SECURE 6LOWPAN NETWORKS FOR E-HEALTHCARE MONITORING APPLICATIONS

DHANANJAY SINGH
Department of Electronics Engineering
Hankuk (Korea) University of Foreign Studies, Yongin (Global Campus), South Korea
E-mail: dan.usn@ieee.org

ABSTRACT

Nowadays embedded computing has tremendous usage into the development of smart environment services such as smart city, smart home, intelligent transportation, e-healthcare monitoring and many more services. Owing to increase in use of these services by companies, several security issues have emerged and this challenges embedded computing framework to secure, protect and process user's data. These services have certain cons like security, lock-in, lack of control, and reliability. Privacy and security are the major concerns in embedded computing services. In this paper, we have designed a novel secure framework for 6lowpan (IPv6 over Low Power Wireless Personal Area Networks) networks, as well as presented a critical analysis of CCMP (Counter with Cipher Block Message Authentication Code Protocol) protocol for secure data management of e-Healthcare monitoring applications.

Keywords: *Wireless Sensor Networks (WSN), 6lowpan, embedded system, healthcare system, secure networks*

1. INTRODUCTION

IETF 6lowpan [1] is the Internet-based computing where the application data, IPv6 communications are merged into the stack of TCP/IP's Data link (adaptation layer). The end users can globally access it through a distributed networking, as a client. 6lowpan is a step on from utility computing and provides a convenient on demand global network access to a shared pool of configurable computing and communication services [2]. Here, services refer to computing healthcare applications and IPv6 based global communication network infrastructure. 6lowpan computing is being widely adopted across many industrial sectors. Security, availability, and performance are the three biggest problems in 6lowpan network adoption. The serious challenge is how it reports security and privacy issues which occur due to movement of data and application on networks, loss of control on data, dissimilar nature of resources, and several security policies [3]. Data storage, processing and movement outside the controls of an organization poses an inherent risk and making it vulnerable to various possible attacks. 6lowpan computing poses privacy concerns because the global healthcare service providers may access of biomedical data that is on wearable devices at patient's body area networks. Hence, various security concerns protocol have been introducing, namely: data security, data confidentiality, and compliance with government regulations, trust, identity management, architecture, software isolation and availability. Irrespective of employing framework having attributes for high reliability and availability for the healthcare services into the 6lowpan scenario.

The security concern AES (Advanced Encryption Standard) [4] is a candidate algorithm, since it is a very tough and non-breakable cipher by several attacks. According to the NIST [4] specification, AES involves various rounds of length 10, 12 and 14 in the encryption process, as more rounds are involved in the transformation and the overall encryption strength increases. AES-CCMP [5] protects AAD (additional authenticated data) against replay attacks. The AAD is derived from the MAC Protocol Data Unit (MPDU) header. It is 22–30 bytes in size. It is made from frame control, IP address of source, IP address of destination, MAC address of source and quality control [6]. Generally, the security is a joint responsibility of the patient services and Doctor. However, 6lowpan computing offers many benefits, for instance, low cost, data security and privacy issues pose serious concerns to this relationship between patients' and

Doctor for global healthcare monitoring scenario. This paper presents a novel secure 6lowpan framework for the improvements of authentication and access control between patient's services and Doctor.

The remaining of the paper is organized as follows. The section 2 presents a brief discussion of wearable devices for biomedical data collection from patient's body area networks. The section 3 presents a secure cross layer based 6lowpan stack for global healthcare monitoring services. Section 4 presents 6lowpan networks algorithm to successfully transfer biomedical data from patient's BAN to 6lowpan gateway in a SHA scenario. Section 5 presents security mechanism for data communication between 6lowpan networks. Section 6 presents the performance analysis of mobility enabled 6lowpan devices and analysis of CCMP protocol with different-2 mode and finally, we have concluded the paper in section 7.

2. WEARABLE DEVICES FOR BODY AREA NETWORKS

Healthcare wearable is a fusion of sensors and IEEE 802.15.4 [7] embedded computing which is 6lowpan and various biomedical sensor devices shown in Fig. 1. Biomedical sensors are occurring simultaneously medical data on 6lowpan devices. There are a specific gateway which is associated with 6lowpan networks. 6lowpan networks have tight coupling between biomedical sensors and IPv6 Gateway. Greedy network mechanism has utilized and face lots of challenges for 6lowpan networks.

Major Challenges:

- Balancing between biomedical sensors in BAN (Body Area Networks).
- Safely transmit biomedical data to the gateway during patient's movement.
- Optimization of energy latency in QoS.

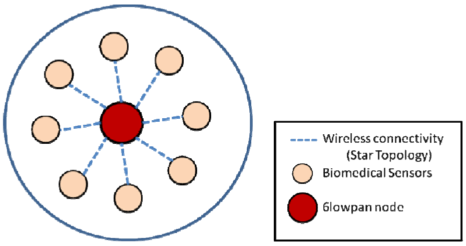

Fig. 1. Healthcare Wearable For BAN.

6lowpan device is associated with several biomedical sensors which has sensing and transmitting capability to enables a certain task in a specific time period. The 6lowpan device transmits biomedical data to the Doctor's mobile phone through the gateway. Gateway initiates the resource solicitation on behalf of an application with the help of address centric routing mechanism. The biomedical data packet used subsequence frame techniques over routing protocol. Hence, with the help of following approaches, we can overcome BAN challenges.

Solutions:

- The 6lopwan device has to choose an active 6lowpan device in a mesh network to successfully transmit its biomedical data to gateway.
- Gateway can measure by localization and transmit distance information (by modified gateway packet) of mobile 6lowpan which is helping to choose the right path.
- Gateway broadcast RREQ message to 6lowpan devices which is using one or two hop. When 6lowpan device transmits its biomedical data packet, then hop (mediator) device should be ignored for sensing activities and use routing to successfully transmit biomedical data to the gateway.

Hence, the biomedical sensors retrieve the personal health data such as ECG, glucose, or fitness related data from patient BAN and transmit it to the gateway operate by the consecutive forwarder over IPv6. IEEE 802.15.4 devices are characterized by short range, low bit rate, low power, and low cost. Many of the devices employing IEEE 802.15.4 radios will be limited in their computational power, memory, and/or energy availability. 6lowpan provides the wireless sensor network (WSN) node with IP communication capabilities by putting an adaptation layer above the 802.15.4 link layer. Different mechanisms performed by adaptation layer require the 6lowpan header encapsulation in the packet for the packet fragmentation and reassembly purpose. Hence, this technique uses high network utilization so security and privacy issues occurs during the communication between 6lowpan devices for biomedical data transfer to the gateway. Hence, the encryption mechanism need over the 6lowpan devices where data must be encrypted during communication between patient's (client) and Doctor (smart phone). We already know that CCM/CCMP [4] is an amalgamation of two modes, the AES Counter Mode and the Cipher Block Chain MAC (CBC-MAC) [8] mode to provide encryption both side 6lowpan and Smart phone. This view approximates 6lowpan device to the so-called secure Internet of networks.

3. 6LOWPAN COMPUTING STACK

The IETF 6lowpan stack based on IEEE 802.15.4, which improves the routability of gateway-assisted 6lowpan networks. More detailed description of 6lowpan stack and IPv6 compression techniques have presented in RFC 4919 [1] and RFC 4944 [2]. In the 6lowpan stack, compressed IPv6 merged into data link layer as adaptation layer into the TCP/IP stack. The 6lowpan device allows communication between neighboring 6lowpan devices in the same environment by diffusing each other in inter-PAN networks. The 6lowpan devices are focused on the efforts of routing metric issues, biomedical data binding, common channel-mechanism, encryption and gateway-assisted routing mechanism.

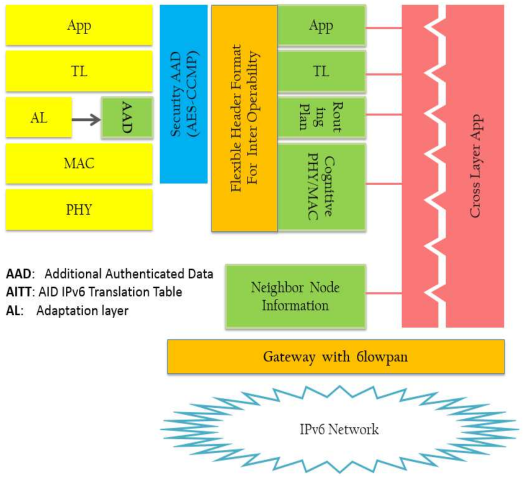

Fig. 2 Secure 6lowpan Protocol Stack.

The designed 6lowpan stack based on cross layer mechanism for conventional routing has showed in Fig.2. MAC layer in to the proposed 6lowpan stack several frame which is beacon frame, data frame, acknowledgement frame and MAC command frame. A beacon frame is used by a 6lowpan gateway to transmit beacons while a medical data frame is used for medical data transfers. For the acknowledgement frame and the MAC command frame, they are used for confirming successful frame reception and handling all MAC peer entity control transfers respectively. Except ack. frame which do not have MAC Service Data Unit (MSDU), other frames have the MSDU which is prefixed with a MAC Header (MHR) and appended with a MAC Footer (MFR).

Frame Hdr	Dispatch Hdr	Hdr Comp 1	IPv6 Hdr compression	UDP Hdr	Medical Data (Healthcare services)

Fig. 3. 6lowpan peer-to-peer communication.

The 6lowpan stack enabled devices have to work in WPAN environment. The proposed cross layer stack focuses on the data link layer as an adaptation layer, based on the standard of IEEE802.15.4 and IETF 6lowpan compression techniques. The compressed IPv6 packets must carry on data frame for real–time 6lowpan peer-to-peer medical data packets communication and acknowledgement frame structure shown in Fig.3.The range of transmission unit in any IPv6 packet is 1280 Octets [2]. Hence, very strong compression algorithm has used to compress IPv6 for IEEE 802.15.4. After the implementation of all header protocols, there are few bytes left for actual usage of the medical data services. To overcome this problem of seamless integration of MAC layer and IPv6 compression techniques have proposed to achieve the header compression, fragmentation and layer-two forwarding [13].

The communication between 6lowpan devices and IP networks have followed several advantages which can be extended to global healthcare monitoring services.

- The combination of 6lowpan with IP based infrastructure can easily be implemented.
- Traditional IP based technologies have been proven and is in use.
- 6lowpan over IP will be more readily available as compared to some proprietary solutions.
- Diagnostics tools, management can easily be extended over 6lowpan networks.
- Seamless integration of IP already exists and can thus focus shall be more on making 6lowpan more efficient and optimized.

Thus, the global healthcare monitoring scenario can be easily suitable target for usage for 6lowpan networks. Hence, Global healthcare monitoring parameter-related information can be carried in the adaptation layer, required by and defined in the 6lowpan stack in Fig. 2.

4. 6LOWPAN NETWORKS FOR SHA

The hospital area has considered for the test-bed of Global communication. The design space is already limited by the unique characteristics of a Lowpan (low-power, short range, low-bit rate). In this scenario, the 6lowpan device has deployed in an organized (manually or automatically), pre-planned manner to create a Smart Hospital Area (SHA). The deployment has an impact on high-node density for location to allocate addresses in the networks. The five 6lowpan devices have used to provide the intended network capability, which is supporting mobility within the range of 6lowpan gateway. However the power source of devices needs to be hybrid; whether the devices are battery-powered or mains-powered, it influences the network design. The system has considered that all 6lowpan devices are wirelessly connect to the 6lowpan gateway (Internet based gateway).

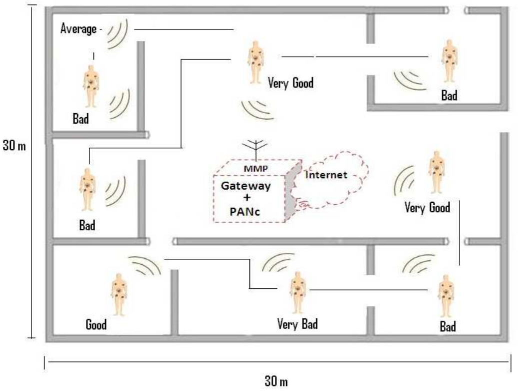

Figure 4. Smart Hospital Area Networks.

Fig.4 depicts a heterogeneous network; it consists of five main parts, biomedical sensors, 6lowpan devices (compressed IPv6 over Lowpan), body area networks, 6lowpan gateway and IP-Based device (Doctor's smart phone). Biomedical sensors senses data and transmits to its associated 6lowpan device, which has limited battery and fixed transmission range. The biomedical sensors does not perform any relaying function or aggregation due to limited constraint. The 6lowpan coordinates the MAC (Medium Access Control) schedule to avoid retransmission within the 6lowpan networks due to collision and aggregates biomedical data to avoid all redundant data received from biomedical sensor devices. There major characteristics of 6lowpan device for SHA networks to support global connectivity.

- 6lowpan device has to fix patient's BAN.
- 6lowpan device has compressed 6lowpan stack for global connectivity.
- 6lowpan device has more energy than biomedical sensors.
- 6lowpan device can calculate their location from gateway.
- Each 6lowpan device has its own IP-address for global connectivity.
- 6lowpan device has more calculation power and data aggregation capacity for data compression to avoid the redundant data in a PAN.
- 6lowpan device has no collision between inter- and intra-IP-WBSN.
- 6lowpan device has capability to adjust the transmission power to do single hop broadcast that's decided by gateway.
- If 6lowpan device is near to gateway, then the level is high; if far, then the level is low and biomedical data flow is always from a higher level to a lower level.

The SHA scenario provides functions to prevent/monitor patient's biomedical data from anywhere. There are very strong 6lowpan network scenario. The proposed algorithm can support sustainable and permanent services like computing, amateur radio, aviation communication between 6lowpan device and 6lowpan gateway.

<u>Algorithm:</u>

6lowpan Detour Routing Procedure in SHA

```
Generate Test Message
  //Bootstrapping
  For All 6lowpan Devices
      Set pheromone 0
  End For
//One-hop broadcast of a test message in the air
  Advertise pheromone
  Update Neighbor Node list
//Routing decision process
6lowpan DetourRouting
  If queue>0 then
    If (Neighbor 6lowpan list for Destination) then
      Forwarding 6lowpan
      = Get Highest Pheromone (Neighbor Node list)
    Else
      Forwarding 6lowpan = Random(Neighbor 6lowpan)
    End If
    Send a packet to Forwarding 6lowpan Devices
    delta =1
  Else
    delta = 0
  End If
  // Pheromone update
  Result = Compute_pheromone (6lowpan Devices)
  Set pheromone Result
```

Reliability and availability are the strong points to measure any technology. The reliability denotes how regularly resources are available without trouble (loss of data, code reset during execution) and how commonly they fail. One of the important aspect that creates serious problems for the reliability of 6lowpan network is down time. To understand routing performance in a 6lowpan networks, we assess three routing strategies: 6lowpan-touring, random-touring, and 6lowpan-detouring. By using only local information similarly to for each strategy, we set the probability that node i chooses node j as a forwarding node among m neighbors as follows:

- 6lowpan-touring: $$\Pi_{i->j} = \frac{g_j^1}{\sum_m g_j^1}, \quad (1)$$
- Random-touring: $$\Pi_{i->j} = \frac{g_j^0}{\sum_m g_j^0}, \quad (2)$$
- 6lowpan-detouring: $$\Pi_{i->j} = \frac{g_j^{-1}}{\sum_m g_j^{-1}}, \quad (3)$$

Where g is the degree of node (number of one-hop neighbors) [9].

The proposed cross layer based 6lowpan stack has been needed to provide data privacy and security. Role-based access control needs to be supported by proper authentication mechanism and needs to include encryption mechanism. The data collection techniques are used point to point, multipoint to point, and point to multipoint for traffic. It has plug-and-play configuration during mobility and real-time data acquisition. 6lowpan device uses global unique IPv6 address for Global connectivity and unique identification of the patient's biomedical data.

The SHA itself does not require globally unique IPv6 address but could be run with link-local IPv6 address. The security is used between 6lowpan networks and 6lowpan gateway for reliable and secure data communication. The SHA networks have several challenges to the use of global connectivity. We have proposed several solutions. The doctor sends a query request to the 6lowpan gateway, and then gateway broadcasts query packet to all 6lowpan devices and then match 6lowpan device is associated with the 6lowpan gateway. The query packets carries patient's IP-address, query data, and signal strength of level 1 with gateway's level 0. After query request is received from 6lopwan gateway, the 6lowpan set their transmission power and reply to 6lowpan gateway with its carry current position. Once biomedical date is received from 6lopwan device, 6lowpan gateway can analyze energy consumption of all 6lowpan devices.

5. PRIVACY AND SECURITY CONCERN FOR 6LOWPAN NETWORKS

Privacy and security is a major area of concern when talking about mobility compliance of 6lowpan devices. Mobility management can have disguised identity and can fake the real identity of the 6lowpan devices. With the help of following challenges, we can consider to develop novel security protocol.

- Integration of all the heterogeneous device integration to a common platform. IPv6 is a huge factor in addressing the scalability and mobility issues of 6lowpan devices.
- Privacy and integrity of 6lowpan device enabled services and IP based smart phone.
- 6lowpan devices must perform all their operations while fulfilling the mobility of the 6lowpan device. The present world is witnessing a surge in smart phones, tablets which have a ubiquitous nature in management of the devices. The real world is full of mobile applications and thus it becomes important for 6lowpan enabled devices to have mobility in their implementation background.

Hence, 6lowpan needs a dynamic and flexible security solution so that biomedical data can be updated easily and is in sync with the security protocols. The 6lowpan networks provide us global connectivity heterogeneous 6lowpan devices. The mobility of 6lowpan networks has created security concern for healthcare services because security is compromised and create inconsistencies from biomedical data collected from different-different patient's (6lowpan devices). There are no central control that can provide viable centralized solution for compromise the healthcare security. A secure communication channel is needed for the interacting with other 6lowpan devices and smart phone (Doctor's). Biomedical data sharing with unsecured 6lowpan networks increase the probability of the risk for SHA. The privacy is very important for healthcare services to be safeguarded. There are several security concerns character for SHA.

- **Confidentiality of Messages**: End to End security of messages exchanged between the 6lowpan devices is required. Some sort of encryption and decryption algorithm must be provided to have the safe travels of data across the Internet.

- **Message Data Integrity**: Data must never be modified between patients and Doctor.
- **Message Source Authentication**: The different sources must be able to identify themselves via some authentication protocols.
- **Message Availability**: Intrusions and malicious behavior must be detected in the system. Various types of Intrusion Detection System could be employed to the security concerns of the system.
- **Message Replay Protection**: The security also needs to be taken care at all the intermediary nodes. There must be strict mechanisms to detect all the duplicate messages as well as replaying of the biomedical data with the help of sequence numbers or time stamping at the 6lowpan network layer.

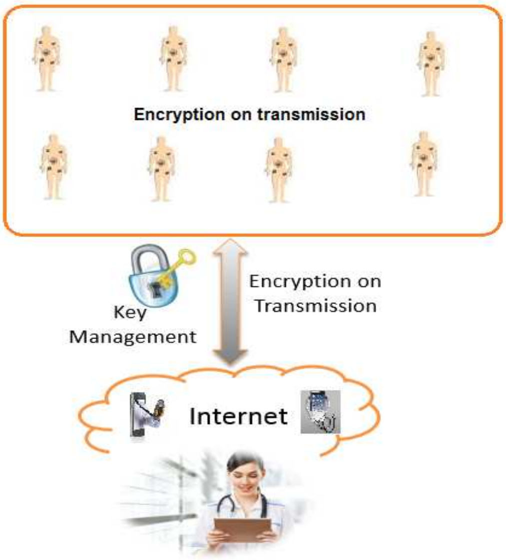

Figure 5. Encryption On 6lowpan Devices.

Thus we need to focus on security concerns mechanism between 6lowpan device networks and gateway to Doctor's smartphone connectivity. 6lowpan stack use the IEEE 802.15.4 protocol as link layer so link-layer security is the present security solution for the Healthcare services. In the link layer communication process needs to be trusted between 6lowpan devices. The communication can use multiple numbers of 6lowpan devices with multiple hops to communicate with 6lowpan gateway. Security key is defined prior to the communication to protect all the respective communication happening in the communication cycle. If this key is compromised, then the security of the whole layer is compromised. Hence the per-hop security arrangement can detect unwanted modification at each of the respective hops. Biomedical data integrity must be provided at the per hop security arrangements with the 6lowpan networks. Link layer security is limited to secure the communication between two neighboring 6lowpan devices. This is one of the flexible options which can be used with multiple protocols at the layers above to the link layers.

Table 1. Secure Features For 6lowpan Devices.

Input	Reason
Increased the vulnerability SHA	More increase in the open networks. Increase of cloud based system, internet expansion, and increase in USB devices, Bluetooth, 6lopwan devices.
Dwindling support for legacy systems	Software updates, patches for security where network support is dwindling. Thus, they become a soft target for malware attacks.
Increased the Non Identifiable, unauthorized services	Unique identification schemes must be devised for millions of devices.
Unauthorized Remote access facilities	Remote access can open doors for interception and tampering.
Exposed biomedical data sensitive	Smart patient data, critical data can be exposed which can lead to catastrophe.
Increased dependence on the software and embedded systems	Majority of targets for malware application is the application layer.

Table 1 shown, security characteristics that can be utilized for secure networks. Encryption mechanism has considered into SHA, where biomedical data must be encrypted during communication between 6lowpan devices and connectivity with the 6lowpan gateway. Therefore, proxies can be used to represent simple networked objects that do not support such functionalities.

This paper has considered Counter Mode encryption mechanism to guarantee biomedical data confidentiality. Rogaway and Wagner [10] has presented that every MPDU encryption, CCMP generates an additional 8 bytes CCMP header. The CCMP header is made of 48 bits nonce PN, 8 bits Key ID, and 8 bits ext IV. CCMP also generates 30 bytes AAD from the MPDU header. In the SHA scenario where patient's (6lowpan) to 6lopwan gateway networking is required, the encryption key K lasts for a whole data communication session. Every session, a new encryption key requires a unique 13 bytes nonce value N for each MAC Protocol Data Unit (MPDU) encrypted. The nonce N ensures that the lifetime of encryption keys K are longer and that any replay attacks are detected and thwarted. N is constructed from the 48 bits packet number (PN), the 48 bits destination IP address (A2), and the 8 bits priority [5].

6. PERFORMANCE ANALYSIS

We analysis the secure routing performance between 6lowpan devices with respect to topology alternating cycle. As the alternating time is shorter and shorter, the performance gap becomes smaller and smaller. In a rapidly dynamic topology, 6lowpan device frequently change and thus, the portion of 6lowpan device's roles diminishes.

Having established the desirability of an AE scheme like CCM/CCMP to be AEAD, the next step is to show how much efficiency is lost by CCM/CCMP for failing to pre-process the AAD. An MPDU varies in size between 1 to 2296 bytes. The number of MPDUs in any given payload greater than 2296 bytes ($M_P \geq$ 2296) hereby referred to as MPDU_N is computed as shown in Equation (1).

$$\mathrm{MPDU}_N = \left\lceil \frac{M_p}{2296} \right\rceil \qquad (1)$$

We already know that the AAD is 30 bytes. This means for every 2296 bytes of payload that goes through the CCM originator processing, some excess data of at least 30 bytes has to be recalculated by the CCM/CCMP authenticated encryption process.

An MPDU may however be far less than the 2296 bytes. Regardless, the problem of CCMP not being able to pre-process AAD will still manifest itself as 30 bytes of AAD has to be generated for every MPDU encrypted. For any given size of plaintext payload $\geq$ 2296 bytes encrypted, the minimum amount of excess AAD hereby referred to as AAD_{Min} is computed in equation (2).

$$\mathrm{AAD}_{Min} = \left\lceil \frac{M_P}{2296} + 1 \right\rceil * 30 \text{ bytes} \qquad (2)$$

Equipped with the minimum amount of excess AAD generated from any payload $\geq$ 2296 bytes, a table and graph is produced, which shows how much efficiency is lost by CCM/CCMP for having to re-compute this surplus AAD. Equation (3) shows the computation for plaintext payload with excess AAD hereby referred to as $P_{+\mathrm{AAD}}$.

$$P_{+\mathrm{AAD}} = M_p + \left(\left\lceil \frac{M_p}{2296} + 1 \right\rceil * 30 \text{ bytes} \right) \qquad (3)$$

Table 2. CCMP Nonce Complexity Compared To Other AEAD Modes.

Mode	Scheme	Nonce	Other Nonce in bytes
CCMP	AE	48 bits (PN)	N =13,
CBC-HMAC	AEAD	128 bits IV	iNonce, oNonce
CWC	AEAD	88 bits IV	None
OCB	AEAD	128 bits IV	None
GCM	AEAD	Variable	None
ESKIMO	AEAD	128 bits IV	None

The hallmark of a good cryptographic security scheme is having a simple clean design with fewer parameters. With fewer mathematical operations to be carried out on fewer parameters, this makes efficiency attainable in both software and hardware implementations. A single extra parameter added to the algorithm of a security scheme could in the long run cost millions of pounds in additional cost of ASICS in hardware implementation. Table 2 shows summary of CCMP nonce complexity compared to other AEAD modes like the CBC-HMAC, CWC, OCB, GCM and ESKIMO. Hence, CCMP recorded 11 p-values and 5 p-values in the fail zones, while CBC-HMAC recorded 12 p-values in both fail zones [11].

We interpret that mobility or unstable link quality, which contributes to changing an intrinsic network topology, minimizes dependencies of specific 6lowpan device. Even though we examine this interpretation, we observe that 6lowpan-detouring maintains the best performance among the strategies. Conclusively, it is beneficial to accommodate a 6lowpane-detouring strategy to fully utilize available network resources and to minimize undesirable impact of a specific 6lowpan device to an entire network 6lowpan devices. Along with load balancing capability of 6lowpan-detouring, we review previous works which deal with the vulnerability of 6lowpan device and its impact to an entire network 6lowpan devices. Hence, the 6lowpan network traffic states for different topology alternating cycle [12].

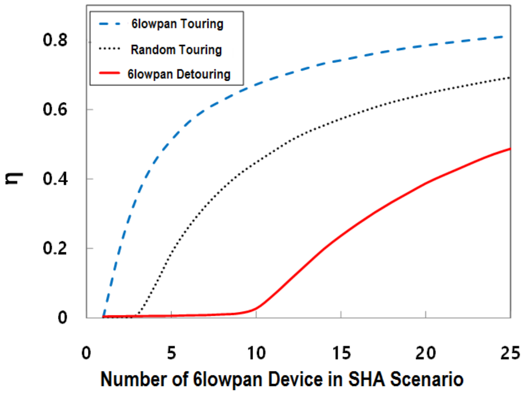

Figure 6. 6lowpan Mobile Networks.

Fig.6 depict 6lowpan network performance for SHA scenario especially in patient's biomedical data communication between 6lowpan devices. Thus, this system would act as an alert to the doctor about his patient's real-time biomedical data. We have considered CCMP security protocol to establish a secure 6lowpan networks where we have included AAD remains constant for the duration of an encryption data delivery session. CCMP should be able to pre-process the AAD just once, at the beginning of the session after the first MPDU is processed. With this, all other subsequent MPDUs that follow will use the same AAD data to maintain efficiency. CCMP however fails to do this. CCMP has to re-process the AAD for every MPDU encrypted. This is because it computes the nonce N before the AAD rather than after it.

Table 3. Summary of CCMP and CBC-HMAC p-values Performances

CCMP	CBC-HMAC	Advantage
11 p-values > 0.95 in fail zone	12 p-values > 0.95 in fail zone	CCMP 33.33%
5 p-values < 0.05 in fail zone	12 p-values < 0.05 in fail zone	
28 p-values in ideal zone	47 p-values in ideal zone	CBC-HMAC 40.42%

In respect to p-values in the important ideal zone, CCMP recorded 28 p-values while CBC-HMAC recorded 47 p-values. The advantage of CBC-HMAC over CCMP is computed as follows: ((47-28)/47)*100% = 40.42%. As summarized in Table 3, shows that the CCMP is not a better PRF than CBC-HMAC, but CBC-HMAC is a better PRF than the CCMP [11].

7. CONCLUSIONS

This paper presents an overview of Smart Hospital Area (SHA) where 6lowpan networks has considered. The 6lowpan networks has investigated in detailed and provide secure 6lowpan networks for SHA scenario. We have developed a secure cross layer based 6lowpan stack for secure global healthcare monitoring services, as well as presented a critical analysis of CCMP (Counter with Cipher Block Message Authentication Code Protocol) protocol for secure biomedical data communication between 6lowpan devices. Finally, we have presented a critical analysis of CCMP protocol with different-2 security mode for secure data communication between 6lowpan networks for SHA scenario.

ACKNOWLEDGEMENT

This work was supported by Hankuk University of Foreign Studies research fund in 2015.

REFRENCES:

[1] N. Kushalnagar, G. Montenegro, and C. Schumacher, "IPv6 over Low-Power Wireless Personal Area Networks (6LoWPAN): Overview, Assumptions, Problem Statement, and Goals", RFC 4919, 12 pages, Aug. 2007.

[2] G. Montenegro, N. Kushalnagar, J. Hui, and D. Culler, "Transmission of IPv6 Packets over IEEE 802.15.4 Networks", RFC 4944, 36 pages, Sep. 2007.

[3] E. Rescorla and N. Modadugu, "Datagram Transport Layer Security Version 1.2," IETF RFC 6347, January 2012, http://www.ietf.org/rfc/rfc6347.txt.

[4] Federal Information Processing Standards Publications (FIPS PUBS) are issued by the National Institute of Standards and Technology (NIST), accessed by 23 may 2015. http://csrc.nist.gov/publications/fips/fips197/fips-197.pdf

[5] Junaid, M., Mufti, M., and Ilyas, M. U. "Vulnerabilities of IEEE 802.11i Wireless LAN CCMP Protocol". Proceedings of World Academy of Science, Engineering and Technology, vol 11, pp 1307-6884, 2006.

[6] Whiting, D., Housley, R., and Ferguson, N. "Counter with CBC-MAC (CCM)", http://csrc.nist.gov/groups/ST/toolkit/BCM/doc

uments/proposedmodes/ccm/ccm.pdf Online accessed by May 6, 2015.

[7] IEEE802.15, online accessed by May 6, 2015.

https://standards.ieee.org/about/get/802/802.15.html

[8] Petrank, E., and Rackoff, C. "CBC-MAC for Real-Time Data Source", *Journal of Cryptology,* vol 13, issue 3, pp 315-338, 2000.

[9] M. Gunes, U. Sorges, and I. Bouazizi, "ARA - the ant-colony based routing algorithm for MANETs," in *Proc. of IWAHN*, 2002.

[10] Bellare, M., and Namprepre, C., "Authenticated Encryption: Relations among notions and analysis of generic composition paradigm". Journal of Cryptology, volume 21, issue 4, pp 469-491, 2007.

[11] I. Ahmed, A. James, D. Singh, "Critical analysis of counter mode with cipher block chain message authentication mode protocol—CCMP", Security and Communication Networks, Volume 7, Issue 2, pages 293–308, February 2014.

[12] S. Jung, D. Singh, D. Kim, "Potential Field Based Routing with IPv6 over Low Power WPAN", ICHIT2011, September 23-25, 2011, Daejeon, Korea, Springer-Verlag Berlin Heidelberg, CCIS vol. 206, pp. 46–53, 2011.

[13] D. Singh, "Mobility and Energy Efficient Mechanism for 6LoWPAN Devices to Support Global Healthcare System", Journal of Theoretical and Applied Information Technology, Vol. 66, No.1, pp. 315 ~ 329, 2014.

[14] D. Singh, "IPv6-WSN: Global Communication Mechanism for Future Internet Services", Advances in Information Sciences and Service Sciences, Vol. 5, No. 10, pp. 832 ~ 839, 2013.

[15] D. Singh, U.S. Tiwary, H-J Lee, W-Y Chung "Global Healthcare Monitoring System using 6lowpan Networks" proc. on 11th International Conference on Advanced Communication Technology (ICACT-2009), , phoenix park Korea, pp.113-117, Feb.2009.