IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified
Vol. 6, Issue 6, June 2017

Cryptanalysis of IPv6 for Secure Communication in Internet of Things

Ms. Aishwarya Ashok Akul[1], Prof. Mrs. Snehal Bhosale[2]

Student (ME), Electronics and Telecommunication, R.M.D Sinhgad School of Engineering, Pune, India [1]

Professor, Electronics and Telecommunication, R.M.D Sinhgad School of Engineering, Pune, India [2]

Abstract: Network security is an important issue in internet of things. An IPv6 network interconnects computer and large number of smart devices .these devices have sensing and actuation capability. These smart devices are connected to the internet, there is possibility that these devices can come under attack. The receiver should be able to verify the sensor data generated by trusted nodes. In some cases it may also be necessary to encrypt sensor data. There are many challenges and issues of implementing secure communication in IOT. We proposed a system, which resolves issue of secure communication. In this paper, we are using IPSec protocol (IPv6) in network .which can authenticate and encrypt the packets of data sent over the network. In this paper, we used AES algorithm for encryption and decryption of the data so attacker cannot modify the packet data. By using IPv6 and AES algorithm we provide End to End secure communication between smart devices on internet.

Keywords: Internet of things; 6LoWPAN; IPv6; AES algorithm; IPSec.

I. INTRODUCTION

Sensor Networks are usually tightly integrated with existing IP based infrastructures using IPv6 over 6LoWPAN. By using 6LoWPAN, sensor node will directly communicate with IPv6 hosts. Thus, 6LoWPAN resolve operation and integration of Internet of Things in existing infrastructures. IPv6 hosts within the internet support have a default IP security. IPv6 hosts in the internet support have a default IP security. if data streams between IPv6 hosts and 6LoWPAN sensor hubs then it's attractive to exploit existing abilities and to secure activity utilizing IPSec.
In earlier year network security has turn into an important issue in wireless sensor communication. Encryption has come up as a solution, and plays a crucial role in information security system. Several techniques are required to protect the shared information. The current work concentrate on cryptography to secure the information while transmission within the network. Firstly the information which is to be transmitted from sender to receiver within the network should be encrypted using the encryption algorithm rule in cryptography. Secondly, by using decryption technique the receiver will read the original information. The paper proceeds as follows, the next section discusses related work. Section III gives information of AES algorithm. In Section IV gives an overview of 6LoWPAN, and IPv6 packet, this section also describes block diagram and experimental setup of our proposed system. Section V we present our simulation results and the subsequent section concludes the paper.

II. RELATED WORK

A. Securing the IoT at the network layer
Granjal et al. [1] discussed the utilization of IPSec for 6LoWPAN. However, actual specifications of the desired 6LoWPAN headers are not given. Moreover, no implementation is provided and no elaborate evaluation of possible communication performance is given. In their study, they analyze the execution times and memory requirements of cryptographically algorithms that they projected for 6LoWPAN/IPSec integration.
The IPSec [2] protocol suite, mandated by IPv6, provides E2E security for any IP communication. Like TLS and unlike link-layer solutions, it includes a key exchange mechanism and provides authentication additionally to confidentiality and integrity. By operating at the network layer, it may be used with any transport protocol, as well as potential future ones. Moreover, it ensures the confidentiality and integrity of transport-layer headers and integrity of IP headers, that can't be carried out with higher level solutions as TLS. For these reasons the research community [3-5] and 6LoWPAN standardizations teams [6] consider IPSec a possible security answer for the IoT. On the opposite hand, some have regarded it as too heavy-weight possibility [7].

B. Embedding cryptographic algorithms
Much research work has focused on reducing complexity of cryptographic algorithms or on improving efficiency of key distribution protocols. For example, TinyECC [8] and NanoECC [9] provide elliptic curve cryptography in order to

IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified
Vol. 6, Issue 6, June 2017

make cryptography feasible on resource constrained devices. Wood and Stankovic [10] and Hu et al. [11] demonstrated efficient cryptography for smart objects using dedicated crypto hardware support. For example, Liu and Ning [12] and Chung and Roedig [13] described key distribution mechanisms that save scarce bandwidth in resource constrained networks.

III. ADVANCED ENCRYPTION STANDARD

Numerous encryption calculations are broadly accessible and utilized as a part of data security. They can be sorted into Symmetric (private) and Asymmetric (public) keys encryption. In Symmetric keys encryption or mystery key encryption, just a single key is utilized to scramble and unscramble information. In Asymmetric keys, two keys are utilized; private and open keys. Open key is utilized for encryption and private key is utilized for unscrambling. Open key encryption depends on scientific capacities, computationally concentrated.
In present day cryptography, AES is widely adopted and supported in both hardware and software system. AES is a repetitive instead of Feistel cipher. It is based on 'substitution–permutation network'. It contains a progression of joined operations, some of which include trade contributions by particular outputs substitutions and others include rearranging bits around changes strikingly, AES plays out every one of its calculations on bytes rather than bits. Consequently, AES treats the 128 bits of a plaintext block as 16 bytes. , the number of rounds in AES is variable and relies on upon the length of the key.AES utilizes 10 rounds for 128-piece keys, 12 rounds for 192-piece keys and 14 rounds for 256-piece keys. Each of these rounds utilizes an alternate 128-piece round key, which is ascertained from the first AES key.AES is a symmetric block cipher. This means that it uses the same key for both encryption and decryption.

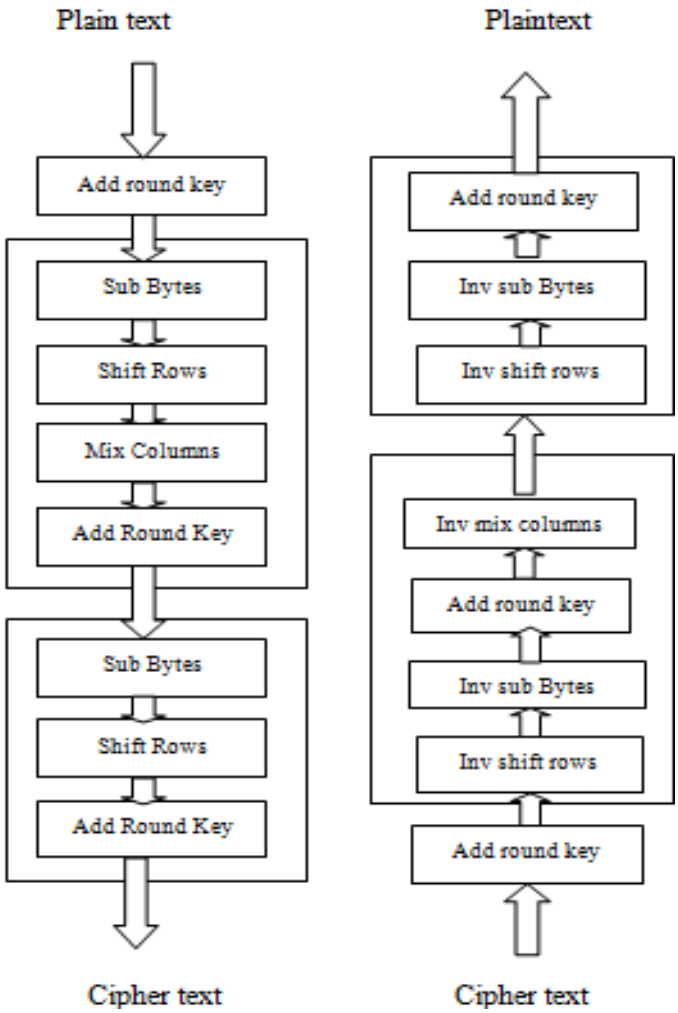

Fig. 1. AES encryption and decryption algorithm

The algorithms begin with an Add round key stage followed by nine rounds of 4 stages and a tenth round of 3 stages. This is applicable for both encryption and decryption with the exception that each stage of a round the decryption

IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified
Vol. 6, Issue 6, June 2017

algorithm is the inverse of its counterpart within the encryption algorithm. The tenth round simply leaves out the Mix Columns stage.

IV. SYSTEM IMPLEMENTATION

A . Packets used in Proposed System.

1) 6LoWPAN;

A 6LoWPAN The Low-power Wireless Personal Area Networks idea originated from that "the Internet Protocol should be the smallest objects, and that low-power object which is having limited processing capabilities should be able to participate in the Internet of Things. The 6LoWPAN is couple between the IEEE 802.15.4 and IPv6 i.e. between two different networks. The most important difference is the size of IEEE 802.15.4 supports only 127 octet's packet size wherever IPv6 packet supports 1280 bytes, where the solution proposed by using 6LoWPAN an adaptation layer that optimize IPv6 packets through fragmentation and assemble by the IEEE 802.15.4 link layer.

For efficient IPv6 header compression, IPHC removes safely IPv6 header fields that are implicitly known to all nodes in the 6LoWPAN network: Version is 6; Traffic Class and Flow Label are both zero; Payload Length is inferred from the 802.15.4 header; Hop Limit is set to a well-known value; addresses are formed using a single prefix and 802.15.4 addresses.

0	1	2	3 4	5	6 7	8	9	10 11	12	13 14	15
0	1	1	TF	NH	HL	CID	SAC	SAM	M	DAC	DAM

Fig. 2. LOWPAN_IPHC encoding for IP header compression.

SAC: Source Address Compression
TF: Traffic Class
NH: Next Header
SAM: Source Address Mode
M: Multicast Compression
DAC: Destination Address Compression
DAM: Destination Address Mode

The IPHC has a length of 2 byte of which 13 bit is used for header compression as shown in Figure .2. Uncompressed IPv6 header fields follow directly the IPHC encoding within the same order as they would appear within the traditional IPv6 header.The general format of NHC is shown in below figure. 3. Next header compression has number of octets; where the first variable length bit identifies the next header type and the remaining bits are used for encoding the header information.

VARIABLE LENGTH	COMPRESSED NH

Fig. 3. LOWPAN_NHC for next header compression format.

B. 6lowpan /IPSec Extension Encoding Format

The 6LoWPAN defines the general format of NHC which will be used to encode ip next header. We characterize NHC encodings for the two IP expansion headers to be namely AH and ESP. 6LoWPAN already defines NHC encodings for IP expansion headers that can be utilized to link ESP and AH extension headers. NHC encodings for the IPv6 Extension Headers comprise of a NHC octet where three (bits 4, 5, and 6) are utilized to encode the IPv6 Extension Header ID (EID). The ID bits in the offered NHC for AH and ESP identify that the current header is AH or ESP. The NHC_EH encoding extension headers is appeared in Figure 4.

BIT	0	1	2	3	4 5 6	7
	1	1	1	0	EID	NH

Fig. 4. LOWPAN_NHC_EH header format.

IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified
Vol. 6, Issue 6, June 2017

EID: Extension Header
NH: Next Header

1) LoWPAN NHC_AH Encoding;

AH provide security against replay attacks, data origin authentication for IP datagram's, as well as connectionless integrity. Authentication Header uses a keyed message integrity code for protecting the complete IP packet including IP header, AH and IP payload.

BIT	0	1	2	3	4	5	6	7
	1	1	0	1	PL	SPI	SN	NH

Fig 5. LOWPAN_NHC_AH encoding format.

PL: Payload Length
SPI: Security Parameter index
SN: Sequence Number
NH: Next Header

The first four bits in the NHC AH represent the NHC ID we define for AH. These are set to 1101.

- If PL = 0: The length of the IPSec header field in Authentication headers avoided. This length can be obtained from the Security Parameter Index value because the length of the authenticating data depends on the algorithm used and are fixed for any input size.If PL = 1: The payload value is carried after the NHC_AH header.
- If SPI = 0: SPI 0 is reserved to point that no security association exists. This doesn't mean that all nodes use an equivalent security association, however that each node has a single preferred Security Association, identified by SPI 1.If SPI = 1: All 32 bits showing the security Parameter Index are carried after the Next Header C compression AH header.
- If SN = 0: A 16 bit sequence number is employed. The left most sixteen bits are assumed to be zero. If SN = 1: All 32 bits of the sequence number are carried after the NHC AH header.
- If NH = 0: the next header field in Authentication Header is going to be used to specify the next header, If NH = 1: The next header field in Authentication Header is avoided. The next header will be encoded using Next Header Compression.

2) LOWPAN_NHC_ESP Encoding;

Encapsulating Security Payload gives authentication, data integrity, and confidentiality protection of IP packets. ESP operates on the IP payload, not on the header. ESP has common fields with authentication header and contains the encrypted payload as well as padding required for block ciphers. ESP only encrypts payload data, pad length, padding, and the next header; if ICV calculation is selected, it includes all header fields in the ESP.

BIT	0	1	2	3	4	5	6	7
	1	1	1	0	-	SPI	SN	NH

Fig. 6. LOWPAN_NHC_ESP encoding.

SPI: security parameter index
SN: sequence number
NH: Next header

The first 4 bits in the NHC ESP represent the NHC ID we define for ESP. These are set to 1110.

- If SPI = 0: The default SPI for the sensor network is used and the SPI field is avoided. We set the default SPI value to zero. If SPI = 1: All thirty two bits indicating the Security Parameter Index are carried inline after the Next header compression ESP header.
- If SN = 0: A 16 bit sequence number is employed. The left most sixteen bits are assumed to be zero.If SN = 1: All 32 bits of the sequence number are carried after the Next Header Compression ESP header.
- If NH = 0:The next header field in ESP will be used to specify the next header and it's carried inline. If NH = 1: The next header field in ESP is skipped. The next header will be encoded using NHC.

IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified
Vol. 6, Issue 6, June 2017

C. IPv6

The Internet of Things and Smart Objects all kind of physical devices such as wireless sensors are expected to be connected to the Internet via IPv6, a new version of the Internet Protocol that increases the address size from 32bit to 128bit.IPv6 provides a highly scalable address scheme mechanism. It provides 2^128 unique addresses. These addresses are sufficient for present and future communicating devices.

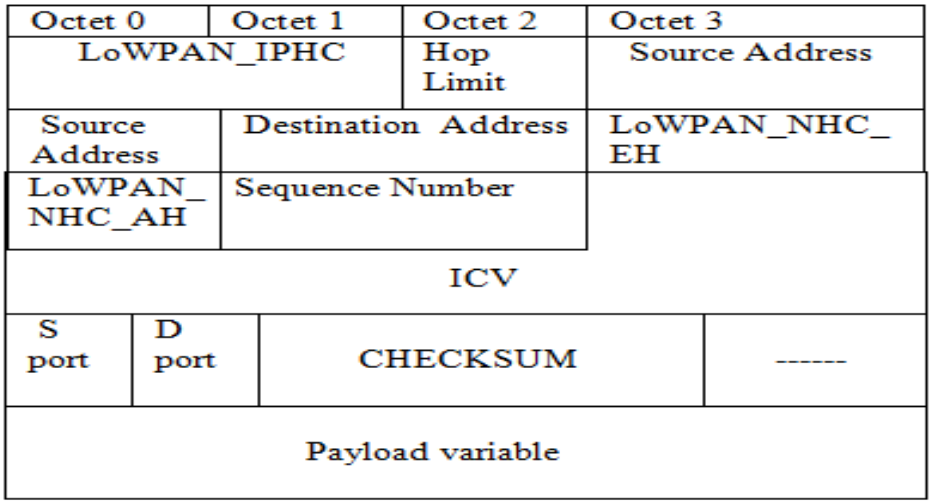

Fig.7. IPv6 packet format

IPv6 decreases the size of routing tables and make it more efficient and hierarchical. IPv6 allows ISPs to aggregate the prefixes of customer's networks into a single prefix and announce this as a one prefix to the IPv6 Internet. In IPv6 networks, fragmentation is handled by the source device, employing a protocol for locating the path's maximum transmission unit (MTU).

D. Proposed System

The proposed method consists of amalgamation of software and hardware. Where software part will be created using Matlab and hardware implantation will be done by using ARM 7 and Zigbee module .The data transmission and reception is done by using Zigbee.

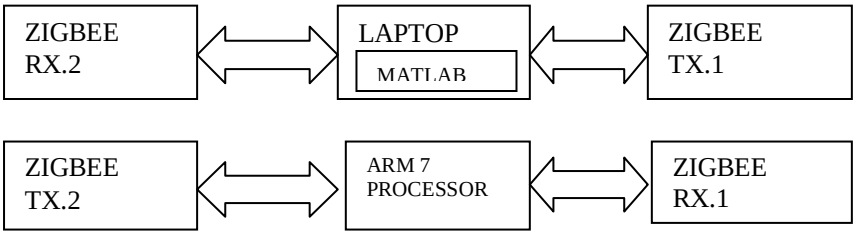

Fig. 8. Block diagram

The packets creation will be undertaken by using Matlab, and we use AES algorithm for packet encryption and decryption. An encrypted data in packet payload for authentication purpose. A packet is consisting of source address and destination address. In our system, we are using two pairs of Zigbee, one for transmitting a packet and one for receiving a packet, a Zigbee transmitter and receiver pair created by their MSB and LSB Bits respectively. The Zigbee Receiver then send these packets to ARM 7, then ARM 7 will do the decryption of packets based on their destination addresses. The packets that fail to match the destination address will be discarded from the system. The once that will match up to the correct address and hence fully authenticated packets will be passed to the second Zigbee paired setup that will retransmit the secure packet to our device and the device will compute the results on basis of graph simulation that will give us the better result packet performance when passed through IPSec.

E. Experimental Setup

Below figure.8 shows experimental setup of our proposed system. It consist of LPC2138 processor, zigbee module, power supply and computer. A LPC2138 processor interface with LCD. We are using four zigbee modules, two for transmitter and two for receiver.

IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified
Vol. 6, Issue 6, June 2017

Fig. 9. Experimental setup of proposed system.

One transmitter and receiver pair is connected processor PCB board and another one pair is connected to computer.in power supply section,we used stepdown transformer to step down 12 volt to 3.3 volt or 5 volt.

V. SIMULATION AND ANALYSIS

A simulation result of our proposed system is shown in below figure. When IPv6 packet are travel through the network, average responses time is increases with number of hops is increases.

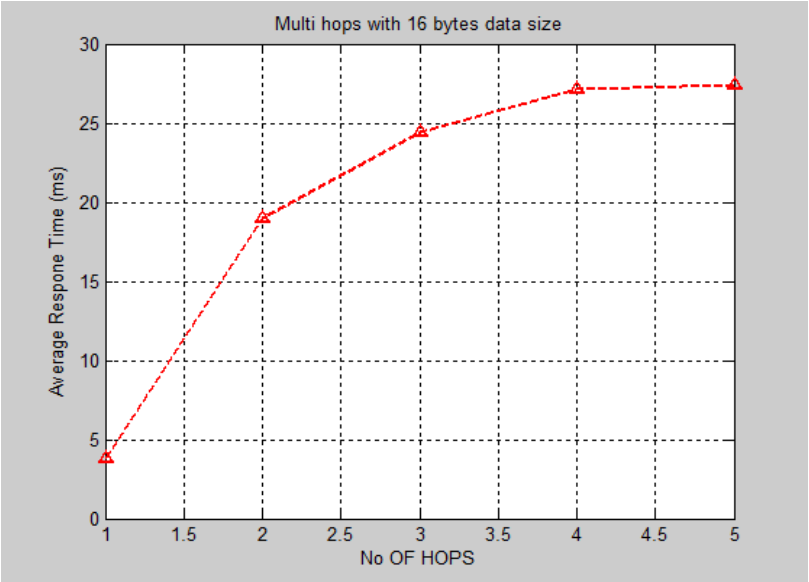

Fig. 10. Graphical representation of average response times vs. No. of hops

When number of packets is transmitted in the network, packet error rate constant and response time is increases. Our proposed system gives a constant error rate of packet even response time of packet is increases.

When number of hops of IPv6 packet is increases then packet error rate is decreases. Our proposed system provides decreased response of packet error rate.

IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified
Vol. 6, Issue 6, June 2017

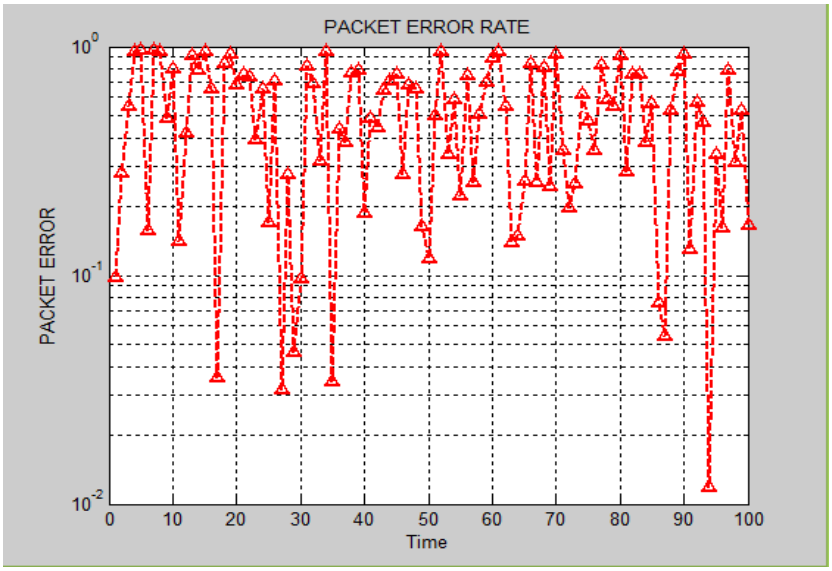

Fig. 11. Graphical representation of packet error rate vs time

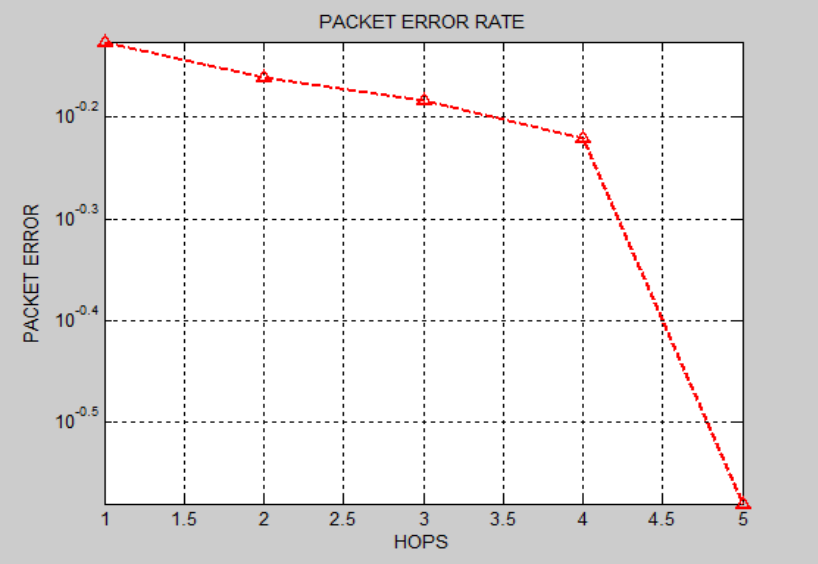

Fig. 12. Graphical representation of packet error rate vs. No. of hops.

VI. CONCLUSION

The earlier technology had compatibility with device communication but it was adequate for substantial performance. In spite this there are certain difficulties that we come across. Especially in Packet data transfer gets affected in when network traffic, isolated network. For example delay in packet delivery, no authentication etc. All this issues can be overtaken by IPsec over 6LoWpan. Besides increased address space, IPv6, as compared to IPv4, also provides a simplified header format, better support for extensions and mandates IP security.

In this paper, we are using IPsec protocol in network. This can authenticate and encrypt the packets of data sent over network. We used AES algorithm for encryption and decryption of the data so attacker cannot modify the packet data. If attacker wants the information in the packet, this packet is discarded by using Zigbee receiver which is connected to ARM 7 processor. Because we provide encryption and decryption keys to transmitter and receiver packet respectively.

In this paper, we have shown that IPsec implemented through 6LoWPAN extensions is a feasible option for providing End to End security in the Internet of Things.

REFERENCES

[1] Granjal J, Monteiro E, Sá Silva J. Enabling network layer security on IPv6 wireless sensor networks. In Proceedings of IEEE Global Communications Conference (GLOBECOM'10), Miami, USA, 2010.

[2] Kent S, Seo K. Security Architecture for the Internet Protocol. RFC 4301, 2005.
[3] Granjal J, Silva R, Monteiro E, Sa Silva J, Boavida F. Why is IPsec a viable option for wireless sensor networks. In Proceedings of 4th IEEE International Workshop on Wireless and Sensor Networks Security(WSNS'08), Atlanta, USA, 2008.
[4] Riaz R, Kim K-H, Ahmed HF. Security analysis survey and framework design for IP connected LoWPANs. In Proceedings of 9th Internationa Symposium on Autonomous Decentralized Systems (ISADS'09), Athens, Greece, 2009.
[5] Roman R, Lopez J. Integrating wireless sensor networks and the internet: a security analysis. Internet Research 2009; 19(2): 246–259.
[6] Deloche G, Kushalnagar N, Hui J, Culler D. Transmission of IPv6 Packets over IEEE 802.15.4 Networks. RFC 4944, 2007.
[7] Alcaraz C, Najera P, Lopez J, Roman R. Wireless sensor networks and the Internet of Things: do we need a complete integration? In Proceedings of 1st International Workshop on the Security of the Internet of Things (SecIoT'10), Tokyo, Japan, 2010. Proceedings of 1st International Workshop on the Security of the Internet of Things (SecIoT'10), Tokyo, Japan, 2010.
[8] Liu A, Ning P. TinyECC: a configurable library for elliptic curve cryptography in wireless sensor networks. In Proceedings of 7th International Conferenc on Information Processing in Sensor Networks (IPSN'08), Washington, DC, USA, 2008.
[9] Szczechowiak P, Oliveira L, Scott M, Collier M, Dahab R. NanoECC: testing the limits of elliptic curve cryptography in sensor networks. In Proceedings of 5th European Conference on Wireless Sensor Networks (EWSN'08),Bologna,Italy,2008.
[10] Wood A, Stankovic J. Poster abstract: AMSecure- secure link-layer communication in TinyOS for IEEE 802.15.4-based wireless sensor networks. In Proceedings of 4th ACM Conference on Networked Embedded Sensor Systems (SenSys'06), Boulder,USA,2006.
[11] Hu W, Corke P, Shih W, Overs L. secfleck: a public key technology platform for wireless sensor networks.In Proceedings of 6th European Conference on Wireless Sensor Networks (EWSN'09), Cork, Ireland, 2009.
[12] Liu D, Ning P. Establishing pairwise keys in distributed sensor networks. In Proceedings of 10th ACM Conference on Computer and Communications Security (CCS), New York,NY,USA,2003.
[13] Chung A, Roedig U. DHB-KEY: an efficient key distribution scheme for wireless sensor networks. In Proceedings of 4th IEEE International Workshop on Wireless and Sensor Networks Security (WSNS'08),Atlanta,USA,2008.

BIOGRAPHIES

Ms. Aishwarya Akul, currently studying M.E in VLSI and Embedded system at RMD Sinhgad School of Engg, Pune. The author has her personal filed of interest in the domain of wireless sensor network, VLSI, Embedded system and Internet of Things.

Prof. Mrs. Snehal Bhosale, currently heading Department of E&TC at RMD Sinhgad School of Engg, Pune. Her main research interests are computer networks, network security and wireless sensor networks. She is currently doing her research on security in IoT in Pune University.