Spring 2019

Literature Survey on IPv6 over low power personal area networks.

Roshan Mathew

Literature Survey on IPv6 over Low-Power Wireless Personal Area Networks.

by

Roshan Mathew

A creative component submitted to the graduate faculty

in partial fulfillment of the requirements for the degree of

MASTERS.

Major: Computer Engineering

Program of Study Committee:
Doug Jacobson, Major Professor

The student author, whose presentation of the scholarship herein was approved by the program of study committee, is solely responsible for the content of this creative component. The Graduate College will ensure this creative component is globally accessible and will not permit alterations after a degree is conferred.

Iowa State University

Ames, Iowa

2019

TABLE OF CONTENTS

LIST OF FIGURES

Page

LIST OF TABLES

Page

ACKNOWLEDGMENTS

I would like to appreciate the opportunity Iowa State University has provided me to complete my creative component.

I would like to thank my program of study committee member and major professor Doug Jacobson for his guidance and support throughout the course of this research.

In addition, I would also like to thank my friends, colleagues, the department faculty and staff for making my time at Iowa State University an amazing experience.

I would like to thank the pillars of my life, my parents whose moral, emotional and mental support is responsible for everything I’m today.

ABSTRACT

As there is an increase in (IOT) Internet of Things, there is a growing implementation of Internet of things in many areas in our day-to-day life. Internet of things entails the linking of different embedded devices like appliances, weather stations and even toys to the internet using the Internet Protocol. Surveys say that the number of embedded devices that are IP-enabled will outnumber the total personal computers in the near future. 6LoWPAN is the name of a concluded working group in the Internet area of the IETF. 6LoWPAN is the technology that enable small, low powered embedded devices to access the internet. 6LoWPAN is a protocol definition that makes IPv6 packets to be carried on top of low power wireless networks, specifically IEEE 802.15.4.

In this literature survey, I am going to give the details about the architecture and design of 6LoWPAN, the routing protocols used, and the security and privacy mechanisms used. There are three types of Lowpans: Ad-Hoc lowpan, Simple lowpan and extended lowpan. I am going to write about the innovative ways to implement security in 6LoWPAN. 6LoWPAN is different because of its small address size and low power features. Hence, to make 6LoWPAN secure new and unique challenges needs to be addressed. The routing protocols in 6LoWPAN are very sensitive because of the limited node's capabilities in terms of power, transmission range and so on. Hence, it is based on layering decisions: application-based, and other parameter bases.

CHAPTER 1. INTRODUCTION

Wireless networks work in accordance with the IEEE 802.15.4 standard which is based on proprietary protocols. This makes the expandability, interoperability and compatibility with one another very difficult. Ipv6 has made a lot of difference and given a lot of hope for wireless embedded devices to run and communicate with one another seamlessly, this is because of the large number of internet address range, which can make more devices available to the internet and make it accessible to the internet. This motivated the Internet Engineering Task Force (IETF) to create the 6LoWPAN standards. 6LoWPAN defines how to layer IPv6 over low data rate, low power and small radio footprint which makes relatively small and low power embedded devices to communicate with the internet and make the internet of things more robust and expandable.

The 6LoWPAN nodes are suitable for devices with small size, constrained power, limited computing and storage resources. Wireless sensor networks is a subtype of LoWPAN,

The characteristics of 6LoWPAN are:

1. The packet size of 6LoWPAN is relatively small i.e. 127 bytes. The resulting maximum size at media access control layer is 102 octets. Out of the 102 octets Link-layer security imposes further overhead of 21 octets in AES-CCM-128, 9 for AES-CCM-32, and 13 for AEC-CCM-64. This leaves 81 octets for data packets [4].
2. 6LoWPAN supports 16-bit short and IEEE 64-bit media access control addresses.
3. The data rates are 250 kbps, 40kbps, and 20 kbps which is relatively low. Hence low-bandwidth is a strategy that 6LoWPAN uses.
4. Star and mesh topologies can be implemented on 6LoWPAN.

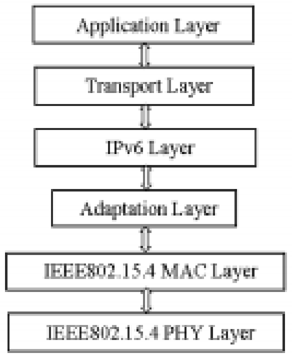
5. Low powered devices: most of the devices are battery operated hence 6LoWPAN must be able to function seamlessly.
6. The devices used in 6LoWPAN are based on sensors or switches, which have low processing and low memory, which makes the devices low cost [4].
7. The devices deployed using 6LoWPAN are in a very large number, it is estimated that the number of devices on the 6LoWPAN will outnumber the total number of personal computers.
8. The devices used in 6LoWPAN may be moving at a fast rate, because they are deployed in an ad-hoc manner. The location can be new and not easily accessible.
9. The reliability of 6LoWPAN devices are low because of uncertainty of radio connectivity, battery drain, device lockups or physical tampering.
10. Sleep time for devices connected to 6LoWPAN may be high to conserve energy. [4]

Fields where 6LoWPAN can be used in:

1. Embedded devices required to communicate with internet-based services.
2. Heterogeneous networks which are low-powered and coupled together.
3. Where scalability is required across outsized network infrastructures with mobility.
4. Automation of healthcare and logistics
5. Building and home automation
6. Enhanced energy efficiency and effectiveness
7. Automation of industries
8. Environment monitoring and forecasting in real time.

9. Smart grid and smart metering

10. Automation in vehicles



6LoWPAN protocol stack reference model [11]

.

CHAPTER 2. HISTORY OF 6LOWPAN

In 1990s it was assumed that Moore’s law would advance computing and communication capabilities at a very rapid pace, making embedded devices implement IP protocols. This was true to an extent, but it didn’t hold true for low powered, cheap microcontrollers and low-power wireless radio technologies. The reason was small microcontrollers made use of 8-bit and 16-bit memory which led to a lot of limitations to implement the traditional IP addressing and networking. The early work on minimizing internet protocols to be compatible with low-power microcontrollers and wireless technologies includes the µIP from the Swedish Institute of Computer Science [2] and NanoIP from the Centre for Wireless Communications [3]. In 2003 the IEEE 802.15.4 standard was released which was the reason that led to the 6LoWPAN standardization. As the IEEE 802.15.4 standard grew in popularity the internet community got encouragement to standardize the IP adaptation for wireless embedded microcontrollers which fits into the criteria for the 6LoWPAN technology.

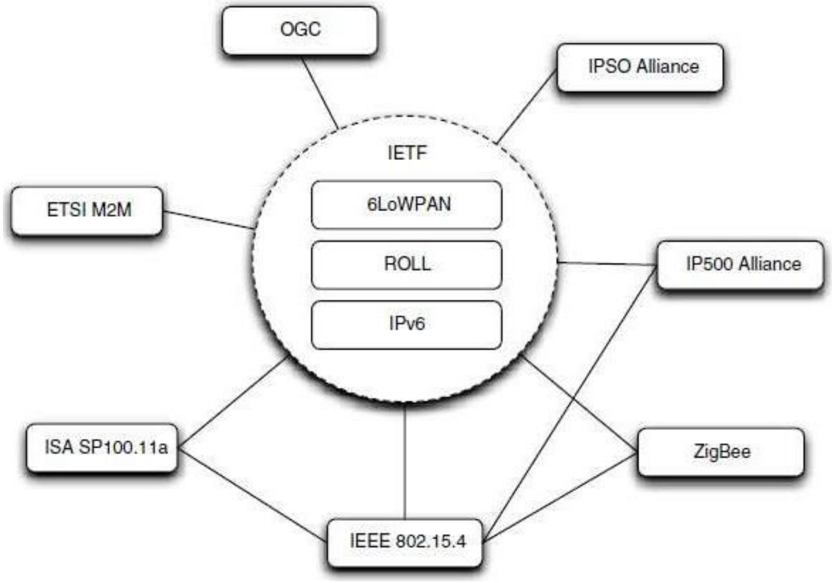


Figure 1: Relation of 6LoWPAN with related standards and alliances.[1]

6LoWPAN specification was first released in 2007, this specification gave an informational RFC 4919 which specified the underlying requirements and goals of the initial standardization, later updates were released which gave a standard track RFC4944 which specified the 6LoWPAN format and functionality. After the experiment and implantations phases were done, the 6LoWPAN working group continued with improvements to the header compression, 6LoWPAN Neighbor discovery and routing requirements.

Later in 2008 a new IETF working group was formed, named as Routing over Low-power and Lossy Networks (ROLL). This working group specified the requirements and solutions for low-power, wireless, unreliable networks. Although these requirements did not restrict an embedded network from using 6LoWPAN, it was a major target.

The ISA in 2008 started to standardize the wireless industrial automation system called SP100.11a, this standardization is based on the 6LoWPAN architecture.

The latest activities related to 6LoWPAN include the IP for Smart Objects (IPSO) Alliance, which was founded in 2008 to promote the use of smart objects and Internet of things in business. The IP500 alliance is developing a recommendation for 6LoWPAN over IEEE 802.15.4 sub-GHz radio communications. Other trends also have an impact on the success of 6LoWPAN technology; they include the ZigBee, machine-to-machine (M2M) communications, the future internet, and the wireless sensor networks (WSNs).

ZigBee protocol had several downsides, which includes reliance on a single wireless link technology, tight coupling with application profiles, and integration and scalability limitations. In 2009 the ZigBee alliance announced that it would integrate the 6LoWPAN and ROLL IETF standards into its future specifications. This led to a much wider range for the ZigBee controller that was beyond just ad-hoc control. 6LoWPAN was also considered a very crucial specification for machine to machine services as it helped extended the capabilities of machine to machine communication by connecting to M2M services through simple routers.

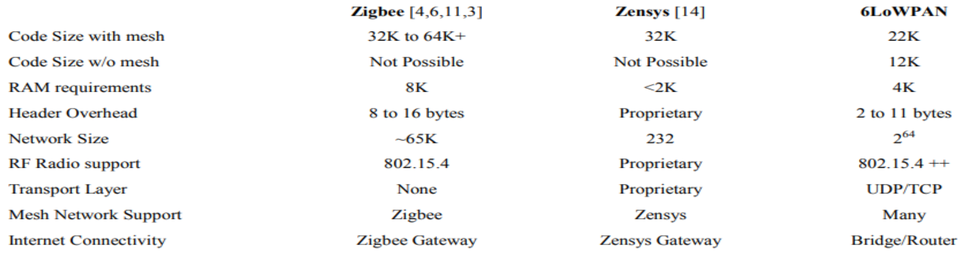
According to the article published by eetimes [1] these are the main reasons why the 6LoWPAN has flourished and grown to the level it currently is.

CHAPTER 3. ARCHITECTURE OF 6LOWPAN

In the 6LoWPAN architecture paper by Geoff Mulligan [1], the 6LoWPAN header size is discussed. The IPv6 address size was increased to 1280 byte MTU, implementing such a high address size would be impractical for 6LoWPAN because of the low power, low energy requirement of small-embedded systems. Hence, the final design takes the concepts of ipv6 and encodes the large ipv6 headers into smaller compressed headers. The ipv6 header can be compressed to as small as 4 bytes meanwhile allowing the features of mesh networks, fragmentation and reassembly. This concept is known as "stacked header" which is similar to the concepts of "you get what you pay for".

This paper first discusses about the need to use the traditional IP protocols rather than creating a new proprietary protocol. IP protocols, which can be pushed to the very edge of the network devices flattens the naming and addressing hierarchy which simplifies the connectivity model. IP protocols also removes the need for complex gateways that in the past, were necessary to translate between proprietary protocols and standard internet protocols. These complex gateways can be replaced by smaller bridges and routers, the good point about the use of bridges and routers is that they are well understood, widely developed and widely available technologies. Another advantage of using IP based protocols is that users can use tools, which are already developed for commissioning, configuring, managing and debugging these

Table 1. Stack Comparison



	Zigbee [4,6,11,3]	**Zensys** [14]	**6LoWPAN**
Code Size with mesh	32K to 64K+	32K	22K
Code Size w/o mesh	Not Possible	Not Possible	12K
RAM requirements	8K	<2K	4K
Header Overhead	8 to 16 bytes	Proprietary	2 to 11 bytes
Network Size	~65K	232	2^{64}
RF Radio support	802.15.4	Proprietary	802.15.4 ++
Transport Layer	None	Proprietary	UDP/TCP
Mesh Network Support	Zigbee	Zensys	Many
Internet Connectivity	Zigbee Gateway	Zensys Gateway	Bridge/Router

networks. Hence, developing entirely new tools and developing skills to handle these new protocols are not necessary. The developers can use the existing standards, which may intern speed up the design, and development process, for example using the RPL protocol for routing would be a better option than creating a completely new protocol from scratch because there is already enough research and testing on the RPL protocol. Other protocols that come under the IP standards are UDP, TCP, ICMP, DNS, and TFTP. Higher standards like load balancing, Caching, Firewalling and mobility could also be used in the designing of the sensor networks.

[5][6][7]

The above stack comparison shows 6LoWPAN has low-cost credentials in comparison to the others. 6LoWPAN has eliminated the use of NAT and DHCP by using zero configuration and neighbor discovery features of the ipv6 protocol, this further reduces the load of 6LoWPAN technology. The basic headers defined in 6LoWPAN are dispatch header, mesh header, fragmentation header and HC1 header (IPv6 header compression header). In the most basic case the mesh header and fragmentation headers can be eliminated and only dispatch header, HC1 header and the IPv6 compression header can be used which sums up to about 4 bytes. Fragmentation header is optional because only while sending large packets, we need to fragment it and while using a mesh network layer under 6LoWPAN there is a need for mesh network header.

60% of the energy spent by sensor devices are generally spent while waiting for the radio and microcontroller to warm up [8] [9] and approximately 90 % is wasted in waking up and listening when there is no data to be heard [9]. Even after looking at this rate, there is a big need for efficiency to utilize the limited available energy and bandwidth. When implementing

6LoWPAN on a T1 MSP430 micro-controller and CC2420 radio, the energy overhead is 2.8% for small data payloads and 2% for data payloads, which are near the frame capacity [10].

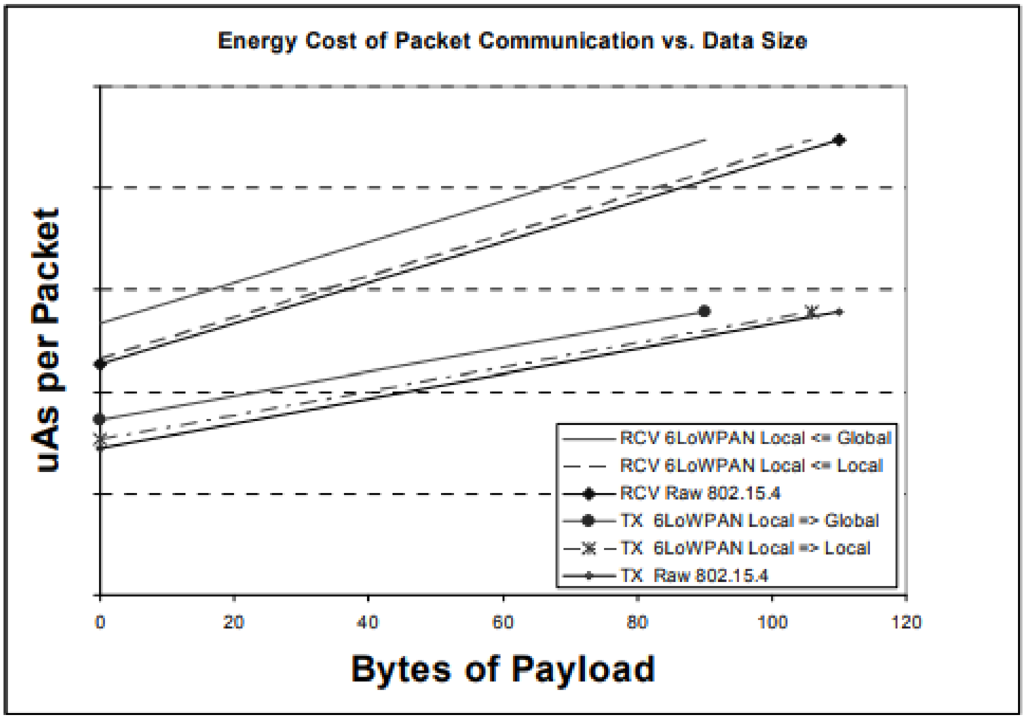


Figure 4: Energy overhead in 6LoWPAN [8]

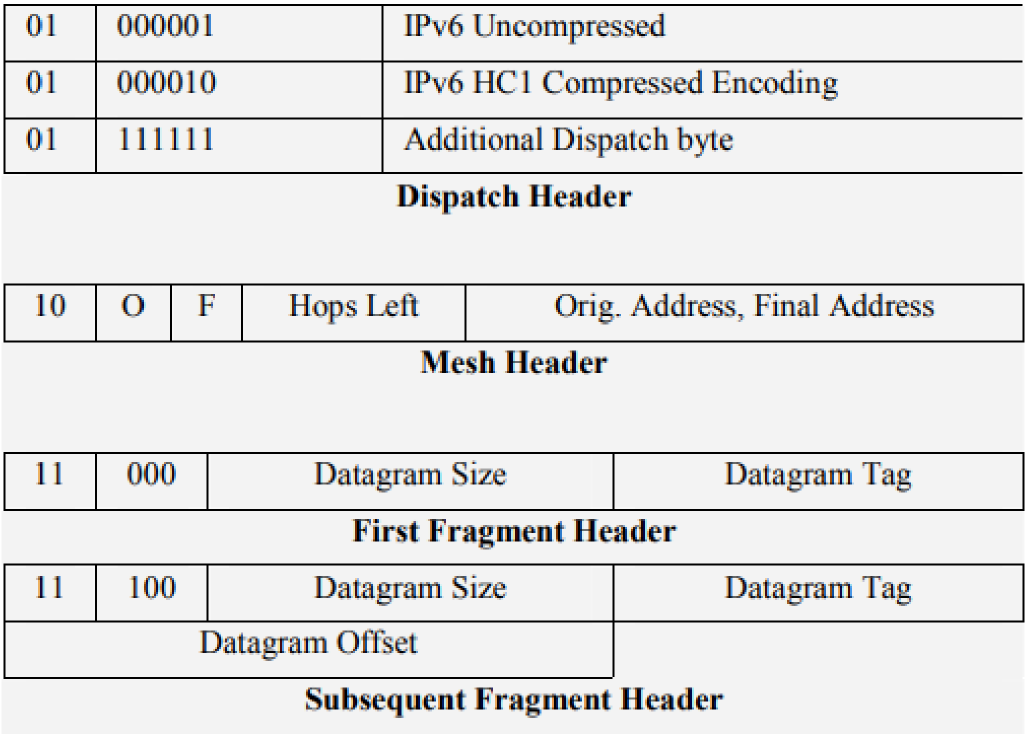
The above graph shows the overhead for local and global transmission header energy costs. The values are calculated by adding the total energy to transmit the packet, which includes the time to wake up the controller and radio. These values are compared to the added overhead of transmitting the 6LoWPAN header. The difference between the local and global overhead is the amount of time required to remove or compress the ipv6 128-bit addresses for local transmission.

6LoWPAN Header Details

Every 6LoWPAN header has a type identifier, these type identifiers are used to identify the headers with a predefined prefix. The dispatch header is 1byte long and the 1s two bits identifies is set to 01 if the network is a 6LoWPAN network or set to 01 if it is a non 6LoWPAN network. The remaining 6 bits are used to indicate whether the field is an uncompressed IPv6 header or an HC1 header defining the IPv6 compressed header. When the type identifier is set to all ones, it means that the header contains an additional byte to allow for 256 more header types.

The mesh header that is 4 bytes long is implemented to standardize how to encode the hop limit, the link layer source and destination of the packet [5]. The mesh header also indicates whether the address size is 16 bit short or 64-bit standard. The hops left is a 4-bit field that is used to indicate the hop limit between the source and destination. The special value of 0xF can be used to allow for network depths of up to 255 hops.

The fragmentation header is about 4 bytes long for the 1st fragment and 5 bytes for the fragments after the first fragments. This header is implemented to support the fragmentation and reassembly of payloads that are larger than the size of the 802.15.44 frame I.e. 102 bytes [11], it includes the fields to specify the size of the original payloads, the size of the original datagram and the sequence numbers for ordering the packets. The datagram tag field is used to identify all the fragments of a single original packet. This fragmentation header is implemented to comply with the ipv6 standards because the IPv6 protocol is required to support a minimum MTU size of 1280 bytes. Most of the sensors would not be using such high data payloads.



01	000001	IPv6 Uncompressed
01	000010	IPv6 HC1 Compressed Encoding
01	111111	Additional Dispatch byte

Dispatch Header

10	O	F	Hops Left	Orig. Address, Final Address

Mesh Header

11	000	Datagram Size	Datagram Tag

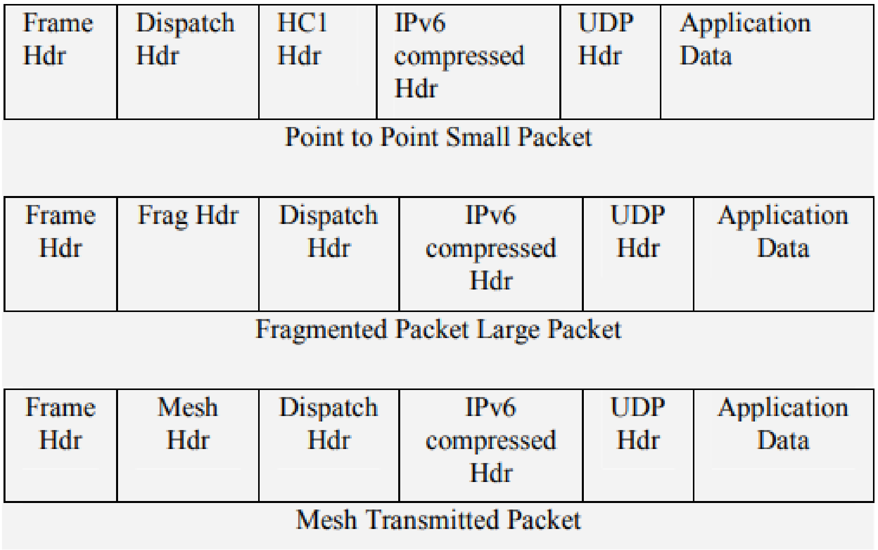
First Fragment Header

11	100	Datagram Size	Datagram Tag
Datagram Offset			

Subsequent Fragment Header

Figure 5: The header layout for 6LoWPAN [5]

Stack headers are implemented so that only what headers the packets require will be used which saves a lot of memory since useless data would not be sent.



Frame Hdr	Dispatch Hdr	HC1 Hdr	IPv6 compressed Hdr	UDP Hdr	Application Data

Point to Point Small Packet

Frame Hdr	Frag Hdr	Dispatch Hdr	IPv6 compressed Hdr	UDP Hdr	Application Data

Fragmented Packet Large Packet

Frame Hdr	Mesh Hdr	Dispatch Hdr	IPv6 compressed Hdr	UDP Hdr	Application Data

Mesh Transmitted Packet

Figure 6: stacked headers [5]

The first case shows a small packet that is point to point, since it is a small packet it uses HC1 header to show the use of compressed IPv6 header and it does not contain the fragment header this header will comprise of approximately 2 bytes.

The second case show a large packet, this packet will use a fragmentation header and a dispatch header to keep account of the fragments and sequence numbers used. This header will be 5bytes long.

The third case show a mesh transmitted small packet, this packet will need the mesh header along with the dispatch and HC1 headers, and it requires about 6 bytes.

HC1 header is responsible for header compression of the IPv6 header. To be successful with this goal the HC1 header need to use the following facts:

1. The ipv6 address used can be a EUI-64 link local address where the lower 64 bits are the devices mac address.
2. The 802.15.4 frame carries these MAC addresses.
3. Some of the fields in the ipv6 are static.

Using all the above features make it possible to compress the standard ipv6 header size to 2 bytes. The remaining fields can be reconstituted without any state information at any of the receiving or intermediate nodes. The use of link local addresses makes it possible to eliminate the need for DHCP servers as the 6LoWPAN can use auto-configuration.

The stacked header approach makes it possible for protocols to extend their header types and define new mesh network layers this can be done by just requesting allocation for a new dispatch type from the IANA.

This section gives details about the 6lowpan headers, and how these headers are used in data communication.

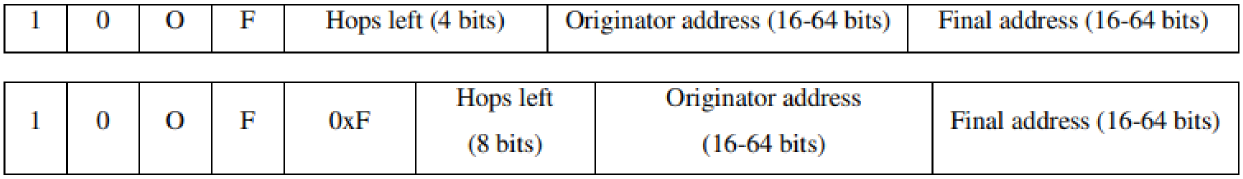
CHAPTER 4. 6LOWPAN ROUTING PROTOCOLS

After reading and analyzing the paper “A Review of 6LoWPAN Routing Protocols” by Gee Keng Ee, Chee Kyun Ng, Nor Kamariah Noordin and Borhanuddin Mohd Ali. I have understood the different concepts related to 6LoWPAN routing protocols.

The most popular routing protocols used in 6LoWPAN are Ad-Hoc On-Demand Distance Vector (AODV), On-Demand Distance Vector (LOAD) and Dynamic Magnet, this paper analyzes the used control messages for the route discovery in different routing protocols. There is a comparison made between different routing protocols in terms of their routing metric such as hop count.

The IPv6 network can accomplish intra-PAN routing via layer-three (adaptation layer) forwarding, in this type of forwarding each 802.15.4 radio hop is an IP hop. As we have seen earlier in the 6LoWPAN architecture the mesh header was defined by the 6LoWPAN to accomplish multi-hop packet forwarding. The mesh header is used to standardize the way to encode the hop limit and the link layer source and destination of the packets. In 16-bit addressing mode the value of originator O and final destination F is one while in a 64-bit addressing mode it is zero. In mesh routing, the sender sets the originator’s link layer address in the Mesh Header to its own address and the final destination link layer address to the packet’s ultimate destination. It also sets the MAC frame to its own link-layer address and puts the forwarder’s link layer address in the destination address field of the MAC frame. After doing this the sender transmits the packet. If the receiver is the final destination of the packet, it consumes the packet, else it reduces the “hops left” field and consults its link layer routing table to change the source address in the MAC frame as its own destination address in the

MAC frame as the next hop towards the destination. If the "Hop left" becomes zero the packet will be discarded.



1	0	O	F	Hops left (4 bits)	Originator address (16-64 bits)	Final address (16-64 bits)

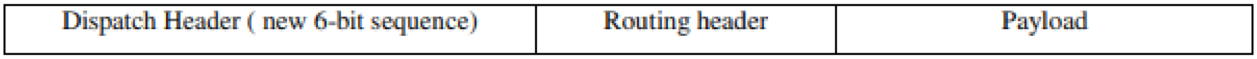
1	0	O	F	0xF	Hops left (8 bits)	Originator address (16-64 bits)	Final address (16-64 bits)

Figure 7: Mesh header

Beyond the mesh header additional routing information can be appended appropriately with the headers to achieve full routing information. There are two routing scheme categories in 6LoWPAN i.e. the mesh under and route over [11].

Mesh under: Performs its routing in the adaptation layer and performs no IP routing within 6LoWPAN network layer where it is based in the IEEE 802.15.4 MAC addresses.

Route over: In the route over approach the routing is performed at the network layer and each node serves as an IP router. The globally unique IP address of each node is created automatically by appending its interface identifier to the IPv6 prefix that is received via router advertisement (RA).



Dispatch Header (new 6-bit sequence)	Routing header	Payload

Figure 8: 6LoWPAN routing header encapsulation [11]

In a mesh-under routing protocol, the routing control packets are placed after the 6LoWPAN dispatch header. In the above diagram we can see that a new dispatch value is required to be assigned for mesh-under routing. By using the dispatch header sequence, multiple routing protocols can be supported on the 6LoWPAN networks.

In route-over protocol, one of the pre-defined dispatch patterns can be chosen as the dispatch value, a compressed or uncompressed IPv6 header will follow this, and route-over routing header will be included in the payload of the IPv6 packet [12].

6LoWPAN Ad-Hoc On Demand Distance Vector Routing (LOAD)

LOAD is a type of AODV, but it is more simplified [13], it runs on the adaptation layer rather than the transport layer. LOAD creates a mesh network topology under the IPv6, therefore IPv6 sees the 6LoWPAN as a single link. LOAD doesn’t use the destination sequence number that is used in AODV. The destination of the route generates the Route Reply (RREP) in reply. The routing metrics in LOAD are the accumulated route cost like LQI and the number of hops from source to destination. If the number of weak links in a route are lesser, the route will be preferred in LOAD. LOAD doesn’t use the precursor list that is used in the AODV routing protocol. These lists used in AODV are to forward the route error (RERR) message in case of a broken link along the route of a data message or the next hop cannot be found in the destination routing table.

The LOAD mechanism responds to link break by making the upstream node try to repair the route locally using route discovery mechanism. The route discovery mechanism uses the Route Request (RREQ) and unicast (RREP) messages. If the repairing node is unable to fix the node, the repairing node will send a unicast (ERRR) message which will give the originator the reason for the repair failure of the failed data message only. The AODV needs a precursor list for forwarding the RERR message. LOAD uses the link layer acknowledgement to save energy instead of a hello message to save energy while keeping track of the route connectivity. LOAD requests MAC layer acknowledgements for every sent data message, which is termed as Link Layer Notification.

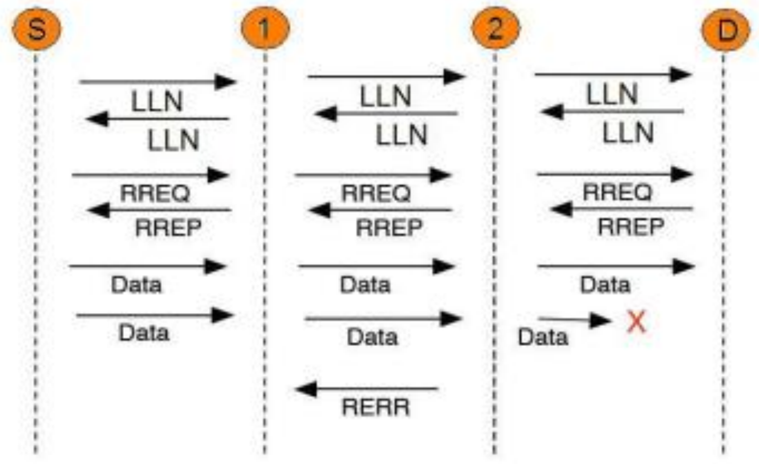


Figure 9: Exchanging the messages using load protocol. [11]

Dynamic MANET On-Demand For 6LoWPAN Routing (DYMO-low)

The DYMO protocol is a simplified version of the AODV protocol which is a simple and effective routing protocol. DYMO performs route discovery and maintenance using the messages: RREQ, RREP, RERR. It uses the RREQ and RREP messages for route discovery, these messages are used to accumulate routing information from each intermediate node. DODV protocol doesn’t use local repair like AODV and doesn’t send hello messages to keep track of the link connectivity. DYMO is implemented above the IP and uses User Datagram Protocol (UDP) as the underlying protocol. This protocol in its entirety cannot be implemented on the 6LoWPAN because it consumes a lot of memory and power [11]. To overcome the problem the DYMO-low was implemented [16], DYMO-low operates on the link layer directly to create a mesh network topology of 6LoWPAN devices unbeknownst to IP, and this causes the IP to consider the WPAN as a single link. DYMO-low can run on both 16-bit link layer short address or IEEE 64-bit extended address. The features which are present in LOAD are like those in DYMO-low except that 16-bits sequence numbers are used in DYMO-low to implement loop freedom. The underlying mechanism and working of LOAD and DYMO-low is same. DYMO-low doesn’t do local repair and route cost accumulations.

Hierarchical Routing (HiLow)

HiLow was proposed for 6LoWPAN to increase network stability. HiLow uses a 16-bit unique address as an interface identifier for memory saving and larger scalability. In HiLow, when there is a child device who wants to join a 6LoWPAN, it will first try to discover an existing 6LoWPAN by trying to scan the area, if it finds a network it will associate with the existing neighbor device and make the neighbor device its parent, it will then receive a 16-bit short address. If no 6LoWPAN is present, it will begin the 6LoWPAN network by itself, by doing so it assigns a zero to its short address.

The child node receives the short address using the equation.

$$C=MC*AP+N \qquad (0<N<=MC) \qquad [11]$$

In the above equation C is the child node address, MC is the maximum number of children a parent can have, AP is the address of the parent, N is the nth child node.

In HiLow, every node is assumed to know its own depth. The node that receives an IPv6 packet is known as the current node. The current node will then determine the next hop to forward the packet using the algorithm [17]. HiLow does not perform any path recovery mechanisms.

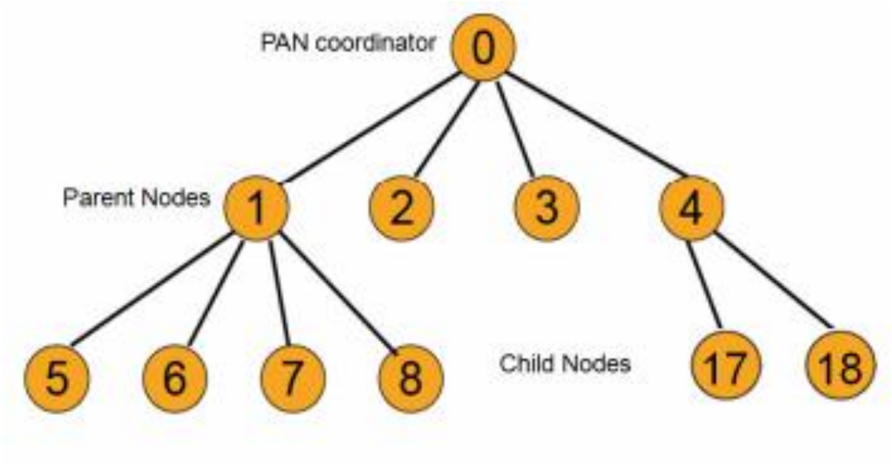


Figure 10: Structure of HiLow routing protocol. [11]

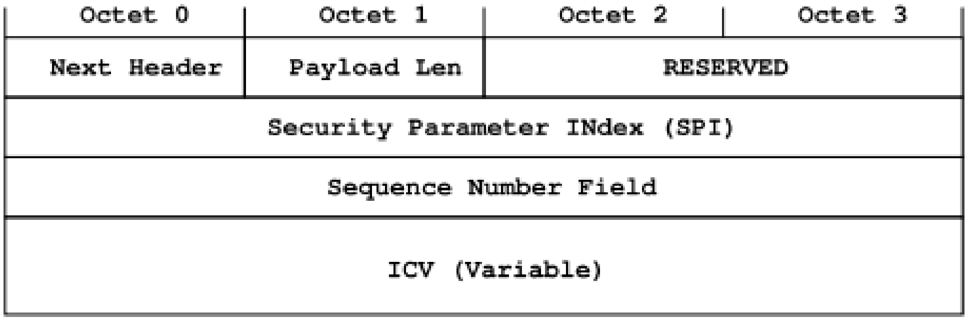
In this section I have reviewed the most popular routing protocols that can be used in the 6LoWPAN, I have written about their working in brief but there is sufficient data to understand the protocols functionality and mechanism.

CHAPTER 5. SECURITY IN 6LOWPAN

From the paper securing communication in 6LoWPAN with compressed IPsec by Shahid Raza, Simon Duquennoy, Tony Chung, Dogan Yazarm, Thiemo Voigt and Ulz Roedig, I have analyzed and understood the 6LoWPAN extension for IPsec. This extension supports IPsec's Authentication Header (AH) and Encapsulation Security Payload (ESP). This paper talks about the communication endpoints and how they are able to authenticate, encrypt and check the integrity of messages using standardized and established IPv6 mechanisms. This paper contributes in specifying, implementing, and evaluating of IPsec.

The IPsec is used for providing data integrity, authentication, and confidentiality. These features are made possible by using the two headers that IPsec defines. The 1st one is the Authentication Header which supports integrity and authentication whereas the 2nd header is known as the Encapsulating Security Payload (ESP) header, this header supports confidentiality, integrity and authentication. Either of these two headers can be used to provide security for IPv6 packets in transit. As we have seen in the earlier stages of this review, 6LoWPAN uses header compression techniques to reduce the size of headers by a significant amount (especially the IPv6 and transport-layer headers). In order to implement IPsec on 6LoWPAN, there needs to a reduction in the header size of the packet, this may difficult to implement because we cannot compromise security. But one positive point over here is that if we are using IPsec, we don't need to use other link layer security mechanisms, which will free up some header spaces.

IPsec provides security to the IPv6 protocols and defines protocols for securing the communication. Authentication header[15] and Encapsulating Security Payload[18], it also defines the algorithms for authentication, encryption and the key standard extensions along with the security associations SA [19].The IPsec specifies the pre-shared key and the Internet Key Exchange (IKE) to establish the SA, these SA are used to provide, how a flow should be treated in terms of security.



Octet 0	Octet 1	Octet 2	Octet 3
Next Header	Payload Len	RESERVED	
Security Parameter INdex (SPI)			
Sequence Number Field			
ICV (Variable)			

Figure 11: Authentication Header [14]

The authentication header's main purpose is to provide connectionless integrity and data origin authentication for IP datagram, it also protects against replays. The message authentication code (MAC) is used to produce the authentication data. Message authentication code is used in the AH header. Hosts that use the Authentication header will have to support a hash-based message authentication code algorithm AES-XCBC-MAC-96 [20]. This mac algorithm is used to calculate the authentication data which can is used in the AH.

ESP is used for encrypting payload of the IP packet; it provides origin authenticity, integrity and confidentiality protection to the IP packets. Unlike AH, ESP doesn't secure the IP header. ESP will store the encrypted payload which will be a part of the IP header, the ESP header will come before the IP header. The contents of the ESP header are SPI, a sequence number, the encrypted payload, padding, reference to the next header and optional authentication data. The SPI is used to identify the SA used, the sequence number is used to prevent replay attacks, padding is required by only some block ciphers.

The AH protocol supports transport mode whereas the ESP supports the tunnel mode. Transport mode secures the ip header and the payload, whereas in tunnel mode the encrypted secured part is added to the packet header as a separate header. The tunnel mode is not desired by the 6LoWPAN because it increases the overhead that is present due to the implementation of additional headers.

6LoWPAN_NHC Extension Header Encoding.

The NHC encoding form which is defined for IP extension headers can be used to encode the AH and ESP extension headers. HC13 defines compression using IPHC for IP headers and NHC for the next header, this is a context aware header compression. The NHC octets are present in the NHC encodings for the IPv6 extension headers, these NHC octets have 3 bits (bits 4,5,6) which are used to encode the IPv6 Extension Header ID (EID). Six out of eight possible EID values are specified by the HC13 draft. The rest two slots (101 and 110) are reserved. The two free slots can be used to encode AH and ESP. The last bit in the IPv6 extension header can be encoded to 1 to specify the next header (AH or ESP).[14]

LOWPAN_NHC_AH Encoding.

The NHC encoding for the AH is defined in this type of encoding scheme.

Each header field is described as:

1. The 1st four bytes in the NHC_AH will give the NHC ID that is defined for AH, this is set to 1101. This complies with the 6LoWPAN standard.[14]
2. Payload Length: The SPI value will provide the length for the payload, as the length of the authenticating data depends on the algorithm used and is fixed for any input size, the payload is omitted if this value is set to 0. If the payload length is set to 1 the length is carried inline after the NHC_AH header.[14]

3. SPI: If set to 1 the SPI is carried inline, and all nodes will use their preferred SPI values, but if it is set to 0 then the default SPI for the sensor will be used. The SPI field will consist of a default value of 1.[14]
4. SN: If 1 all 32 bits of sequence numbers will be used, and some will be carried inline whereas if it is set to 0 only 16-bit sequence number will be used because the leftmost 16 bits will be set to 0.[14]

The minimum length of a standard AH supporting the mandatory HMAC-SHA1-96 is 24 bytes. After compression we obtain a header size of 16 bytes.

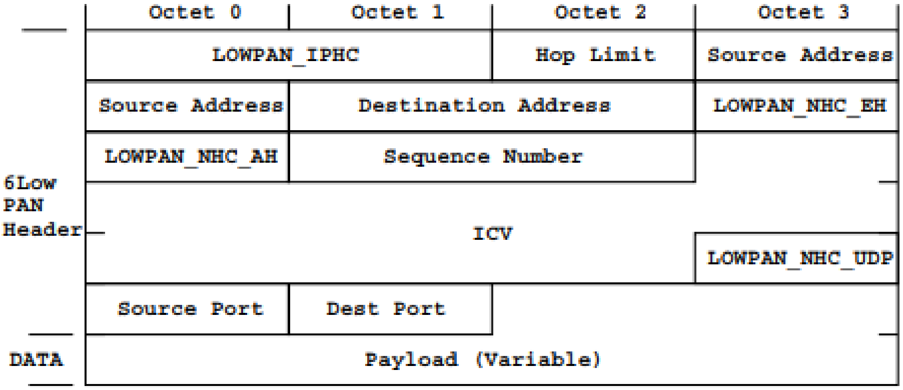


Figure 12: Compressed IPv6 packet using AH [14]

LOWPAN_NHC_ESP Encoding.

The security parameter index, the sequence number, the next header fields and the NHC id for ESP is encoded using NHC. This paper proposes 1110 as NHC ID and 1101 as NHC for AH. The full details for this type of assignment wasn’t explained in the paper because of space limitation. The ESP overhead without authentication along with AES-CBC and perfect block alignment comes to 18 bytes. But after doing some compression it can be reduced to 12 bytes. ESP also has an overhead of 30 bytes, which after compression can be reduced to 24 bytes. [14]

The 6LoWPAN nodes, which are capable with AH, can directly communicate with unmodified IPsec hosts on the conventional internet. 6LoWPAN nodes with ESP can also directly communicate with unmodified hosts on the internet. If ESP is used and if the upper layer headers like UDP cannot be compressed then there is a need for gateways between the sensor network, the IP header will be unable to expand and access the encrypted UDP headers. The UDP header compression along with ESP is not possible with the traditional compression algorithms; therefore, a new compression algorithm needs to be implemented to complete the task.

Secure Authentication and Key Exchange Schemes in 6LoWPAN

From the paper SAKES: Secure Authentication and Key Establishment Scheme for M2M Communication in the IB-Based Wireless Sensor Network (6LoWPAN) be Hassan Redwan Hussen, Gebere Akele Tizazzu, Miao Ting, Taekkyeun Lee, Youngjun Choi and Ki-Hyung Kim I have learnt the key exchanged and secure authentication schemes that is used in 6LoWPAN.

The different security attack scenarios for 6LoWPAN are sinkhole attack: in this type of attack the attacker can spoof to tell that it is the best node to the destination. So the attacker can attract many nodes to connect to it by spoofing.

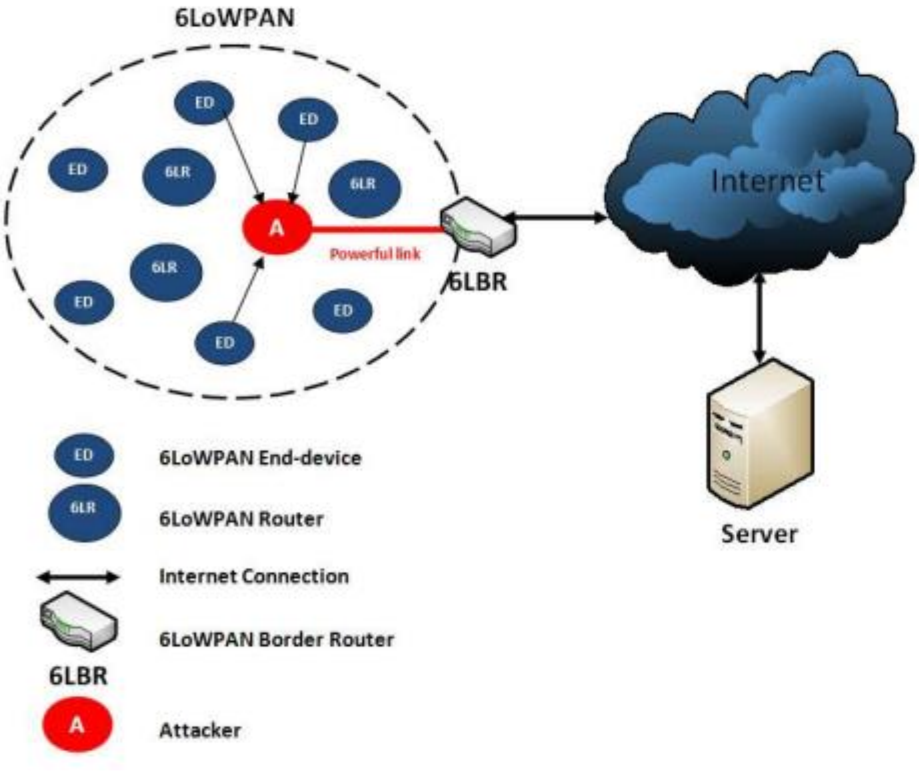


Figure 13: Spoof-attack example. [21]

Another attack is a wormhole attack, in this type of attack the attacker can cause collision between two nodes; the attacker creates a false impression regarding the packets that are sent between nodes. The packets that are send between large nodes will be shown to have lesser number of packets in comparison to their actual value. This can cause obscurity in the traffic flow for all the nodes in the network. Therefore, the attacker can use wormhole link to show different path of the packet transmissions. Which can cause resource depletion for no reason.

This paper uses key authentication to demonstrate authentic communication between two nodes, and if there is proper encryption between the data sent, then the above attacks can be avoided.

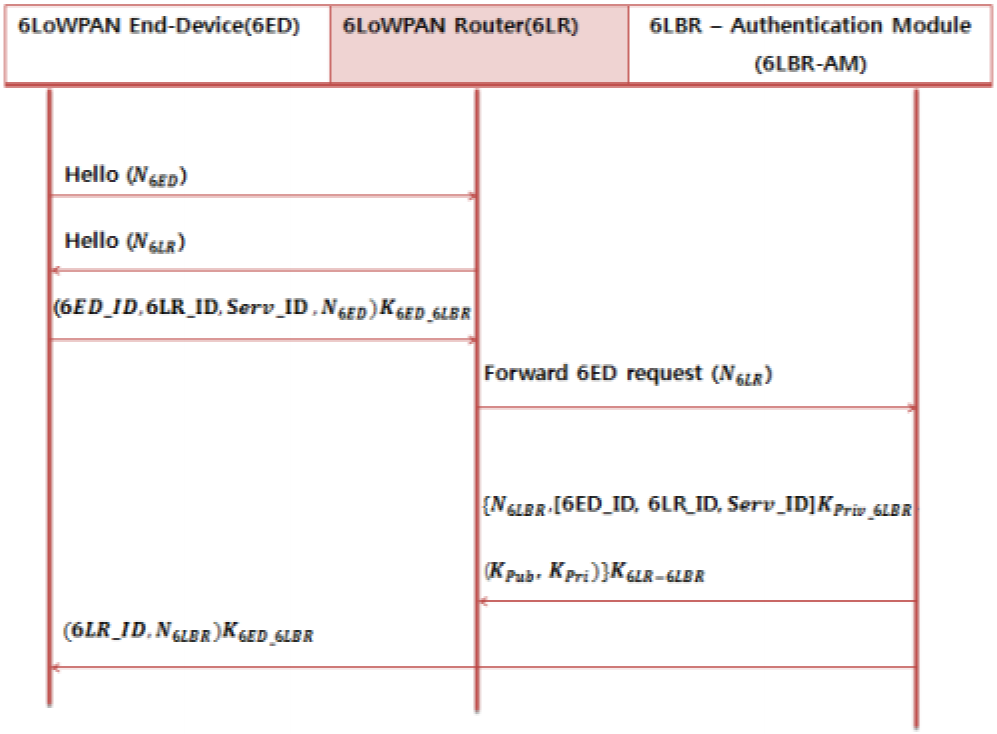

6LoWPAN End-Device(6ED)
6LoWPAN Router(6LR)
6LBR – Authentication Module (6LBR-AM)
Hello (N_{6ED})
Hello (N_{6LR})
($6ED\_ID$, 6LR_ID, $Serv$_ID , N_{6ED})K_{6ED_6LBR}
Forward 6ED request (N_{6LR})
{N_{6LBR},[6ED_ID, 6LR_ID, $Serv$_ID]K_{Priv_6LBR}
(K_{Pub}, K_{Pri})}$K_{6LR-6LBR}$
($6LR\_ID$, N_{6LBR})K_{6ED_6LBR}

Figure 14: Authentication messages [21]

This paper gives details about the way to authenticate the messages that are sent and received between nodes, it gives the algorithm and pseudo code that is used. It uses Diffie-Hellman key exchange technique to transmit data. This technique can be used in areas such as smart grid, metering, transportation, health and environmental monitoring.

In this section, we have studied about the different security mechanisms used in 6LoWPAN and the reason why security in 6LoWPAN is hard to implement.

CHAPTER 6. CONCLUSION

In this paper, we have at a variety of topics in the 6LoWPAN domain. The history of 6LoWPAN talked about the various stages in the development of 6LoWPAN and how it evolved to its current stage. In the architecture part of the paper, we looked at the header format of 6LoWPAN networks. The important part of the architecture is getting the size of the header to be so small that it runs on devices, which use low power and energy resources. In the routing section, we looked at the different routing protocols that will be suitable for 6LoWPAN. In the security part, the implementation of IPsec in 6LoWPAN was studied. 6LoWPAN is a technology, which facilitates the growth of the internet of things; IOT is considered the future of the internet. Many different embedded devices will be able to smoothly communicate with each other using 6LoWPAN. 6LoWPAN can be used in variety of applications in the future such as small-embedded systems, which use low power and have low memory that need to communicate with internet based services. Therefore, thousands of these sensors can be used to communicate with the internet, which will redesign how systems work. Low-power heterogeneous networks that have to be coupled together, in the future this will change because of 6LoWPAN since low power network devices will be capable to communicate on the internet, the need to be coupled will be eliminated and these devices will work independently. Using 6LoWPAN technology healthcare automation will increase drastically in the future because even small medical instruments for example a thermometer will be capable to access the internet, this will result in a much better healthcare system. This technology can be used in supply chain management, where packages need to tracked and distributed with precision. 6LoWPAN can be used in the construction and building industries where the tools and machines can become more efficient. In energy efficiency and power generation industries, 6LoWPAN has tremendous applications. This is because applications such as the smart thermostat has proven to be beneficial in saving energy on a per household basis. The implementation of the smart grid and other power management technologies can be very helpful in saving environmental resources. In the health and fitness, industry 6LoWPAN enabled sensors can be used in sensors measure different bodily functions such as heartbeat, ECG etc. that is crucial for personal growth. The rate of industry automation can be increased in the future using 6LoWPAN technology. 6LoWPAN can be used in environmental monitoring and weather forecasting, because of the vast amount of sensors present in the weather monitoring equipment, the way in which the sensors communicate with each other can be improved. 6LoWPAN can be used in artificial intelligence and various machine-learning applications..

REFERENCES

[1] “6LoWPAN: The Wireless Embedded Internet - Part 2: 6LoWPAN History, Market Perspective & Applications.” *EETimes*, www.eetimes.com/document.asp?doc_id=1278812

[2] Braun, Torsten, Thiemo Voigt, and Adam Dunkels. "Energy-efficient TCP operation in wireless sensor networks." *Praxis der Informationsverarbeitung und Kommunikation* 28.2 (2005): 93-100.

[3] Jardak, Christine, et al. "Implementation and performance evaluation of nanoip protocols: Simplified versions of tcp, udp, http and slp for wireless sensor networks." *Wireless Communications and Networking Conference, 2008. WCNC 2008. IEEE*. IEEE, 2008.

[4] Kushalnagar, Nandakishore, Gabriel Montenegro, and Christian Schumacher. *IPv6 over low-power wireless personal area networks (6LoWPANs): overview, assumptions, problem statement, and goals*. No. RFC 4919. 2007.

[5] Mulligan, Geoff. "The 6LoWPAN architecture." *Proceedings of the 4th workshop on Embedded networked sensors*. ACM, 2007.

[6] Galeev, M. Home Networking wit Zigbee http://www.embedded.com/showArticle.jhtml?articleI D=189 02431

[7] Jones, S. TI Zigbee Z-Stack on the CC2430 and MSP430 http://www.motherboardpoint.com/t161906-ti-zigbee-zstackon-the-cc2430-and-msp430.html

[8] Culler, D., Hui, J. 6LoWPAN Tutorial. Tiny OS Technology Exchange 2007

[9] Pister K., Conant, R. Dust Networks – Bringing the information revolution to the Physical World http://www.dust-inc.com/news/web_seminars/06-12-06%20Seminar_Presentation.pdf

[10] IEEE Computer Society IEEE 802.15.4 – Wireless Medium Access Control and Physical Layer (PHY) Specifications for Low-Rate Wireless Personal Area Networks (WPANs)

[11] Ee, Gee Keng, et al. "A review of 6LoWPAN routing protocols." *Proceedings of the Asia-Pacific Advanced Network*30 (2010): 71-81.

[12] Kim, E.; Kaspar, D.; Gomez, C.; Bormann, C.; Problem Statement and Requirements for 6LoWPAN Routing”, daft-ietf6LoWPAN-routing-requirements-02, 2009.

[13] Kim, K.; Daniel Park, S.; Montenegro, G.; Yoo, S.; Kushalnagar, N. 6LoWPAN Ad Hoc On-Demand Distance Vector Routing (LOAD), draft-daniel-6LoWPAN-load-adhoc-routing-03, 2007

[14] Raza, Shahid, et al. "Securing communication in 6LoWPAN with compressed IPsec." *Distributed Computing in Sensor Systems and Workshops (DCOSS), 2011 International Conference on*. IEEE, 2011.

[16] Kim, K.; Park, S.; Chakeres, I.; Perkins, C. Dynamic MANET On-demand for 6LoWPAN (DYMO-low) Routing, draftmontenegro-6LoWPAN-dymo-low-routing-03, 2007.

[17] Kim, K.; Yoo, S.; Park, J.; Daniel Park, S.; Lee, J. Hierarchical Routing over 6LoWPAN (HiLow)”, draft-deniel-6LoWPANHiLow-hierarchical-routing-00.txt, 2005.

[18] S. Kent. IP Encapsulating Security Payload. RFC 4303, 2005

[19] S. Kent and K. Seo. Security architecture for the internet protocol. RFC 4301, 2005

[20] V. Manral. Cryptographic algorithm implementation requirements for encapsulating security payload (esp) and authentication header (ah). RFC 4835, 2007

[21] Hussen, Hassen Redwan, et al. "SAKES: Secure authentication and key establishment scheme for M2M communication in the IP-based wireless sensor network (6L0WPAN)." *Ubiquitous and Future Networks (ICUFN), 2013 Fifth International Conference on*. IEEE, 2013