Volume 5, Issue 9, September 2015 ISSN: 2277 128X
International Journal of Advanced Research in Computer Science and Software Engineering
Research Paper
Available online at: www.ijarcsse.com

On Coding of the IPv6 and the Transmitted Data

Mustafa A. Salman
Departmentof Mathematics,
Ajman University of Science &Technology, UAE

Abstract— In this paper, the reliability of the internet of things, have been studied, in particular, the error detection and error correction codes of the addresses of the IPv6 and the data transmitted between the addresses in the internet of things. Different codes have been suggested according to the amount of possible risk of any alteration in addresses or data received by objects and the probability of occurring errors in the transmission process.

Keywords— object; identification protocol IPv6; linear codes; parity check digit code; message; codeword; source; destination; primitive polynomial; probability; bit.

I. INTRODUCTION

The Internet of Things (IoT) is the internet of future on which every thing is capable to communicate and interact with the others. This raises many challenges about the transmitted or stored data such as the reliability and the security of the data transmitted and received [1],[2]. Reliability and security are the concern of the stakeholder that the data transmitted from source (addresses and information) should be received at destination correctly, which means any data should be coded in a way that the incorrect received message must be detected and may be corrected depending on the coding system's capability. The security concern is that the data must be allowed to authorized people only. Security is beyond the scope of this paper. The coding system capability depends on the redundant digits (bits) added to the message (word) to have a codeword. In [3],[4] a different treatment for the identification protocol of version 6 (IPv6) of the IoT was suggested to reduce the length of the addresses to a maximum of 51-bit up to year 2100 in the warst possible case. Such a huge number of addresses 2^{51} together with the information transmitted between addresses will have a huge amount of communication, which must be transmitted and received correctly to provide trust and reliability of the IoT. Since the information transmitted between different addresses can be coded in the same way the addresses are coded, the ward "data" or "message" will be used , from now on, for both addresses and information to be transmitted.The transmitted data must be coded according to it's value which is determined by the amount of risk of any alteration in the data during transmition. The capability of coding system, should be also, related to the probability of occurrence of an error.

An (n,k) - Code is a code on which the message (word) length is k-bits and the check digits is (n-k)-bits which sum up to n-bit codeword or coded message. The check digits will provide the system, a capability to detect or correct certain number of errors depending on the number of bits (n-k) which will be added to the word before transmition. With the huge number of transmitted data (addresses and information) the coding system must be very efficient to have a high capability of detecting or correcting error with a minimum number of check digits.The capability of any code to detect or correct errors depends on Hamming distance between codewords, which is the number of places they differ [5].

Theorem [6]

- A code will detects all sets of t or fewer errors if and only if the minimum hamming distance between codewords is at least t+1.
- A code will correct all sets of t or fewer errors if and only if the minimum hamming distance between codewords is at least 2t+1.

Theorem: [6]

If f(x) is a primitive polynomial of degree m then the (n,n-m)-code generated by f(x) will detect all sets of single and double errors whenever $n \leq 2^m - 1$.

Corollary:

If f(x) is a primitive polynomial of degree m-1 then the (n , n-m)-code generated by g(x) = f(x) (x+1) will detect all sets of odd number of errors and double errors whenever $n \leq 2^m - 1$.

II. CODING OF THE TRANSMITTED DATA

Capability of a coding system depends on the generating polynomial, since the codeword must be divisible by the generating polynomial. Division of codeword by (x+1) will have the effect of detecting any odd number of errors. This code is the (n , n-1)-parity check digit code. The division by a primitive polynomial f(x) of degree m will have the effect of detecting all sets of double errors whenever the codeword is of length $n \leq 2^m - 1$.

Hence a generator polynomial g(x) = f(x) (x+1) will have the capability of detecting all sets of 1, 2, 3, 5, 7, . . . , $2^m - 1$ error and correct one error, since tha minimum Hamming distance between any two codewords is 3. In this paper, work of Salman [3] and [4] will be considered which showed in a thorough study for IPv6, that a vector space of dimension 51

over GF(2) (sequence of 51-bit) will cover all needs of addresses in the internet up to year 2100 in the worst possible case. The coding systems of the transmitted data can have the capability of detecting or correcting certain number of errors by adding check digits to the 51-bit addresses. It is also possible to use the same length of block for the information to be transmitted between different addresses. As a consequence, it may use the same primitive polynomial that generates a code for both addresses and informations or use different primitive polynomials.

In general, a primitive polynomial of degree m will generate a cyclic group of order $2^m - 1$and this cyclic group together with 0 will form the Galoa field $GF(2^m)$. Since the qoutient [$GF(2^m)$: GF(2)] is isomorphic to m-dimensional vector space over GF(2) say V(m,2) then this vector space can be generated by the standard basis:

e_1 = (1 0 0 0 . . . 0 0 0),
e_2 = (0 1 0 0 . . . 0 0 0),
e_3 = (0 0 1 0 . . . 0 0 0),
.
.
.
e_m = (0 0 0 0 . . . 0 0 1).

That is any vector in the vector space V(m,2) can be generated by a linear combination of the above basis. Using the above, the linear code can be implemented by considering only the m elements of the basis on which , the generating matrix and the parity check matrix can be constructed.

In general, encryption of data message has no effect on the length of the message which means the plaintext has the same length of the ciphertext. Encryption is an alteration of the data while any coding system requires adding check digit to the message to have a coded message. Coding has different level (different capabilities) depending on number of check digit attached to each message. Hence applications of internet of things must be classified to different level or different classes according to the level of risk of any alteration in the transmitted data and the probability of occurrence of errors in the transmitted data. If the level of risk is low in any alteration in the data and the probability of occurring an error is low too, a parity check digit (52,51)-code may be addapted which will detects all sets of odd number of errors. If the risk of any alteration in the transmitted data is high or the probability of occurring an error is high then a linear code generated by a polynomial g(x)=f(x)(x+1), is addapted where f(x) is a primitive polynomial of degree 6 and $n \leq 2^6 - 1 = 63$. Chose n to be 58 and k=51 and then the code will be (58,51)-code which will detect all sets of 1,2,3, 5, 7, . . . , 57 errors and correct one error. Detection of an error will leave two choices either correcting the error or re-transmitting the message and that depends on each individual case. The transmitted data of applications in the IoT will be classified to two classes according to the level of risk and the probability of occurring errors. It is possible, of course, to have more than two classes and then have more than two coding system. The coding systems which will be suggested to the classes are the linear coding systems that generated by a product of primitive polynomial with (x+1). List of primitive polynomials or irreducible polynomials over GF(2) may be found in many papers and one of the oldest one is the work of Marsh [7] which list all irreducible polynomials up to degree 19 while in [8] a program to check the irreducibility of polynomials over GF(p) was pesented which can be used to check irreducibility of polynomials of higher degree. In this work a primitive trinomial $x^6 + x + 1$ will be used together with (x+1) to generate the required (58,51)-linear code.

Let $f(x) = x^6 + x + 1$, then f(x) is a primitive polynomial over GF(2).

Hence $g(x) = (x^6 + x + 1)(x+1) = x^7 + x^6 + x^2 + 1$ generates a (58 , 51)- linear code capable of detecting all sets of 1, 2, 3, 5, 7, ... ,57 errors and correcting one error. This means a 7 digits will be added to each 51-bit message to have 58-bit codeword which is divisible by g(x). Clearly it is possible to get a better use for this code by chosing n , the length of the codeword, to be $2^6 - 1 = 63$ instead of 58 and then having (63 , 56)-linear code with the same capability but longer codeword. The restriction to 51+ 7 check digits comes from the maximum length of the addresses in the Ipv6 [4]. Chosing primitive polynomial of degree 7 instead of 6 will produce a (127, 119)- linear code with the same capability which can cover the length of the recent addresses [9] of the IPv6.

III. CLASSIFICATION OF THE APPLICATION OF THE IOT

Application of the IoT will cover all aspects of life and communications between objects, will be classified according to the amount of risk of any alteration in the transmitted and received data together with the probability of occurrence an error. Although the probability of occurring an error can be determined or expected in advance but the level of risk will certainly depends on the evaluation of stakeholder case by case. Applications on which the data transmitted between objects will be classified to the following two classes:

1- Low Risk **AND** Low Probability of occurrence of an Error:

Low risk class will corresponde to all communication related to objects on which any alteration in the transmitted data will cause a minor damage. The probability of occurring errors will be regarded low for all indoor communication, most of district communications, all communications that are performed inside market, cars, factories, and many more. Any communication having the two properties, low risk and low probability of having an error, will be coded with the parity check digit (52,51)- code.

3- High Risk **OR** High Probabilty of occurrence of an Error:

Class of high risk will corresponds to all essential communications related to life, economy, military, and disasters.The probability of occurring errors will be regarded high for all national and international communications, and most of outdoor comunication. The opinion of the stakeholder will have essential role in deciding the level of risk for any related application. Any communication of an application having one or both properties, will be coded by using a (58 , 51)-linear code which has more capability than the parity check digit code.

In the above, the communication of any application will have a convenient coding system, according to the two properties, the risk and the probabilty of having an error. If both properties, low risk and low probability, are present in any application then the parity check digit is convenient else a linear code with a higher capabilty of detecting and correcting errors will be more convenient. This is summorized by the following table on which more detailes concerning the applications [1],[2], are given:

Table I Classification of the application of the IOT

Type of Risk	Low Risk **AND** Low Probability of Occurrence of an Error	High Risk **OR** High Probabilty of Occurrence of an Error
Code	(52,51)- Parity check digit code	(58,51) - Linear code generated by $g(x) = f(x)(x+1)$where $f(x) = x^6 + x + 1 = x^7 + x^6 + x^2 + 1$
Some Applications	- Indoor sensors (Frigerator, Waste, Temperature, Lighting, Shower Tempreture, Humidity,…) - Car Sensors (Door, Tire Pressure, Petrol, ...) - Some of Outdoor Sensors (Weather , Traffic, Air Polution, Humidity, Health, Travel, Production, Transportation, . . .) - Market and Factories (Prices, Check in and Out Material , Noise, Gasses, Parking, Production, …), …	Some of Outdoor Sensors (Vibration of Bridges and Building, Fire Detection, Mixing Drug ,…) - Economy (Mobile Phone as a Credit Card, Flow Assets, …) - Education, Researches … Military (Guided Missile, Air Attack, ...) Disaster (Level of Water in a Damp, Water Polution, …)

IV. CONCLUSIONS

This is a complementary work to the new look of the IPv6 as a 51-dimensional vector space over GF(2) on which the reliability of the IoT is treated by setting a convenient coding system for the different classes of applications of the IoT. The coding system attached to each class depends on two factors, the level of risk of any alteration in the transmitted data and the probability of occurrence of an error. The parity check didgit-code were suggested for the low risk and low probability of occurrence of an error while the linear (58, 51)-code for the high risk of any alteration in the transmitted data or the high probability of occurrence of an error.

REFERENCES

[1] D.Evance, "*The Internet of Things, How the next Evolution of the Internet is changing everything*", CISCO white paper(2011).
[2] P. Hartwell, "*Methodology, The Internet of Things, How the next Evolution of the Internet is changing everything*", CISCO white paper(2011).
[3] M.A. Salman, *On Identification of Internet of Things*, (2014), International Journal of Sciences: Basic and Applied Research (IJSBAR) (2014) Volume 18, No 1, pp 59-62
[4] M.A. Salman, *On Identification protocols of version 4 and 6*, International Journal of Engineering Science Invension ISSN: 2319- 6734 volume 3 octobe 2014 p18-21
[5] P. Sweeny, *Error Control Coding fromTheory to Practice*.John Wiley and Sons, 2002.
[6] W.J.Gilbert, W.K. Nicholson, *Modern Algebra with Application*, wiley 2003.
[7] R.W. Marsh, *Table of Irreducible polynomial over GF(2) through degree 19*, NSA,Washington,D.C 1957
[8] M.A.Salman, A.Fouad, N.Ghanim, *Program to test Irreducibility of Polynomials over GF(p)*, National Conference of Computer Applications, Baghdad 1991.
[9] S. Deering, R. Hinden," *Internet Protocol, Version 6 (IPv6) Specification*", RFC 2460(1998).

