International Journal of Scientific Research in Engineering and Management (IJSREM)
Volume: 09 Issue: 06 | June - 2025 SJIF Rating: 8.586 ISSN: 2582-3930

Novel Mechanisms for Generating IPv6 Addresses in IoT Environments: Enhancing Security and Efficiency

T N KHALEEL NOUSHAD[1], S JAVEED AKHTAR[1], SAKA SUNEETHA[1], GAMASU SAI NIKHIL[1*]
[1]*Department of Computer Science,*
Indian Institute of Industry Interaction Education and Research, Chennai, Tamil Nadu 600066

Abstract - After these many years of IPv6 stateless auto-configuration service it is going to get the real push, as the number of Internet connected things hits the roof. Auto-configuration is basically a technique that is aimed to link the device to the internet as well as the local area network. Its key is the Neighbour Discovery Protocol (NDP), and it eliminates the necessity of administratively assigning certain addresses. Thus, the physical address of the computer being one of the factors used for definition of its IPv6 address. Still, many users have submitted complaints on the issue of privacy as being a challenge as per the result of this. Others are concerned in a way that doing the analysis on the packets may be able to recover the actual machine. This section provides a brief overview about the suggested, methods in the literature. In this work, a new probability IPv6 address generation approach using RFID ID tags is proposed. From the perspective of the time it takes to get the job done, our solution is much more efficient than others.

Key Words: IPv6, stateless Auto-Configuration, Internet of Things (IoT), Neighbour Discovery Protocol (NDP), Auto-Configuration, Local Area Network (LAN), IPv6 Address

1.INTRODUCTION

Internet of Things is on the brink of changing each and every facet of society, including human existence. There is a new dimension to our participation in the world since through gadgets on the Internet we read, investigate, commute, entertain, and even consume online. With the new advancements of technology, has come a new form of real world, one which lacks time-lag, and is burdened with vast amounts of information and the feeling of omnipresence. The optimal strategy is to implement a solution to address the unpreventable proliferation of internet-connected objects within our society in the not-too-distant future. In this regard, my article focused on RFID technology. A label, or rated "tag" and a reader communicate by means of information that is transmitted through electromagnetic waves; this is the core of the system. In the present day, RFID is implemented in a plethora of systems. Small items will be able to communicate with each other over the internet when the tag is converted into IPv6 address. The ability for the objects to connect and communicate either with objects in the same vicinity or through the internet is the core of "internet of things"(IoT). As such, it is quite obvious for Internet of Things devices to have at least one Network Interface. This work presents an approach for mapping RFID tag IDs to IPv6 addresses.

2. RELATED WORK

Many small objects that are utilized daily do not possess microprocessors and cannot enter into the computer network. Such kind of communication will be possible through employment of radio frequency identification, RFIDs and the incorporation of tags within objects. This is because the Internet of Things is a multidimensional concept that consist of different technologies which can be ancient or newly developed. Wireless sensor network (WSN), radio frequency identification (RFID) [1], WSN, Wi-Fi type wireless network [2], RPL: routing protocol for low-power and lossy networks [3], 6LowPAN [4], IEEE 802. 15. 4 [5], Bluetooth Low Energy, BLE [6] are part of the technologies and protocols the support the Internet of Things, IoT. Comparing the strategies of using IPv6 addressing and a general introduction to IPv6 challenges have been given by Gyanendra [7] in IoT environment. IoT device IP identification for Electronic Product Code and non-ID objects: After a study. The authors of [8] offer a solution that they base on the idea of forming a separate 48-bit Media Access Control (MAC) addressing structure with the reference RFID tag. Another method of assigning an IP address to an RFID tag is through the generated address from the DHCP server where the address may be dynamically assigned to the tag. That is right but it is not clear whether this method will work with all the EPC types. The biggest issue regarding this mechanism is that it is neither scalable nor very flexible. a new approach to the IPv6 addressing for objects that it is based on the EPC mapping [9]. To construct an IPv6 (128-bit) address, they used EUI-64 B first, then replaced the EUI 64-bit for 64-bit EPC in their hierarchical methodology. Based on this approach, DMAs are unable to transfer data on EPCs which extend beyond 64-bits in size.

This is a second addressing system that employs CGAs. This technique involves taking 64 bits Net ID and joining it with EPC code EM1400 for use as host ID. The following three issues may occur when performing EPC mapping: If the EPC has been mapped to fewer than 64 bits, then the algorithm includes a right padding of zeros. When set to 64 bits, it shall remain in its plain form as applied to all other scenarios. Finally, the system uses measures that allow the size of the messages to exceed 64 bits. To observe these, this approach to addressing is at the same time hierarchical and compliant with RFID tags. In addition to this it has no need for any more hardware and it is easy to integrate into any existing established system. This again puts the mechanism into the CGA category because the hash functions that are used to this end compress lengthy EPCs. Hash algorithms increase the time needed to generate the IPv6 addresses, map and allocate the addresses to the respective nodes since it involves additional computer computations. Along with reconnaissance attack prevention, it correlates the addresses and effectively addresses the DoS attacks it is very lightweight in terms of operations, and requires minimal management attention. It was in [10] where the idea of incorporating RFID with a mobile phone format was proposed. The purpose for this project is to come up with other methods of vocab reading from mobile devices other than from servers. This can include the process of the mobile phone requesting specific data from memory and the identification number from the tag in order to find the IPv6. For example in an all IPv6 scenario it may determine the global EPC. In the event that there is no IPv6, the mobile device makes a devoted IPv6 for the RFID tag by concatenation of 64 bits Net ID and 64 bits of host.

Regrettably, this constrains the flexibility of the mechanism as it demands the mobile telephone to incorporate the IPv6 structure.

A system that support IPv6 address and is designed to support a mobile communications. On the reader side this technique utilizes Mobile IPv6. The house agent HA is a manager needed by the MIPv6 [11] for ureAddresses. The HA stores the prefix of the reader's subnet which is emanated from the tag ID. Then, HA will forward the network prefix to the relevant node (CN). From the message, CN conveys the IP address to the reader. The reader then passes the data to a Tag as part of the process of establishing an IPv6 address. Finally, an acknowledgment message containing the IPv6 IP address obtained by CN will be transmitted back to CN. From the above-stated studies, it can be concluded that to perform the task of generating IPv6 address more numbers of network nodes are to be added in the network or additional functions are assigned to the RFID readers present at the network boundary. However, the time it takes to document or map and assign IPv6 addresses also rises as another disadvantage. This helped us achieve a saving of the algorithm's temporal complexity and gave us an easily implementable method to generate IPv6 addresses in our work.

3. RFID TECHNOLOGY

RFID technologies are becoming increasingly popular in recent years due to their application in effective tracking and security. RFID defined as a technique that can automatically write and read data to the tags via Radio Frequency fields. From the context, the various applications of radio frequency identification tags are well elucidated and can be attached to products, animals, or even people. An RFID tag is comprised of an antenna and integrated circuit coupled with the reader to analyze the data before sending it to the computer. The radio frequency identification tag comes in three varieties: There are three types of investment accounts active accounts, passive accounts and semi-passive accounts.

3. RFID TECHNOLOGY

Speaking of IPv6 networks' configuration, EUI-64 is one of the recommended techniques. Unicast IPv6 addresses may also be painted using the following method called the "Extended Unique Identifier" method. The greatest innovation of this address generation process is that Apple has chosen the MAC address of the device as the basis. Well, if you have five minutes of your time let me jog your memory, MAC address is always unique numbers. To be precise, this makes it possible for a device to be assigned an IPv6 address that it uses. This protocol is however different from IPv4 in that stations do not have to obtain their IP address, look for a DHCP server where they can acquire an IP address then proceed to engage the IP before they can communicate. In the following section, the configuration of the IPv6 address in EUI-64 format shall be explained. The flow chart of this approach is described next: The activity in this approach is illustrated below in the form of a flow chart as shown in the figure 1 below.

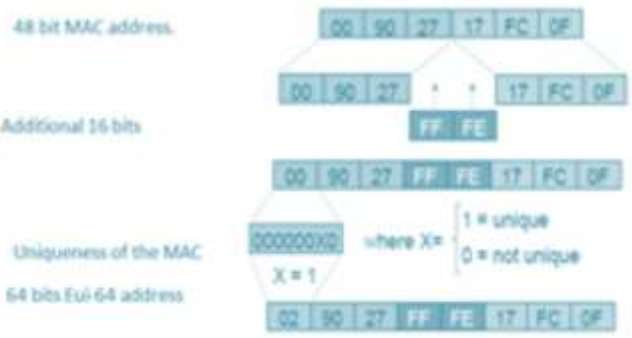

Fig 1: EUI-64 technique

1. The particular network card's prefix is "FE80:The first step is to obtain the following details: Device ID = 'IP CAM 0001:0010:0100' and MAC address = '0900: 2707: Fd0F'. To merge them, you must copy the prefix in front, take the first three bytes of the MAC address, and then append FFFE to the end of the string.
2. The next part of the third byte, the seventh, will also have "+1" added to it which will alter its decimal value.
3. Finally, after erasing the '0' which is unnecessary the corresponding IPv6 address is written down.

However, as this solution suggests, one of the weaknesses of this approach is that it depends on the identification of the interface based on the MAC address. This is rather concerning because the Host component will remain the same regardless of the network connections.

5. CGA IPv6 ADDRESS GENERATION

There appear to be a good number of algorithms for generating CGAs as can be evidenced from figure 2 below.
The node has to create a structure called CGA Parameters if it is to create a CGA. This data structure is used later on as a parameter by the hash function, it is shown in Figure 2.

1. The first is called the modifier, which is always a 128-bit random integer. This of course has its implications for both the overall safety of the address in play, as well as the potential danger.
2. A subnet prefix copies or replicates the first 64 bits of an address which is also referred to as the subnet prefix.
3. During the DAD, the number of collisions detected is represented by an 8-bit collision counter or a larger number or value.
4. By analogy, the public key of the node is placed in the public key field.
5. Additional usage codes can be coded into an address contained in the extension fields of CGA.

During the creation of the CGA address, two condensates/ hashes are generated on two parts of the CGA Parameters data structure; these are – hash1 as well as hash2. The following is a procedure for generating a new address in the CGA:

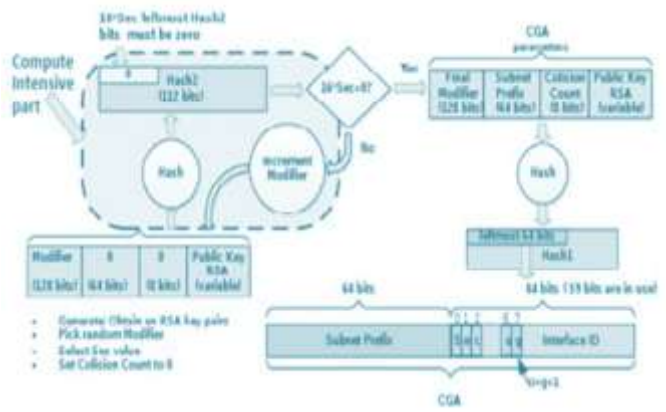

Fig 2.Algorithm for Generating CGAs

6. THE SUGGESTED PROCESS

The XNOR operator serves an important purpose in a function of the implemented mechanism. The operator XNOR, which will have the tag ID as the first operand and NetID of the network will be the second operand, to derive the IPv6 address. The logical operator XNOR is performed only on two operands and both operands can be either TRUE or FALSE and results in a TRUE only when operands are equal. The XNOR operator indicates the outcome R. That will be received for any conceivable combination of A and B as represented in the following truth table. To state it more clearly, the given logical operation, which is known as XNOR, has the meaning of "The result is TRUE if and only if the two entries are identical".To accomplish these transfers, objects must interact with their corresponding network nodes. However, due to the fact that RFID tags require an Internet address for example by IPv6, such items cannot connect to the network. Here, we explain a method by which we can allocate an IPv6 address to the RFID tag with its respective RFID tag ID. Therefore, we will have to implement this using the XNOR operator where we have Net ID as one of the inputs and the tag ID the other.

1. The remaining bits that identify a tag are less than 64 bits.
2. As mentioned before the tag identifier has a size of 64 bits.
3. Actually the tag identification is made of more than 64 bits.

1. This network ID is always kept, which will ensure that the resulting address is routed in the network.

2. Computer complexity is reduced.

3. Thus, it can be seen that the chance of collisions are low and two tags cannot possibly have two addresses when a tag is within the range of two readers.

The feature of being able to retrieve the tag identification from the IPv6 address using the operator XNOR in both directions is very important and is expressed by C = A XNOR B => B = C XNOR A.

5. Of course, other additional accessories are not necessary.

7. APPLICATION

A middleware program was developed to facilitate that solution. After reading the tag, the RFID reader will then send the unique identification number of the tag to the RFID host (HR). The second one which is related to the reader has the responsibility of mapping the tag's identification number to an IPv6 address. It also makes it possible to store the ID of the tag in to the database. The next procedure for one to get an IPv6 address is sending an RS message which stands for Router Solicitation. It will then receive from the router the Netid identification also known as the network prefix. In the manner illustrated in Figure 2 below, the HR is able to come up with an IPv6 address interface identification that is unique from the network identification got from the router. This combination is then used to derive the IPv6 address for the RFID tag. Figure 3 illustrates the sequence of address creation.

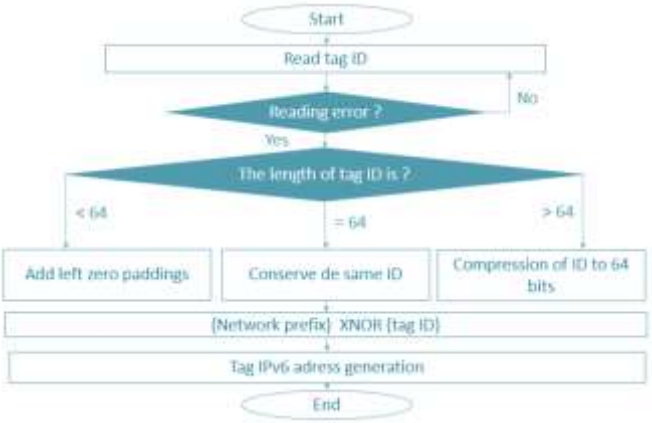

Fig 3.The suggested method.

8. THE SUGGESTED PROCESS

Finally, the construction of the planned mechanism is presented in figure 4.

Figure 4: The suggested mechanism's architectural layout.

The first one is an RFID tag. Thus, the second device is an RFID scanner. Thirdly, an RFID host and an internet-connected router.

ID tag	CRC 64	Prefix Net	XNOR	New ID	IPv6 address

Fig 5. Example of how to create the IPv6 address of the tag.

Figure 5 shows a sample tag with an IPv6 address.

8.1. Address generation steps

Step one: To add the RFID tag, it is as easy as clicking the 'click here to add a new line' button. Figure 6 shows the integration of the RFID tag.

Figure 6: RFID tag installation.

Deciding what the RFID tag's identification is: In this stage, we use an RFID reader to read the tag ID, which is unique to the tag. At this point the reader tag identification is entered in the tag id field. In this case, it demonstrates how the software is establishing a connection through a wireless connection to a network. An IPv6 connection is used as the access point and is obtained from a smartphone. The value FE80: 0: 0: 0, used as the prefix of a local link address, clears Net ID IPv6 field. The reading is summarized in figure 7.

Figure 7: That is how the identification within the tag can be deciphered.

The third process entails assigning an IPv6 address for each RFID tag; this process starts when the 'save' button is clicked. Figure 8 illustrates the procedure of generating an IPv6 address.

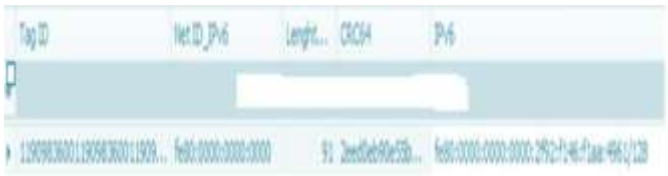

Fig 8. The IPv6 address is generated.

Our algorithm's execution time for IPv6 address creation is computed and stored in the "time of execution" field.Connectivity and interface assignment using the generated address: The IPv6 address is produced using the tag identification, allocated to a network interface, and then tested by pinging this address. We determined our algorithm's and [12]'s time complexity separately from the machine. It provides an estimate of the algorithm's runtime by listing the longest possible time to produce an IPv6 address for each conceivable tag ID size. We discover that our method generates IPv6 addresses faster than the CGA technique, as shown in the implementation results (Figure 9).

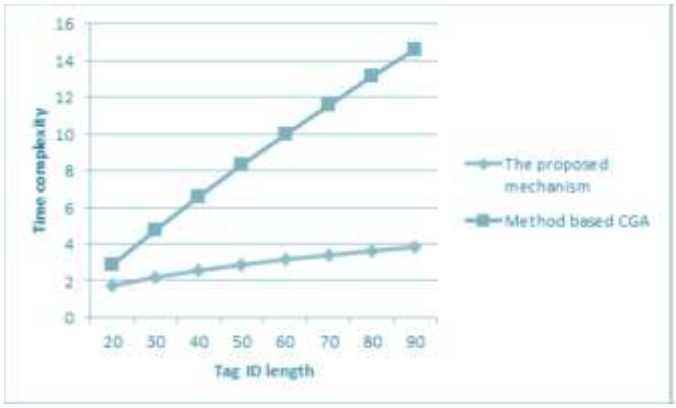

Fig 9: Unfortunately, time is something that has many layers of complexity involved in it.

9. CONCLUSIONS

The uses of RFID technology range from the management of commodities, electronic tickets, health care, transport and even identification cards; this shows the integration of RFID in our day to day activities. Many articles in academic journal have explained how RFID can be used to associate "things" with the web by using IPv6. This paper seeks to demonstrate how IPv6 addresses can be obtained from RFID tags by looking at the operators and applying the operator XNOR to arrive at a result of the Net ID and the tag ID. It avoids a number of concerns and problems connected with previous mapping methods, for example, that they are time-consuming.

REFERENCES

1. Hahm, Oliver, Emmanuel Baccelli, Hauke Petersen, and Nicolas Tsiftes. "Operating systems for low-end devices in the internet of things: a survey." IEEE Internet of Things Journal 3, no. 5 (2015): 720-734.
2. Erinaferro, F. "Bluetooth Andwi-Fi Wireless Protocols: A Survey And A comparison." IEEE Wireless Communications, IEEE (2005).
3. Vasseur, J., Navneet Agarwal, Jonathan Hui, Zach Shelby, Paul Bertrand, and Cedric Chauvenet. "RPL: The IP routing protocol

designed for low power and lossy networks." Internet Protocol for Smart Objects (IPSO) Alliance 36 (2011): 1-20.

4. Albarakati, Aiman J., Junaid Qayyum, and Khalid A. Fakeeh. "A survey on 6lowpan & its future research challenges." International Journal of Computer Science and Mobile Computing 3, no. 10 (2014): 558-570.
5. Palattella, Maria Rita, Nicola Accettura, Xavier Vilajosana, Thomas Watteyne, Luigi Alfredo Grieco, Gennaro Boggia, and Mischa Dohler. "Standardized protocol stack for the internet of (important) things." IEEE communications surveys & tutorials 15, no. 3 (2012): 1389-1406.
6. Frank, Raphael, Walter Bronzi, German Castignani, and Thomas Engel. "Bluetooth low energy: An alternative technology for VANET applications." In 2014 11th annual conference on wireless on-demand network systems and services (WONS), pp. 104-107. IEEE, 2014.
7. Kumar, Gyanendra, and Parul Tomar. "A survey of IPv6 addressing schemes for Internet of Things." International Journal of Hyperconnectivity and the Internet of Things (IJHIoT) 2, no. 2 (2018): 43-57.
8. Yoon, Dong Geun, Dong Hyeon Lee, Chang Ho Seo, and Seong Gon Choi. "RFID networking mechanism using address management agent." In 2008 Fourth International Conference on Networked Computing and Advanced Information Management, vol. 1, pp. 617-622. IEEE, 2008.
9. Garcia-Alfaro, Joaquin, Jordi Herrera-Joancomartí, and Joan Melià-Seguí. "Security and privacy concerns about the RFID layer of EPC Gen2 networks." Advanced research in data privacy (2015): 303-324.
10. Ma, Yi-Wei, Chin-Feng Lai, Yueh-Min Huang, and Jiann-Liang Chen. "Mobile RFID with IPv6 for phone services." In 2009 IEEE 13th International Symposium on Consumer Electronics, pp. 169-170. IEEE, 2009.
11. Mehdizadeh, Abbas, Sabira Khatun, Borhanuddin M. Ali, R. S. A. Raja Abdullah, and Gopakumar Kurup. "Route optimization security in mobile IPv6 wireless networks: A test-bed experience." In Advances in Computer Science and Engineering: 13th International CSI Computer Conference, CSICC 2008 Kish Island, Iran, March 9-11, 2008 Revised Selected Papers, pp. 153-159. Springer Berlin Heidelberg, 2009.
12. Jensen, Steffen Elmstrøm Holst, and Rune Hylsberg Jacobsen. "Integrating RFID with IP host identities." Radio Frequency Identification from System to Applications (2013): 111-130.