This full-text paper was peer-reviewed and accepted to be presented at the IEEE WiSPNET 2016 conference.

Header Compression and Neighbor Discovery in 6LoWPAN based IoT – A Survey

Hemal Shah
Ganpat University
Mehsana, Gujarat , India
hemal.shah@ganpatuniversity.ac.in

Mr. Rahul Shrimali
Saffrony Institute of Technology
Mehsana, Gujarat, India
rahul.shrimali@saffrony.ac.in

Vrajesh Parikh
GTU PG School
BISAG Gandhinagar,
Gujarat, India
vrajesh.2188@gmail.com

Abstract: **The Internet of Things (IoT) is the next generation technology which is expected to bring a major revolution in the art of creating smarter environments. In order to uniquely identify each device in smart environment, a new protocol using IPv6 over Low-power Wireless Personal Area Network (6LoWPAN) has been developed which supports management of sleep cycles of device for power management. However issues in a LoWPAN networks include bountiful utilization of bandwidth due to over dissemination of packets during Neighbor Discovery (ND) and headers with larger size lead to prodigal power consumption leading to short network life. This paper is a survey on state-of-art of ND techniques like ND++, Context Aware Resource Discovery (CARD) & HC techniques like Generic Header Compression, compressed DTLS in 6LoWPAN. The outcomes of the survey show that there is a prospect of optimization in ND and HC, with a clear aim to enhance the efficiency of 6LoWPAN for the low power and low processing capabilities of IoT devices.**

Keywords: **Internet of Things (IoT), 6LoWPAN, Header Compression (HC), Neighbor Discovery, Context Aware Resource Discovery, Generic Header Compression (GHC), Datagram Transport Layer Security (DTLS)**

I. INTRODUCTION

With the fast growing technology the communication is no more confined between devices and humans. In other words we have reached to an era where the IoT devices are designed and expected to communicate to each other using Machine-to Machine paradigm. The embedded devices used in IoT are usually expected to work in low power wireless frequencies. These devices are IP enabled, can work using IPv6 over Low Power Wireless Personal Area Network (LoWPAN i.e. IEEE 802.4.15) and they make up network of Internet of Things. If the devices are self-powered, optimal use of bandwidth plays key role in deciding the throughput of network, its efficiency and life time. In this survey paper, we mainly focused on Neighbor Discovery, sometimes also referred as Resource Discovery (RD) or Service Discovery (SD). The major issues in ND are extra packet transmissions over the medium due to multicasting nature of neighbor discovery & router discovery, duplicate address detection and many more. Similarly the Header Compression needs optimization so as to make the payload lightweight to suit the application resulting into minimum power consumption and advantage like expending the remaining bandwidth for data transmission. The discussion in this paper is based on RFC 4944, an IETF document that specifies transmission of IPv6 packets over IEEE 802.15.4 network. Apart of this the discussion is based on other different RFCs that deal with HC, ND and Generic Header Compression (GHC). The rest of the paper is organized as following. Section II contains the inception of 6LoWPAN from IPv6 with basics of ND, HC and GHC in 6LoWPAN and existing challenges. Section III contains related work which includes the discussion of alternate details and techniques available for ND and HC and finally we conclude with survey outcomes in Section IV by identifying the future research gap, scope and directions.

II. INCEPTION OF 6LOWPAN FROM IPV6

The core internet is made up of router and servers include around million nodes which has extreme high capacity. The core network is managed by IPv4, as far as unique identification of each node on the network is concerned [1], and then we have the IoT network which is expected to have trillions of devices connected to the internet as shown in fig. 1[1]. It is expected that by 2020 there would be around 26 billion to 50 billion [2] such devices, which motivate us to have an addressing scheme that can handle more than 2^{32} unique addresses, which is nothing but the maximum capacity of IPv4 addressing scheme.

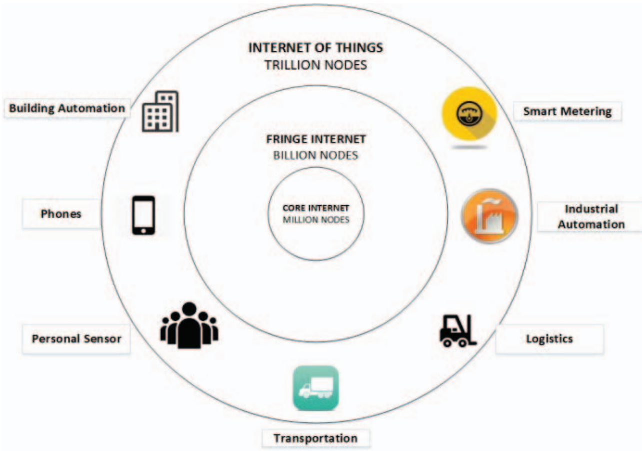

Fig. 1. Internet [1]

Again there are some more limitations of IPv4 that makes it undesirable to be used in an environment where one wants an auto-configurable inter mobile-device communication. IPv4 implementation needs either manual configuration or a stateful address configuration protocol like Dynamic Host Configuration Protocol (DHCP), so there is a need to have simpler and automatic configurable settings that do not depend on the DHCP support. IPv4 packets also need cryptographic service to protect data from being viewed or modified during transit. Additionally if the IPv4 packet is encrypted with some proprietary solutions, then it cannot use the TCP and UDP ports for identification. These all characteristics of IPv4 make it unsuitable for IoT, which has most of its devices mobile and working on wireless medium. Thus the limitations of IPv4 have brought the current internet at the verge to accept the IPv6 which is capable of enormously large addressing capacity of 2^{128} devices, which are approximately 3.4×10^{38} addresses. Again IPv6 includes auto-address configuration. It also allows multicast rather than broadcast which saves network bandwidth [3] from unnecessary packet transmission.

RFC 2460 defines the standards related to IPv6 and RFC 4861, elaborates the ND in IPv6. According to RFC 4861, the ND for IPv6 section 3(Protocol Overview) is capable of solving issues of Router Discovery, Prefix Discovery, Parameter Discovery, address resolution, next hop determination, neighbor unreachability detection, Duplicate Address Detection (DAD) etc. This RFC also defines five types of ICMP packet types, Router Solicitation (RS), Router Advertisement (RA), Neighbor Solicitation (NS), Neighbor Advertisement (NA) and a redirect message. Fig. 2 shows how the neighbor discovery, DAD and address resolution is done in the IPv6. When the interface gets enabled, the host sends a RS packet in order to get a RA packet out of the scheduled time and which contains the address prefixes. This is used to determine whether other address is sharing same link and/or address configuration and determining the hop value [4]. RA messages sent by routers are generally multicast packets. Similarly the multicast NS message is sent by the node to determine whether the neighbor is still in reach via a cached link-layer address, to get the link layer address of neighbor [4]. It is also used for DAD. A multicast NA message is sent against the NS message or a node may send unsolicited multicast NA to determine change in the address [4].

Therefore, this multicasting of packets in the ND process makes it prodigal to be implemented in low bandwidth wireless network on the low battery powered embedded devices with low buffering capacity for IoT. Along with this IPv6 have optional support for authentication and encryption using IP security, and other web service make use of transport layer or secure socket layer security which may be too complex for simple IoT devices [1] to handle. Along with this features current IP requires links and enough frame length which is minimum 1280 bytes for IPv6, such substantial bandwidth is needed for heavy application protocols [1]. Thus these features of IPv6 are not needed to be implemented in IoT as they are meant for traditional IP network, which are supposed to be all time powered and have no processing or storage constraints.

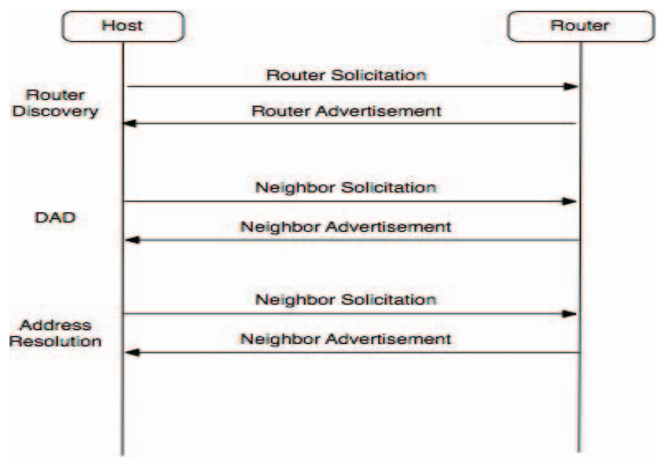

Fig. 2. Neighbor discovery in IPv6 [1]

The fig. 3 shows time line presenting the development of work done by IETF on 6LoWPAN ND and HC till date.

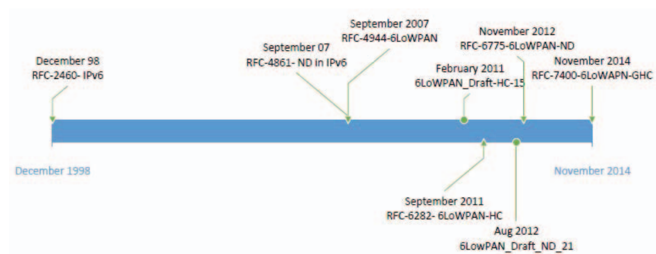

Fig 3 6LowPAN time line

A. Why 6LowPAN?

The basic assumption of IP is that devices are always connected. 6LoWPAN is basically IPv6 plus low power RF [1], which has several benefits, like it is lightweight, energy efficient, scalable, has reliable standards and provides end-to-end data flow. It would allow extending the already existing IP network. Again the network that needs a full fledge TCP/IP stack along with operating system and a powerful processor are the major bottleneck for IoT devices. This is because embedded devices used in IoT have several challenges to overcome that include power management and duty cycles. Multicast feature of IP causes unnecessary power drain in multi hop networks; limited bandwidth restricts the frame sizes [1]. Thus in order to make sure that the above problems are sorted to a certain extent 6LoWPAN must be used.

B. 6LoWPAN Protocol Stack

The stack shown in Fig.4 is the 6LowPAN protocol stack along with the TCP/IP protocol stack to illustrate the comparison of where exactly the 6LoWPAN resides. It can be seen clearly that instead of IP as in TCP/IP the LoWPAN resides at network layer with IPv6. This can be shown as a LoWPAN below IPv6 but practically they are implemented as a single section.

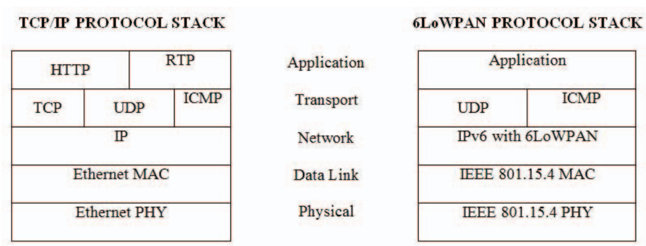

Fig. 4. 6LoWPAN Protocol Stack [1]

Again one would mark that the 6LoWPAN stack is not having TCP at the transport layer, this is because TCP is not useful in LoWPAN. It doesn't deal with packet loss in wireless mediums. And so is the case with HTTP as it is not that useful with the LoWPAN. Rather than using HTTP, one can use AMQP, MQTT, XMPP that are special application level protocols specially developed to suit needs of IoT.

C. ND, HC AND GHC IN 6LoWPAN ACCORDING TO RFC

The main use of ND in IPv6 is to discover and monitor the presence of other nodes on the link [4]. It is also used to know the link layer address, find routers and maintain data related to the nodes in the near vicinity so that they might be used as a relay node to pass on the data to node that is out of reach using store-carry-forward mechanism. There are number of shortcomings of ND in IPv6; some of which include heavy packet exchange between node and router for DAD, and the NS for address resolution in multicast [4]. Again sending periodic RA packets over the medium to reveal the existence of router, which is for sure an unwanted communication considering the LoWPAN networks of IoT. And finally because the wireless network is lousy in nature the links are often unstable and so the nodes appear to be moving, despite not so, which cannot be handled by the IPv6 [5].

The ND in 6LoWPAN defined in RFC 6755 specially addresses the optimization that is needed due to the application of IPv6 in IEEE 802.15.4 and other similar link technologies. This is because low power applications are not expected to use multicast signaling due to power conservation needs [5].

Apart of this the wireless links are not expected to follow the traditional IP subnet and IP link concepts. ND for IPv6 was designed keeping transitive networks in mind as it rely on the traditional link concept of IPv6 and heavily uses multicasting which is not desirable feature to use in the low-power, lousy networks. So RFC 6775 was developed with some goals and assumptions. The goals mainly included minimization of signaling by avoiding multicast flooding of packets, provide support for sleeping nodes, multi-hop DAD and dissemination of context information to hosts so as to perform header compression. The assumptions include that, the link is wireless, low power and lousy, 6LoWPAN is configured in a way that the routers are made to share more than one IPv6 address prefixes, allowing mobility of nodes without changing their address between the routers [5].

RFC 6775 discusses the various options used by the specification and also describes the address registration option used by the hosts; the 6LoWPAN Context Option and the Border Router Option used for the router-to-router communication in detail. Thus with several optimizations made in the RFC 6775 it has been proved in [7] that the message exchange on the network is reduced by 60-80% and its discussion is done in the section III.

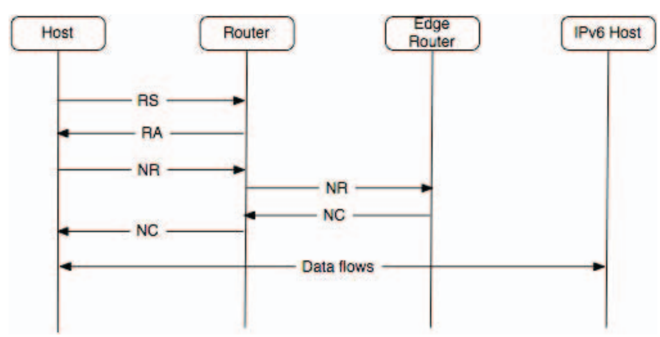

Fig.5. 6LoWPAN-ND [5]

Here figure 5 shows a scenario where all the devices are connected through a wireless link and are a multi-hop network. So we have a multiple IP hope inside this mesh network. And so now we have RS, RA and instead of NS, NA to do the node registration. The host registers to the router and get a confirmation, the router is already registered to the edge router. So in order to allow the network wide activity, registration to the edge router is must. Again the registration here is basically a soft binding and is expected to live longer not longer than a day or up to a week. Or the nodes may sleep for a week. And once the things are done normal data flow are allowed.

The main challenges in ND are to propose a mechanism that needs least amount of packet transfer for a node to keep in touch with the neighbor nodes and router. For example multicasting of NS is no more used for address resolution in 6LoWPAN instead a router maintains a cache which stores information related to neighbors, so if the address is not present in the cache the address either doesn't exist or is assigned to a node attached to another router on the LoWPAN. Similarly 6LoWPAN uses Duplicate Address Request (DAR) and the Duplicate Address Confirmation (DAC) between 6LoWPAN Routers (6LR) and the 6LoWPAN Border Router (6LRB) for DAD, avoiding the use of NS and NA for this purpose. So another challenge can include proposing a mechanism for DAD over multiple hops.

Header Compression is another important parameter to reduce overheads in 6LoWPAN. If the 6LoWPAN header is containing extra information that is of no use would surely result in wastage of bandwidth. Apart of this it would also tend to make the data packet heavier in size. The RFC 6282 HC [8] defines the alternative of the RFC 4944 section 10. It defines the new compression of multicast addresses and a framework for compressing the next headers. It allows compression of arbitrary prefixes by relying on shared context. Thus the challenge is that the compression and the decompression of headers must be done based on the context that is shared prior to communication; else the receiving node won't understand the packet.

Section 3 of RFC 6282 defines the 6LoWPAN_IPHC header, which defines the way IPv6 header, is compressed. The 6LoWPAN_IPHC uses 13 bits, and for effective compression it relies on the entire 6LoWPAN information section 3.1.1 [8]. The 6LoWPAN header is attached after 6LoWPAN_IPHC, which may be compressed if the field is partially elided. Apart of this 6LoWPAN also defines the Context Identifier Extension, which is vague definition of the conceptual context that must be shared between the node that is compressing the packet and the node that is decompressing it. However the context sharing and management are marked as out of scope. Again the actions for the invalid or unknown context are also defined as out of scope. The RFC 7400 has tried to address a typical issue, which is called 6LoWPAN Generic Header Compression (GHC). There is always a need of new specifications for every kind of header that needs compression, and it does not actually give an extension of the current scheme like Robust Header Compression (ROHC). The technique is slightly less efficient but has a capacity of compressing headers of all types and even for header like payloads [9]. So it's a kind of general data compression scheme. But still the problem remains unsolved because even if the slightest change is made to the header that is old or a new header has been accepted, needs to reopen the 6LoWPAN HC and make proper amendments.

J. Hui, et al.; [8] have also presented that the context used to encode the source address is not expected to encode the destination address using the same context. Thus considering the fact that the context can be according to the need of the application the sections ahead contain some proposals and the effects related to it.

III. RELATED WORK/ ALTERNATES PROPOSED

By far from the discussion of the 6LoWPAN it is quite clear that there is indeed a lot of scope in ND optimization and the HC for researchers to work on. The next two sub-sections discuss the related work done till now in the same directions. It also includes future directions in their relative area along with challenges.

A. Neighbor Discovery

The ND is bulky set of processing that consumes more power considering IPv6 as discussed earlier; however the ND in 6LoWPAN is a light weight as compare to IPv6. This has been proved [7] by performing experiments in the Contiki operating system with same topology, with an aim to measure the difference between the ND of 6LoWPAN and IPv6. And the hour long simulations prove that the optimized RFC 6775 ND protocol reduces the over-all message exchange ration by 60-80%. There is as such no work done to compare the HC of RFC 6775 with the GHC defined in RFC 7400, so it can be considered as an future direction to work on and may then be define a better header compression mechanism that mitigates the issues.

Monika Grajzer, et al.; [10] has proposed a ND++ protocol for provisioning self-configuring service. They have proposed a mechanism offering a possibility of automated, unsupervised network configuration and operation. The mechanism of stateless address auto-configuration provides a way by which an IPv6 network can self- configure which is not yet fully supported by MANETs. Althought the current IPv6 has some level of Stateless Address Auto-configuration (SAA) but it lacks efficiency and adequate scope if the network is quite large in size. To address this issue the authors have proposed an enhancement of IPv6 ND protocol, which they call it as ND++ and are specially meant for DAD in MANETs with an aim to deal mobility of nodes and changing topology. The experiments are done in NS3 by comparing the Multi-hop protocol routing against ND++. The implementation has been done in 2 phase where the first phase involves the standard DAD procedure for 1-hop neighbor, where as in the second phase additional DAD is performed by means of multi hop NS so as to cover extended range of n hops. The results reveal the fact that the DAD is successfully done with reasonable reduction in the overheads in network.

Another technique has addressed the issue of recurrent opportunistic contact between the static and mobile devices thus making a point that the standard periodic probe making routing algorithms cannot be used in such situations, rather a protocol that becomes more resilient to such opportunistic contact should be made. By leveraging the characteristics expressed by these patterns, knowledge based discovery solutions can be designed in order to restrict the use of energy resource associated with the aggressive probing-based discovery phase. To address this they have introduce a Context Aware Resource Discovery framework that leveraging Q-Learning, a machine learning technique which extends the functionalities of asynchronous neighbor discovery protocols, while being capable to reduce energy wastage and discovery latency. The proposal addresses only mobile to device interaction [11].

The Q-learning is a temporal difference method which is one of the main types of reinforcement learning method other than dynamic programming and Monte Carlo method. Q-learning is an algorithm by Watkins 1989 and the implementation is basically a mathematical model. The approach can achieve and maintain a good balance of energy consumption versus discovery latency and residual useful contact time for a variety of simulation setups, emulating the behavior of devices in realistic scenarios typically found in Smart Buildings and Smart Cities deployments, outperforming both 'non-learning' based approaches but also other learning-based approaches, and without requiring any manual tuning of the parameters involved in its decision making engine.

The other challenges for further development can include, discovering a mobile node that can be a smart phone to register to the network and then communicating with the nodes to right away get the data that they have been sensed. So the important here is the introduction of a foreign node to network for seamless communication.

B. Header compression and Context based system for 6LoWPAN

Shahid Raza, et al.; [12] has proposed a header compression for datagram transport layer security (DTLS). The proposal includes linking of the compressed DTLS with 6LoWPAN using standard mechanisms.

The DTLS is a protocol mainly used for security of traffic for client server based applications and it is composed of record protocols that carry other protocols such as Handshaking, Alert and application data. The compression mechanism includes development of 6LoWPAN_GHC for client server application.

Finally a technique has been proposed to complete the context that is designed to compress address because till then there wasn't any detailed design. Now the problems of the context is that in the traditional network the Maximum Transmission Unit (MTU) can be over thousand bytes but it's less in the 6LoWPAN. The IEEE 802.15.4 standard specifies MTU only 127 bytes [8], even more these bytes must yield parts of them for Media Access Control (MAC) payload and security mechanism, left quite a little peace for data transmission. Context are important concept in 6LowPAN network because they are used to record prefix of addresses, address compression and it is defined by the new ICMP6 options in 6LoWPAN to transmit the context information. Apart of this they also have addressed an error detection mechanism. So the author has proposed a complete context system for the router and the node, and has proved with the implementation that the proposal works fine [12].

IV. CONCLUSION AND FUTURE WORK

In this paper we have reviewed existing techniques for HC and ND that are proposed to optimize the working of 6LoWPAN. For Neighbor Discovery in 6LoWAPN, we have reviewed two techniques. Context Aware Resource Discovery (CARD) - a machine learning technique and ND++ - a technique proposed to enhance the IPv6 ND for DAD.

The CARD system is based on Q- learning that is trying to make a ND protocol resilient to the changing patterns of opportunistic contacts between static infrastructure and mobile devices, whereas the ND++ is based on connected topologies for DAD in a MANET scenario. So both of them are two separate techniques, and can be used to mitigate two distinct issues of opportunistic contact learning and DAD respectively. As a part of future work we propose multiple device discoveries within a predefined time frame in a scenario having large number of devices using the CARD technique, and testing the ND ++ protocol for realistic topologies modeling real world conditions like urban scenarios.

In HC, DTLS compression has been proposed but the technique has not been tested yet to see its efficiency and security it provides, which can be considered as area of work. Again there is also a paper that discussed and proposed a context for 6LoWAPN header along with error detection mechanism. Similarly there can be a context proposed so there is no need to have separate header compression for new headers and header like payloads. Apart from this, there can be comparative study done between the IPv6 header format, 6LoWPAN HC and GHC to analyze the effects in the test beds or simulation environment. And finally the packet size for 6LoWPAN being quiet limited, it is desirable to have layer 2 and layer 3 compressions for better security and bandwidth utilization, which is yet to be explored.

REFERENCES

[1] Zach Shelby and Carsten Bormann "6LoWPAN the Wireless Embedded Internet", 1st ed, *John Wiley & Sons* Ltd, UK, 2009.

[2] Raymond James & Associates "The Internet of Things – A Study in Hype, Reality, Disruption and Growth." St Petersburg, Florida, 800-248-8863 Jan 24, 2014

[3] IETF Standard, Internet Protocol Version 6 (IPv6) Specifications RFC 2460, December 1998.s

[4] IETF Neighbor Discovery for IP version 6 (IPv6)" RFC 4861, September 2007 obsoletes 2461.

[5] IETF Neighbor Discovery Optimization for IPv6 over Low-Power Wireless Personal Area Networks (6LoWPANs)" RFC6775, Nov. 2012.

[6] IETF Transmission of IPv6 packet over IEEE 802.15.4 networks" RFC 4944, September 2007

[7] Mohamed A. M. Seliem, et al. "Performance Evaluation and Optimization of Neighbor Discovery Over Contiki OS*" *IEEE World Forum on Internet of Things* (WF-IoT), Seoul, South Korea, March 2104, 119-123

[8] IETF Compressoin Format for IPv6 Datagram over IEEE 802.15.4 Based Network" RFC6282, September 2011.

[9] C. Bormann, "Generic Header Compression for 6LoWPAN" RFC7400 Internet Engineering Task Force, November 2014.

[10] Monika Grajzer, Mariusz Głąbowski "Performance evaluation of Neighbor Discovery++ protocol for the provisioning of self-configuration services in IPv6 mobile ad hoc networks", *16 th IEEE International Telecommunication Network Strategy and Planning Sumposium, Funchal,* 2014, 10.1109/NETWKS/.2014.6959266.

[11] Riccardo Pozza, et al, "CARD: Context-Aware Resource Discovery for mobile Internet of Things scenarios". *IEEE 15th International Symposium. A World of Wireless, Mobile and Multimedia Networks (WoWMoM)*, Sydney NSW, June 2014, /10.1109/WoWMoM.2014.6918976.

[12] Shahid Raza, et al. "6LoWPAN Compressed DTLS for CoAP" *8th IEEE International Conference on Distributed Computing in Sensor Systems*, Hangzhou, May 2012, 978-1-4673-1693-4.

[13] Nan Li, Xiaohong Huang "A CONTEXT SYSTEM FOR 6LOWPAN NETWORK "*Proc.of IEEE IC-BNMT2011*, shenzhen, Oct 2011 978-1-61284-158-8