags can be attached to anything that includes products, animals or even humans for identification purposes. Each RFID tag has two parts: a chip for data processing and an antenna for sending/receiving signals. There are three types of RFID tags: active tags, passive tags and semi-passive tags. Table 1 briefly shows the differences between these three types of RFID tags.

**Table 1:** Differences between three types of RFID tags.

| TAG RFID | Active | Passive | Semi passive |
| --- | --- | --- | --- |
| Battery required | Yes | No | Yes |
| Range | Up to hundreds of meters | Up to a few meters | Up to hundreds of meters |
| Cost | High | Low | Medium |
| Size | Large | Small | Medium |
| Storage capacity | High | Low | Low |

### IPv6 autoconfiguration (EUI-64 method)

Among the methods used in IPv6 autoconfiguration is EUI-64 [25]. "Extended Unique Identifier" is a way of forming IPv6 addresses of unicast type. This method of generating addresses is unique because it is based on the MAC address of the device. As

a reminder, MAC addresses are unique identifiers. Concretely, this allows a device to assign itself an IPv6 address. It is a plus compared to IPv4 which required to the stations, to have an IP in order to communicate, to locate a DHCP server and to ask for an IP. We will now see how an IPv6 address in EUI-64 is calculated. The Figure 1 shows the steps of this method.
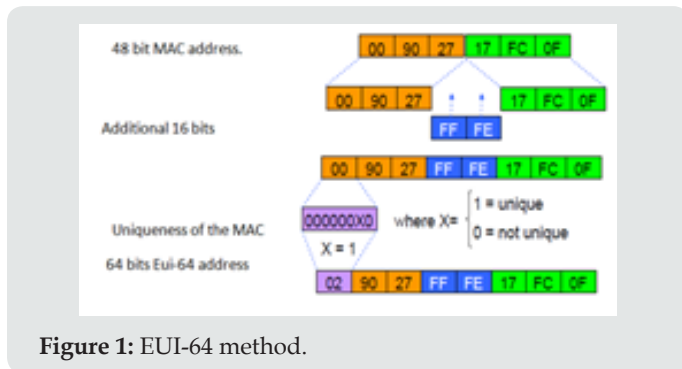
**Figure 1:** EUI-64 method.



**Figure 2:** CGA Generation Algorithm.

We can therefore see that the process of forming the IPv6 address in EUI-64 is done in three steps:

1. First, we take the prefix which is "FE80:0000:0000:0000" and the MAC address "0090: 2717: FC0F" of the network card concerned. They are combined by taking the prefix + first 3 bytes of the MAC address + FFFE + last 3 bytes of the MAC address.

2. Then, we make a modification on the seventh bit of the third byte on which we will make a "+1" thus modifying its value in decimal.

3. Finally, we write the final IPv6 address by removing the unnecessary "0".

The disadvantage of this method is that it uses the interface identifier from the MAC address, because even if we change the network, the Host part remains stable.

### CGA IPv6 address generation

In order to generate a CGA [26], the node must build a data structure called CGA Parameters. It is on this data structure that will later be called the hash function as shown in Figure 2.

1. A modifier: this is a random number encoded on 128 bits. This increases the security of the address as well as the hazard of the address.

2. A subnet prefix copies the subnet prefix part of the address (the leftmost 64 bits).

3. A collision counter, on 8 bits, encodes the number of collisions detected during the DAD (Duplicate Address Detection) [27].

4. The public key field contains the public key of the node.

5. The extension fields allow CGA addresses to be extended to new uses.

The generation of the CGA address consists in calculating two condensates (or hash), named hash1 and hash2, on different parts of the CGA Parameters data structure. The algorithm for generating a new CGA address is illustrated in Figure 2.
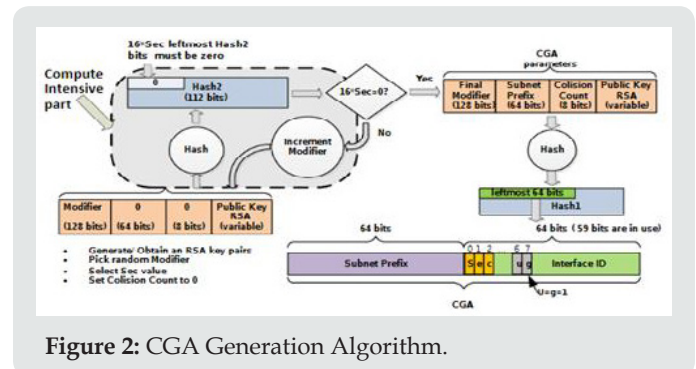
In our paper, we suggest another method based on the ID tag and the equivalence function.

## The Proposed Mechanism

The principle of our mechanism consists in using the operator XNOR [28]. Indeed, to generate the IPv6 address from the tag, we will use the operator XNOR whose two operands are the Net ID of the network, and the ID of the tag.

### NOR (equivalence function)

The logical operator XNOR uses two operands, which can each have the value TRUE or FALSE; it combines a result which is TRUE only if the two operands have identical values. The operator XNOR is defined by its truth table, which indicates for all possible values of A and B, the value of the result R as follows Table 2.

**Table 2:** XNOR truth table.

| A | B | R= A XNOR B |
|---|---|---|
| 0 | 0 | 1 |
| 0 | 1 | 0 |
| 1 | 0 | 0 |
| 1 | 1 | 1 |

As we can see, the logical XNOR can be defined by the following sentence: "The result is TRUE if and only if the two entries are identical".

### He process of the proposed mechanism

Communication between objects and corresponding nodes on the network is essential for exchanging update information and data. However, objects with an RFID tag cannot reach the network because they need an Internet address such as IPv6 [29]. In this section, we propose a mechanism to generate an IPv6 address for RFID tags based on their unique identifiers. So, to do that, we will use the operator XNOR whose two operands are the Net ID and the ID of the tag.

There are three cases depending on the length of the tag identifier:

1. The length of the tag identifier is less than 64 bits.

2. The length of the tag identifier is 64 bits.

3. The length of the tag identifier is greater than 64 bits.

In the first case, to obtain the 64 bits, we add to the identifier of the tag a zero on the left. In the second case, we directly use the 64 bits of the tag ID. However, in the third case, the length of the ID exceeds 64 bits; we use the CRC-64 hash function. After obtaining the ID with 64 bits, we use the operator XNOR with the network ID to generate the host ID of the tag's IPv6 address. Since the XNOR function is bijective, i.e. f (x) = f (y) => x = y, this implies that the code generated by the function will be unique.

Therefore, this solution will overcome many problems and restrictions presented by other IPv6 address generation algorithms, such as:

1. The generated address will be a routable address since the network ID of the network is always preserved.

2. Less computational complexity.

3. The address is unique, which implies that the collision problem is not probable, as well as the risk that a tag could have two different addresses if it is present in the interrogation range of two readers is out of the question.

4. The tag identifier is easily retrievable from its IPv6 address (the operator XNOR in both directions), due to this property; C = A XNOR B => B = C XNOR      A.

5. No additional devices.
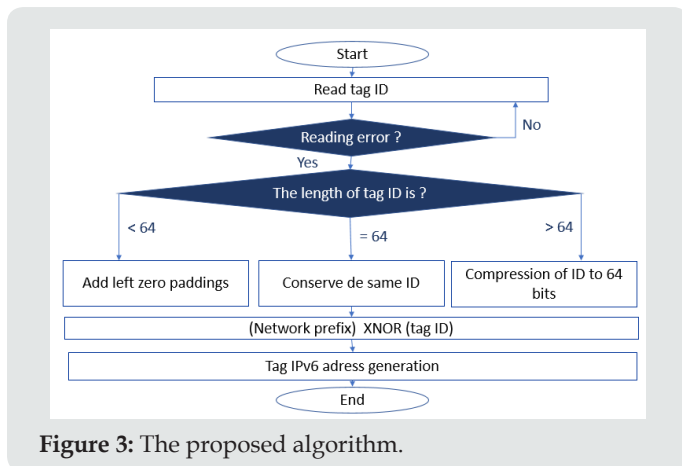
## Middleware application



**Figure 3:** The proposed algorithm.

To implement your solution, we have developed a middleware application. First, the reader will read the RFID tag identifier, and then send it to the RFID host (HR). The latter is an application linked to the reader; it is responsible for converting the tag identifier into an IPv6 address. It also allows the storage of tag identifiers in a database. Then, it sends an RS message (Router Solicitation) to the router which provides it with the Netid identifier (the network prefix) to generate an IPv6 address. The HR generates a unique IPv6

address interface identifier according to the algorithm proposed in Figure 2 and adds it to the network ID received from the router to generate the IPv6 address of the RFID tag. The address generation process is illustrated in Figure 3.

## Implementation and Evaluation

### Network topology

The architecture of the proposed mechanism is illustrated in Figure 4. It consists of the following elements:

1. RFID tag.

2. RFID reader.
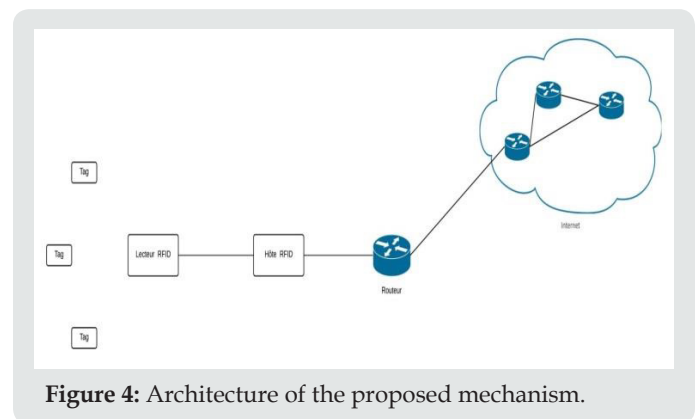
3. RFID host.

4. A router connected to the internet.



**Figure 4:** Architecture of the proposed mechanism.

An example of constructing the tag's IPv6 address is illustrated in Figure 5.

| ID tag | CRC-64 | Préfix Net | XNOR | New ID | IPv6 address |
|---|---|---|---|---|---|
| 02 0000A79 00013D 00015ECD | 196f2639a551 e1e8 | 2001::/64 | 690D9C65AAE3E16 | 0690:D9C6:5AAE:3E16 | 2001:: 0690:D9C6:5AAE:3E16 |

**Figure 5:** Example of IPv6 address construction of the tag.

### Pv6 address generation steps

**Adding the RFID tag:** In this step, we will add an RFID tag by clicking on "click here to add a new line. The addition of an RFID tag is shown in Figure 6.
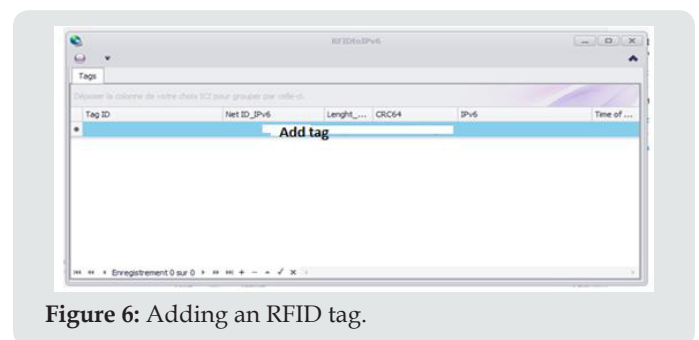


**Figure 6:** Adding an RFID tag.

**Reading the identifier of the RFID tag:** In this step, we read the tag identifier using an RFID reader. When this is done, the tag id field is filled with the identifier of the tag read by the reader. In this example, the application is connected to a network via a Wi-Fi connection. The access point is a smartphone providing an IPv6 connection. The Net ID_IPv6 field is reset by the value FE80: 0: 0: 0, it is the prefix of a local link address. The reading is illustrated in Figure 7.
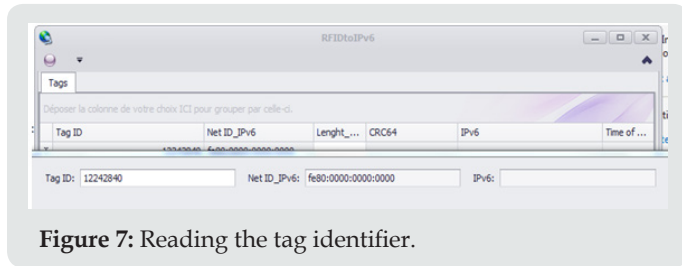


**Figure 7:** Reading the tag identifier.

**Generation of the IPv6 address:** In this step, when we click on the 'save' button, our algorithm generates an IPv6 address associated with the RFID tag. The generation of the IPv6 address is illustrated in Figure 8.
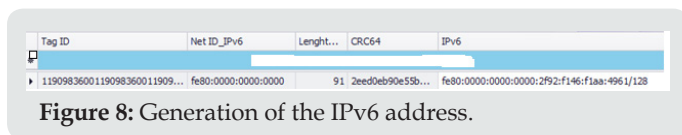


**Figure 8:** Generation of the IPv6 address.

In the "time of execution" field, the execution time of IPv6 address generation is calculated using our algorithm. Figure 9 illustrates the IPv6 address generation execution time.
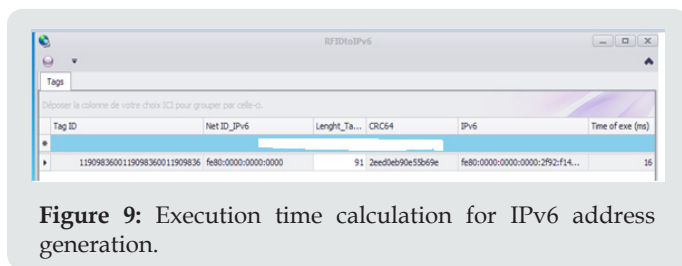


**Figure 9:** Execution time calculation for IPv6 address generation.

In Figure 10, the prefix is generated from a modem connected to the internet, it is a global prefix for an IPv6 connection (2002: c444: b1b5: 0000).
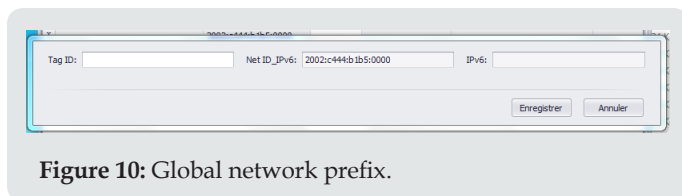


**Figure 10:** Global network prefix.

**Assignment of the generated address to an interface and connectivity test:** After having generated the IPv6 address (Figure 8) from the tag identifier, it is assigned to an interface in the network, then the ping of this address is tested, the result is illustrated in Figure 11. Independently of the machine, we calculated the time complexity of our algorithm and that of [19]. It expresses time requirements of an algorithm by giving, for each possible size of tag ID, the maximum time that might be needed to generate the IPv6 address. The Table 3 shows the comparison of the time complexity in both algorithms.
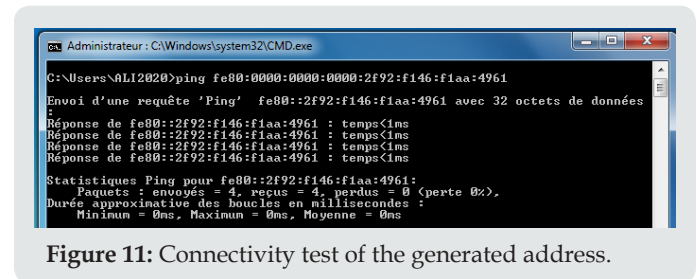


**Figure 11:** Connectivity test of the generated address.

**Table 3:** Time complexity comparison.

| Algorithm | Time complexity |
|---|---|
| Proposed algorithm | $O(\log^2(n))$ |
| CGA method [6] | $O(2^{16*Sec}) + O(\log 4(n))$ |

The CGA algorithm has a complexity of $O(2^{16*Sec}) + O(\log 4(n))$, while our algorithm has a complexity of $O(\log 2(n))$. Our algorithm considerably reduces the IPv6 address generation time since its global time complexity $<< O(2^{16*Sec}) + O(\log 4(n))$.

The Figure 11 shows the time complexity comparison between our mechanism and method based CGA.

According to the results of the implementation (Figure 12), we find that the IPv6 address generation time of our algorithm is less than that of generation by the CGA algorithm.
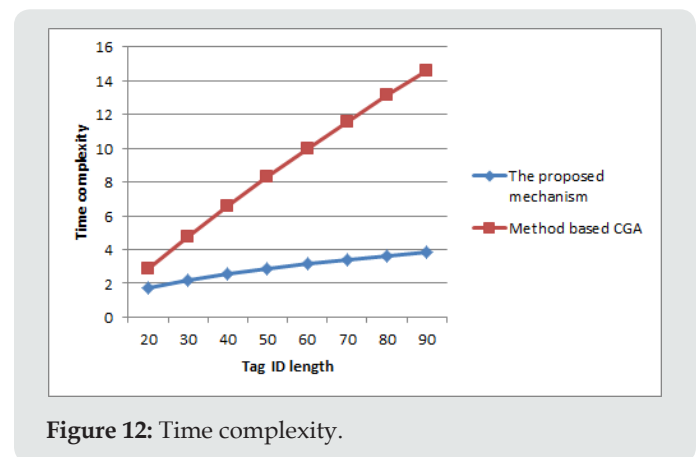


**Figure 12:** Time complexity.

## Conclusion and Perspectives

RFID plays an increasingly important role in our daily life for the management of goods, electronic tickets, health care, transport or even identity cards. In the literature, several studies have been devoted to the use of RFID technology to connect "objects" to the Internet using IPv6. In this paper, we proposed a mechanism to generate an IPv6 address from RFID tags based on their unique

identifiers using the operator XNOR whose two operands are the Net ID and the ID of the tag. The proposal overcomes several problems and limitations present in other mapping methods, including time complexity.

## References

1. Hahm O, Baccelli E, Petersen H, Tsiftes N (2015) Operating Systems for Low-End Devices in the Internet of Things: a Survey.

2. Finkenzeller Klaus (2010) RFID handbook: fundamentals and applications in contactless smart cards, radio frequency identification and near-field communication.

3. Ferro Erina, Francesco Potorti (2005) Bluetooth and Wi-Fi wireless protocols: a survey and a comparison. IEEE Wireless Communications 12(1): 12-26.

4. Vasseur J (2011) RPL: The IP routing protocol designed for low power and lossy networks. Internet Protocol for Smart Objects (IPSO) Alliance 36.

5. Winter Tim (2012) RPL: IPv6 routing protocol for low-power and lossy networks.

6. Kushalnagar Nandakishore, Gabriel Montenegro, Christian Schumacher (2007) IPv6 over lowpower wireless personal area networks (6LoWPANs): overview, assumptions, problem statement, and goals. RFC 4919.

7. Palattella Maria Rita (2013) Standardized protocol stack for the internet of (important) things. IEEE communications surveys & tutorials 15(3): 1389-1406.

8. JeongGil Ko, Andreas Terzis, Stephen Dawson-Haggerty, David E Culler, Jonathan W Hui, et al. (2011) Connecting low-power and lossy networks to the internet. IEEE Communications Magazine 49(4).

9. Hui Jonathan W, David E Culler (2008) Extending IP to low-power, wireless personal area networks. IEEE Internet Computing 12(4).

10. IEEE Standards Association (2011) IEEE Std 802.15.4-2011-IEEE standard for local and metropolitan area networks-part 15.4: Low-rate wireless personal area networks (LR-WPANs).

11. Frank, Raphael, Walter Bronzi, German Castignani, Thomas Engel (2014) Bluetooth low energy: An alternative technology for VANET applications. 2014 11th Annual Conference on Wireless On-demand Network Systems and Services (WONS).

12. Decuir Joseph (2014) Introducing Bluetooth Smart: Part 1: A look at both classic and new technologies. IEEE Consumer Electronics Magazine 3(1): 12-18.

13. Mackensen Elke, Matthias Lai, Thomas M Wendt (2012) Bluetooth Low Energy (BLE) based wireless sensors. Sensors 2012 IEEE.

14. Gyanendra Kumar, Parul Tomar (2018) A Survey of IPv6 Addressing Schemes for Internet of Things. International Journal of Hyperconnectivity and the Internet of Things 2(2): 1-15.

15. Mehdi Imani (2020) A survey on subjecting electronic product code and non-ID objects to IP identification. Engineering Reports.

16. Yoon Dong Geun, Dong-Hyeon Lee, Chang Ho Seo, Seong Gon Choi (2008) RFID networking mechanism using address management agent. Networked Computing and Advanced Information Management, 2008. NCM'08. Fourth International Conference on.Vol. 1.

17. Lee Sang-Do, Myung-Ki Shin, Hyoung-Jun Kim (2007) EPC vs. IPv6 mapping mechanism Advanced Communication Technology. The 9th International Conference on Vol 2 IEEE.

18. Garcia-Alfaro J, Herrera-Joancomartí J, Melià-Seguí J (2015) Security and Privacy Concerns About the RFID Layer of EPC Gen2 Networks. In: Navarro-Arribas G, Torra V (Eds.), Advanced Research in Data Privacy. Studies in Computational Intelligence pp.1-567.

19. Jensen Steffen Elmstrøm Holst, Rune Hylsberg Jacobsen (2013) Integrating RFID with IP host identities. Radio Frequency Identification from System to Applications.

20. Aljosha Judmayer, Johanna Ullrich, Georg Merzdovnik, Artemios G Voyiatzis, Edgar Weippl (2017) Lightweight Address Hopping for Defending the IPv6 IoT. In Proceedings of the 12th International Conference on Availability, Reliability and Security (ARES '17).

21. Ma Yi-Wei (2009) Mobile RFID with IPv6 for phone services Consumer Electronics, 2009.ISCE'09. IEEE 13th International Symposium on IEEE.

22. Dominikus Sandra, Jörn-Marc Schmidt (2011) Connecting passive RFID tags to the Internet of Things. Interconnecting Smart Objects with the Internet Workshop, Prague.

23. Mehdizadeh A, Khatun S, Ali BM, Raja Abdullah RSA, Kurup G (2008) Route Optimization Security in Mobile IPv6 Wireless Networks: A Test-Bed Experience. In: Sarbazi-Azad H, Parhami B, Miremadi SG, Hessabi S (Eds.), Advances in Computer Science and Engineering CSICC 2008 Communications in Computer and Information Science 6.

24. Madiha Khalid, Umar Mujahid, Najam-ul-Islam Muhammad (2019) Ultralightweight RFID Authentication Protocols for Low-Cost Passive RFID Tags. Security and Communication Networks 2019(11): 1-25

25. Rostański M, Mushynskyy T (2013) Security Issues of IPv6 Network Autoconfiguration. In: Saeed K, Chaki R, Cortesi A, Wierzchoń S (Eds.), Computer Information Systems and Industrial Management CISIM 2013 Lecture Notes in Computer Science 8104.

26. Aura T (2003) Cryptographically Generated Addresses (CGA). In: Boyd C, Mao W (Eds.) Information Security ISC 2003 Lecture Notes in Computer Science 2851.

27. El Ksimi A, Leghris C (2018) Towards a new algorithm to optimize IPv6 neighbor discovery security for small objects networks. Secur Commun Netw 2018: 1-11

28. Nabihah Ahmad, Rezaul Hasan (2011) A new design of XOR-XNOR gates for low power application. 2011 International Conference on Electronic Devices, Systems and Applications (ICEDSA).

29. Khalid EL KHADIRI, Ouidad LABOUIDYA, Najib ELKAMOUN, Rachid HILAL (2018) Performance Evaluation of IPv4/IPv6 Transition Mechanisms for Real-Time Applications using OPNET Modeler. International Journal of Advanced Computer Science and Applications(ijacsa) 9(4).

To Submit Your Article Click Here: **Submit Article**
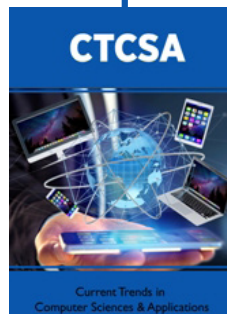
**Current Trends in Computer Sciences & Applications**

**Assets of Publishing with us**

- Global archiving of articles
- Immediate, unrestricted online access
- Rigorous Peer Review Process
- Authors Retain Copyrights
- Unique DOI for all articles