A Hybrid Adaptive Security Framework for IEEE 802.15.4-based Wireless Sensor Networks

Taeshik Shon and Yongsuk Park
Convergence Device Lab, Digital Media & Communications R&D Center, Samsung Electronics
416, Maetan-3dong, Yeongtong-gu, Suwon-City, Gyeonggi-do, 443-742, Korea
[e-mail: {ts.shon, victorious.park}@samsung.com]
*Corresponding author: Yongsuk Park

Received September 19, 2009; revised November 14, 2009; accepted November 27, 2009; published December 31, 2009

Abstract

With the advent of ubiquitous computing society, many advanced technologies have enabled wireless sensor networks which consist of small sensor nodes. However, the sensor nodes have limited computing resources such as small size memory, low battery life, short transmission range, and low computational capabilities. Thus, decreasing energy consumption is one of the most significant issues in wireless sensor networks. In addition, numerous applications for wireless sensor networks are recently spreading to various fields (health-care, surveillance, location tracking, unmanned monitoring, nuclear reactor control, crop harvesting control, u-city, building automation etc.). For many of them, supporting security functionalities is an indispensable feature. Especially in case wireless sensor networks should provide a sufficient variety of security functions, sensor nodes are required to have more powerful performance and more energy demanding features. In other words, simultaneously providing security features and saving energy faces a trade-off problem. This paper presents a novel energy-efficient security architecture in an IEEE 802.15.4-based wireless sensor network called the Hybrid Adaptive Security (HAS) framework in order to resolve the trade off issue between security and energy. Moreover, we present a performance analysis based on the experimental results and a real implementation model in order to verify the proposed approach.

Keywords: Security, energy consumption, reliability, wireless sensor network

A preliminary version of this paper appeared in IEEE ISWPC 2009, Feb 11-13, Melbourne, Australia. This version includes an updated architecture and its implementation cases. In performance analysis and implementation, new experimental results and an analysis of implementation results are newly added. Moreover, the performance analysis is also revised and an energy calculation equation is added.

DOI: 10.3837/tiis.2009.06.002

1. Introduction

Wireless sensor networks with low-power devices have been used as an infrastructure as well as a core technology in order to implement ubiquitous computing environments. A variety of rapidly increasing applications of wireless sensor networks are driven by ecological, military, living environment, and health and personnel related areas. These increasing sensor network applications can sometimes include very sensitive information such as military monitoring, personnel related information, and individual health data because of its native characteristics. In order to protect such sensitive data, various security functionalities are required for wireless sensor networks. Applying additional security features to a sensor node means an increase of energy consumption and a decrease of network life, inevitably. However, wireless sensor networks have inherently constrained resources such as low computation, low memory, short communication range, and low battery life. Specifically, the energy consumption problem continues to remain one of the biggest issues in wireless sensor network as well as a challenge barrier of battery capability. Thus, there is a significant contradiction between providing security functionalities and decreasing energy consumption.

In this paper, we concentrate on a security architecture approach in order to resolve the energy consumption in wireless sensor network. The basic idea for the problem is to apply an appropriate security suite to a packet adaptively. It means that not all of the packets need to have the same security capabilities, so it should be required to consider network and data characteristics when a packet is sent. Thus, we propose a Hybrid Adaptive Security (HAS) framework which can provide efficient security capabilities according to the network and data features considering the energy consumption problem. Our main contribution in this paper is to design a security framework which is capable of dynamically assigning an appropriate security level to packets, and can be practically applicable to a real wireless system such as IEEE802.15.4. Additionally, we make its actual implementation and build a prototype employing the proposed framework.

This paper is structured as follows. An overview and introduction of IEEE 802.15.4/Zigbee security and existing security architectures are given in the Section 2. The proposed approach and use cases are discussed in Section 3. In Section 4, performance evaluation results and an office demonstration using real implemented nodes are presented. The paper is concluded in Section 5.

2. Related Work

2.1 Overview of IEEE 802.15.4/ZigBee

IEEE 802.15.4 is a standard technology for implementing Wireless Personal Area Networks (WPANs) with ease of installation, short range operation, reasonable battery life, and simple protocol stack. Moreover, the standard can be applied for not only home networks, but also a very small device network called by a wireless sensor network. In other words, the IEEE 802.15.4 standard has defined the wireless medium access control and physical layer for low rate wireless personal area networks since 2003. The purpose of the IEEE 802.15.4 standard is to provide low complexity, low cost, low power consumption, and low data rate wireless connectivity. The physical layer supports three kinds of frequency bands such as 868 MHz, 915 MHz, and 2450 MHz with different channels. The gross data rate is from 20kbps to

250kbps. The MAC layer has some characteristics for LR-WPAN. First, two different devices, i.e., Full Function Device (FFD) and Reduce Function Device (RFD) are supported. FFD can be a PAN coordinator, a coordinator, or a simple device. The PAN coordinator is the principal controller of the PAN and provides functionalities such as establishing a new network, assigning a logical network address, permitting other devices to join/leave, maintaining lists of neighbors and routes, routing network packets, and joining/leaving a network. On the other hand, RFD is a simple device to transfer network layer packets and join/leave a network [1].

ZigBee Alliance [2] is developing the very low-cost, very low power consumption, two-way wireless communications standard based on the IEEE 802.15.4 standard. The ZigBee specification is managed by ZigBee alliance, a group of over 170 companies which are manufacturing related semiconductors, development tools and products. The ZigBee architecture consists of ZigBee Network (NWK), Application Support Sublayer (APS), ZigBee Device Object (ZDO), and Application Framework (AF). ZigBee NWK is in charge of organizing and providing routing mechanisms over a multi-hop network built on top of the IEEE 802.15.4 PHY and MAC. ZigBee APL (Application Layer) includes APS, ZDO, and AF. First, APS provides an interface between NWK and APL through a general set of APS data entity and APS management entity services that are used by both the ZDO and the ZigBee company-defined application objects. ZDO represents an interface between the application objects, the device profile and the APS. Finally, the Application Framework provides an environment wherein application objects are hosted on ZigBee devices [3][4][5].

2.2 IEEE 802.15.4 Security and Existing Security Architecture

IEEE 802.15.4 security consists of four kinds of security services which are access control, message integrity, message confidentiality, and replay protection. The access control feature should prevent unauthorized users from participating in the network. In other words, only authorized users can join a legitimated network. Also it is supported by an access control list which includes a variety of security information. Message integrity means the validity of transferred data and message authentication implies the message sender's verification using a cryptographic key. These message integrity and authentication functions are guaranteed by using a message authentication code. The message authentication code is appended to each message sent. Also, several security suites are defined in the IEEE 802.15.4 security specification. The security suites consists of eight different security levels, and each level means a kind of cryptographic algorithm, the mode of block cipher, message authentication code, and the size of message authentication code. The first is the null suite with no security. The next are AES-CTR, AES-CBC-MAC, and AES-CCM. However, these three suites can have three kinds of message authentication codes of 32, 64, 128 bits, separately. AES-CTR implies only encryption mode, AES-CBC-MAC is only message authentication, and then AES-CCM has all modes using encryption and authentication [3][4][5].

There have been few security researches on wireless sensor networks. Especially, there are only a few security architecture researches on providing security features/levels in wireless sensor networks. TinySA [6] is implemented on "smart-dust" using the TinyOS operating system to provide a light-weight security architecture for wireless sensor networks. It is composed of a suite of security protocols and cryptographic primitives to ensure confidentiality, integrity and authenticity of communication in a sensor network using an ECC (Elliptic Curve Cryptography) algorithm. The main contribution of the TinySA architecture is to provide ECC-based WSN security in order to fulfill an energy efficient communication and light-weight public-key cryptography. Tanveer et al. [7], present a cluster formation, secure key management scheme, and a secure routing algorithm to address the special security needs

of tiny sensor nodes and sensor networks as a security framework. Their work tried to propose optimized topology, key-management, and routing for wireless sensor network. Neeli et al. [8] present a security concept called adaptive security architecture. The security architecture is divided into low level, medium level, and high level according to application services. The three defined levels of security can deal with the exigencies of every wireless sensor network service. Slijepcevic et al. [9] propose a communication security framework where a security mechanism is defined for each data type. By employing this multi-tiered security architecture in which each mechanism has different resource requirements, they allow the efficient resource management that is essential for wireless sensor networks. The security level I is reserved for mobile code in case the most sensitive information is sent through the network. The security level II is dedicated to the location information conveyed in messages. The security level III mechanism is applied to the application specific information. So, the work of Neeli and Slijepcevic presents the concept of a security level for wireless sensor networks. In other words, a security level means classifying the security capabilities according to specified measures such as application services. They proposed their own security architecture with security levels, however their works were inadequate to present verified results using a simulation and real implementation.

3. Approach for Hybrid Adaptive Security (HAS) Framework

3.1 Security Suite and Decision Matrix of HAS Framework

A security suite means a set or combination of security operations which is designed to provide security services on MAC frames. Basically, the proposed security suite in **Table 1** is similar to the security suite of IEEE 802.15.4 [1]. However, the most significant point is that the proposed security suites can be dynamically applied to MAC frames according to various characteristics of wireless sensor networks. Moreover, the proposed security suite doesn't have a "None" as a security suite name.

Table 1. Security Suite of HAS Framework

	Suite #1	Suite #2	Suite #3	Suite #4	Suite #5	Suite #6	Suite #7
Authentication		O	O	O	O	O	O
Confidentiality	O				O	O	O
MAC Size	0	32	64	128	32	64	128

In other words, the main contribution of the suites is to provide flexible and dynamic security capability in a security framework employing the decision matrix of **Table 2**. For instance when a packet is sent or received in a wireless sensor network, the appropriate security suite is decided by the various sensor network features such as the network and data/application characteristics. In case of network characteristics, the features can be classified into Public, Commercial, and Private. These attributes of network characteristics have a different secrecy by using keys and its length. A "Public" network attribute means a kind of open network which everybody can connect and it does not guarantee strict confidentiality. However, a "Private" network means it needs very strong and strict security requirements because the network can have a high potential to deal with sensitive information. A "Commercial" attribute is located at the middle of the previous two network features. In addition, each

network characteristic has an authentication code of 32, 64, 128 bits for Public, Commercial and Private, respectively.

Data characteristics are first divided into application and control attributes. First, application data means the collected data (sensing) from application services in wireless sensor networks. Such application attributes consist of Periodic, Urgent-Periodic, On-Demand, and Event-Driven sensing data, separately. Second, control data means the kind of management signals or messages used for operating sensor networks. For example, such messages with security key information (Security), routing information (Routing), geometric information (Location), or update code data (OTA) can be included as the control data. Therefore, if one node tries to send a packet to another node in a wireless sensor network, the characteristics of the network including the node should be first considered. And then the data characteristics are chosen from "App" and "Ctrl" for the network characteristic "Pub". After confirming the two-tier decision procedure(network and data characteristics), an appropriate security suite is finally selected by the decision matrix of **Table 2**. If a target wireless sensor network has the characteristic of "Pub" and its application is "Per", security suite #1 or #2 can be applied for network communication between nodes. Additionally, the suites' selected feature values can be tuned or optimized according to the real-site conditions.

Table 2. Decision Matrix of HAS Framework

SS / #N Features			#1	#2	#3	#4	#5	#6	#7
Pub (32)	App	Per	O	O					
		Urg	O	O					
		On-D	O	O					
		Event	O	O					
	Ctrl	OTA	O				O		
		Loc	O				O		
		Rout	O				O		
		Sec	O				O		
Com (64)	App	Per			O		O		
		Urg			O		O		
		On-D			O		O		
		Event			O		O		
	Ctrl	OTA	O					O	
		Loc	O					O	
		Rout	O					O	
		Sec	O					O	
Pri (128)	App	Per				O		O	
		Urg				O		O	
		On-D				O		O	
		Event				O		O	
	Ctrl	OTA	O						O
		Loc	O						O
		Rout	O						O
		Sec	O						O

*SS : Security Suite, Pub : Public, Com : Commercial, Pri : Private, Per : Periodic, Urg : rgent-Periodic, On-D : On-Demand, Event : Event-Driven, OTA : Over-the-Air Mobile Code, Loc : Location, Sec : Security

3.2. Hybrid Adaptive Security (HAS) Framework

We present the Hybrid Adaptive Security (HAS) framework, the new security architecture for IEEE 802.15.4-based wireless sensor networks that supports the security suites with the decision matrix.

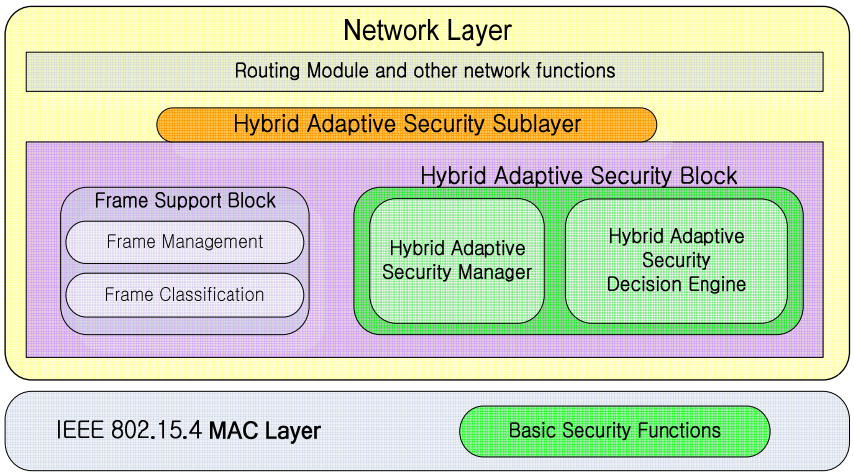


Fig. 1. Hybrid Adaptive Security Architecture

Fig. 1 depicts the proposed whole HAS architecture in IEEE 802.15.4-based network stack with the security suite and decision matrix. Basically, the network stack is based on IEEE 802.15.4 MAC and PHY. In the network architecture, the HAS framework is composed of the hybrid adaptive security block and frame support block specifically. The hybrid adaptive security block has a responsibility to apply an appropriate security suite to a packet or frame for efficiently using security operations such as authentication, integrity, encryption and decryption. It satisfies the security properties (security suite and decision matrix for the HAS framework) outlined in Section 3.1. The Hybrid Adaptive Security block consists of the Hybrid Adaptive Security Manager (HASM) module, which performs a security probing operation with HASDE for the arrived packets from the network layer, or extracts security suite information from an arrived frame in the MAC layer. It also has the Hybrid Adaptive Security Decision Engine (HASDE) module, which is a kind of security suite library that includes specific security features such as key length, encryption algorithm, and integrity function. When a frame or packet has arrived at HASM, it performs a kind of probing process about security related information. In other words, HASM analyzes security suite information, and then performs cryptographic operations with HASDE. After the HASM analyzes security related information such as application-type and network-type, it requests security suite information to HASDE, and then the HASDE module performs a decision process to find out an appropriate security level from the decision matrix of the HAS framework. Moreover, the frame related support blocks have two kinds of functions, which are frame classification and frame management. The Frame classification (FC) module performs a classification operation for received frames from the MAC layer. The Frame Management (FM) module performs a management operation for received network packets from the upper network layer.

In addition, the hybrid adaptive security framework can support a user defined security suite to update a cryptographic algorithm and security functionalities' specification through the Virtual Sensor Profile (VSP) platform (as illustrated in **Fig. 2**). In case of the IEEE 802.15.4

suite, static security suites and its cryptographic algorithms are always used and repeated when sensor nodes try to communicate. This means that for each sensor node, there are no options(or candidates) to change the security parameters under the IEEE 802.15.4 security suite architecture.

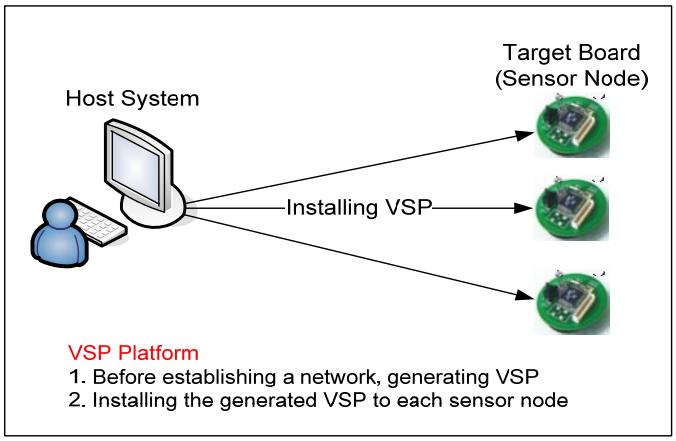


Fig. 2. Virtual Sensor Profile Platform

For instance, when sensor nodes are deployed for a specific sensor network application, a security suite with the same security specification is always applied for the nodes in a wireless sensor network, and thus there are no opportunities to find a more appropriate suite. However, in this paper, the VSP platform can provide some flexibility for updating a security suite and its parameters by using a VSP security profile with a configuration file to support a user generated security suite with various crypto algorithms. VSP consists of the basic sensor node information (address, sensor ID, sensor type, etc,.) and the security profile information. The security profile contains the various attributes (network, application, user-defined, etc,.) that assist the security suite decision process. The VSP platform is a set of PERL modules and scripts to generate a sensor node specified configuration file for sensor developers. In the VSP platform, when the sensor network stack and sensor node software are downloaded, the VSP is also installed. The purpose of VSP generation platform is to allow the developers to customize a security suite in the HAS framework for each sensor through VSP configuration files.

Fig. 3 shows an instance of VSP usage. After the VSP is initially installed to each node, a sink or base station node can send an updating message to the other nodes. The update messge includes the network and data attributes according to the WSN application or services. Thus, each node can have a differentiated security suite. Moreover, by using user solicit parameters, a node can change the crypto specification in a default security suite such as a user defined suite.

3.3. Use Cases of HAS Framework

In order to confirm the operations of the HAS framework, two scenarios are presented; incoming and outgoing packets. **Fig. 4** and **Fig. 5** show the incoming cases of secured and unsecured frames. TheFC module first performs the frame classification operation of received frames from the MAC layer. In other words, after receiving a frame, the FC confirms whether it is secured or not. If the frame is unsecured, the FC sends it to an upper network module according to the frame header information in **Fig. 4**.

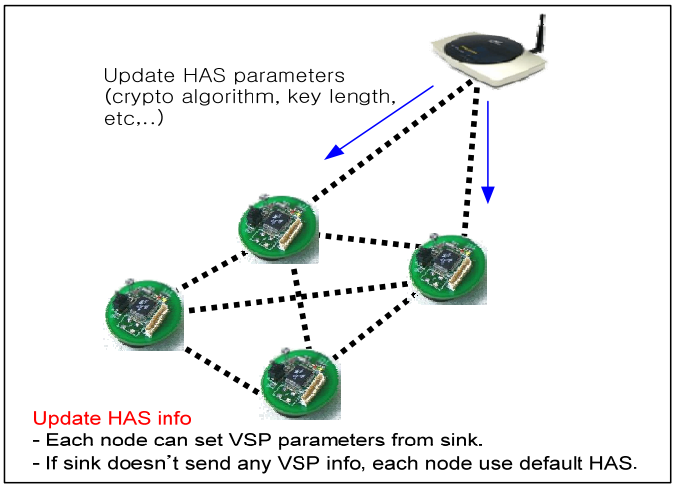


Fig. 3. Use case of Virtual Sensor Profile

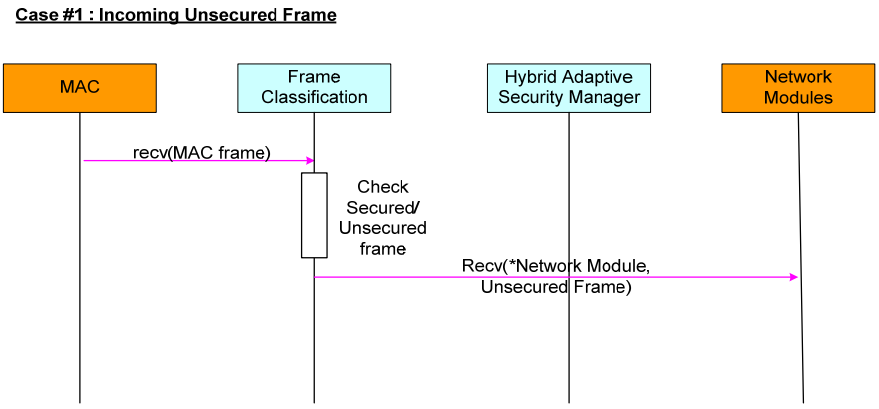


Fig. 4. Incoming case of Unsecured Frame

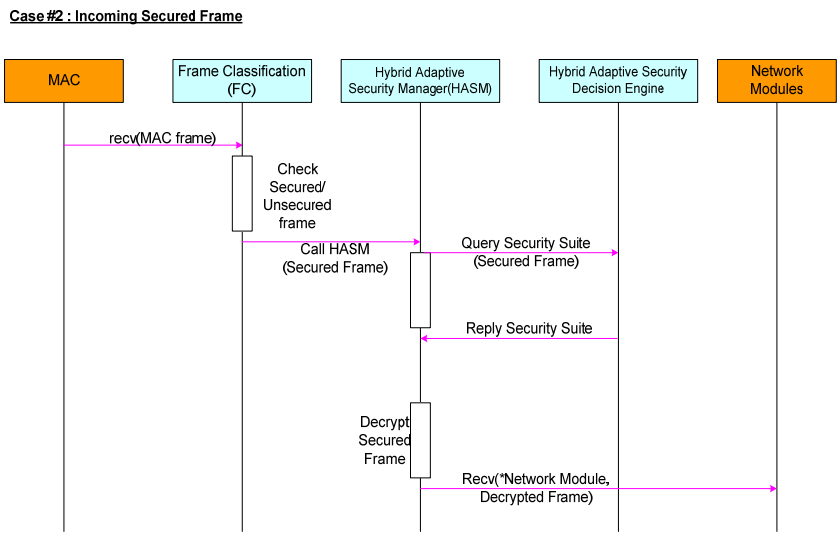


Fig. 5. Incoming case of Secured Frame

On the other hand, if the received frame is secured, the FC sends it to the HASM module in order to check the frame's security suite, and then the HASM requests the frame's security suite information to the HASDE. The HASDE performs a decision process using the frame's security suite information, and then it returns the appropriate security suite information to the HASM. After receiving the decided security level, the HASM decrypts the frame using the replied security suite information. The decrypted frame is sent to a network module according to the network header information in **Fig. 5**.

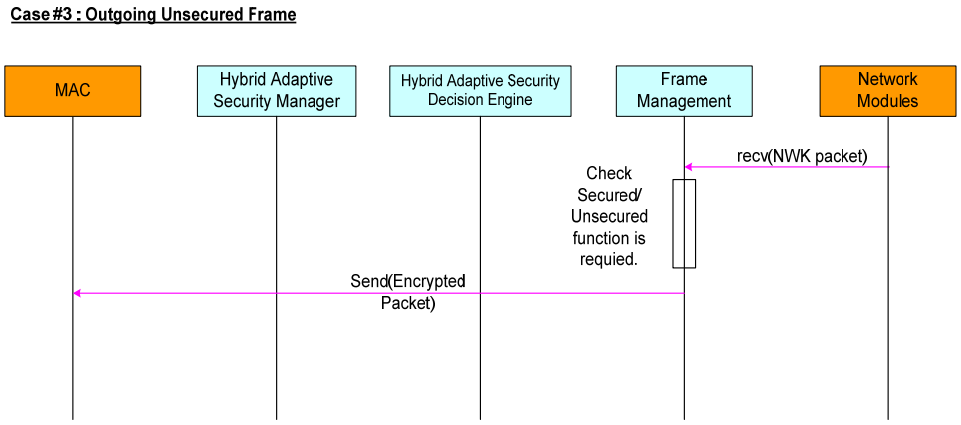


Fig. 6. Outgoing Case of Unsecured Packet

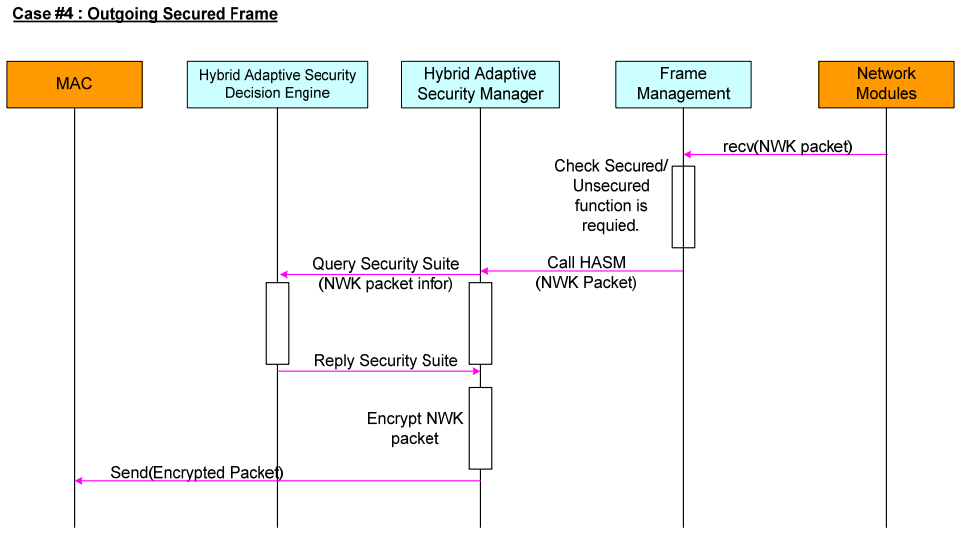


Fig. 7. Outgoing Case of Secured Packet

Fig. 6 and **Fig. 7** describe the outgoing cases of secured and unsecured packets. The FM module first performs the frame management operations for received packets from the upper network layer. Specifically, the FM module checks whether the frame requires security or not and if it requires a security option, the FM module checks its network header to probe for the various data types before delivery to the HASM. If the network packet doesn't need any security features, the FM sends the packet to the MAC layer as shown in **Fig. 6**. Otherwise, the FM sends the packet to the HASM module in order to check the frame's required security suite

based on the network and data attributes from the packet header. The HASM requests the received packet's security suite information to the HASDE module. After the security suite decision process, the HASDE returns the appropriate security suite to the HASM, and then the HASM encrypts the packet by following the replied security suite information. The encrypted packet is sent to the MAC layer as shown in **Fig. 7**.

4. Performance Analysis and Implementation

4.1. Experiment and Results

In order to analyze the performance of the proposed HAS framework approach, we evaluate the expected overhead for calculating the size of the security header in the HAS framework. The expected overhead can be derived from a polynomial equation that has an auxiliary security header size and a message authentication code as a variable, and has a weighted (by usage frequency) value as a coefficient. As for the size of the security header, the default size is 5 bytes (4 bytes for the frame counter and 1 byte for the key counter). Moreover, if a security suite in the HAS framework uses the MAC code to support message authentication, the accumulated header size can be 4, 8, 16 bytes, separately. Thus, one possible combination is 0, 5, 9, 13, 21 and the expected header size can be a variable in a polynomial equation, which is represented by EOS# (Expected Overhead Size) as shown in equation (1). W# is a coefficient in a polynomial equation that represents a weighted value, which is the usage frequency of the security capability (suite) combination under the conditions associated with a specific WSN application or service. Through adjusting weighted values as coefficients, we can suggest a solution for the total overhead of the HAS framework such as equation (2). The weighted values of the estimated overhead equation can be changed according to the security policy and the network (site) condition. Thus, more optimized values can be found by a site tuning method that reflects the network and its application/service features. The kind of work involving security rules and site tuning is not the focus of this paper. The applied weighted value of the equation (2) is obtained from many trials during our experiments. Thus, the derived result is one of the candidates that can be utilized for IEEE 802.15.4-based wireless sensor networks using the HAS framework.

$$\begin{aligned} &Expected\ \ Overhead\ \ of\ \ HAS\ \ Framework \\ &= W_0 * EOS_0 + W_1 * EOS_1 + W_2 * EOS_2 + W_3 * EOS_3 + W_4 * EOS_4 \qquad -(1) \\ &where, \\ &\quad EOS_{\#} : Expected\ \ Overhead\ \ Size, \\ &\quad W_{\#} : Weighted\ \ Value\ \ of\ \ HAS\ \ Framework \end{aligned}$$

$$\begin{aligned} &Expected\ \ Overhead\ \ Calculatio\ n \qquad -(2) \\ &= 0.45 * 0 + 0.20 * 5 + 0.15 * 9 + 0.1 * 13 + 0.05 * 21 \\ &= 0 + 1.0 + 1.35 + 1.3 + 1.05 = 4.7 \\ &where, \\ &\quad EOS_{\#} = 0, 5, 9, 13\ \ and\ \ 21, \\ &\quad W_{\#} = 45\%, 20\%, 15\%, 10\%, and\ 5\% \end{aligned}$$

From the derived equation (2), we can obtain a total overhead of 4.7 if the HAS framework uses 45%, 20%, 15%, 10% and 5% for the weighted values (coefficients) in the polynomial

equation that calculates the expected overhead. Moreover, we can analyze the energy efficiency by calculating the energy consumption per packet according to the packet size with the security header. In case of the proposed approach, the security header is 4.7 bytes by EOS calculation. The security header size of IEEE 802.15.4 is 21 bytes with the default 5 byte security related header and the 16 byte authentication header. A sensor node with the TI CC2420 RF chip is used as a base H/W platform [10], and its current consumption is 18.8 mA and the supply voltage is 3 v. The consumed energy is calculated by equation (3), and then the proposed HAS framework was compared with IEEE 802.15.4 with and without security.

$$Energy(j) = \frac{Supply\ \ Power * Current\ \ Consumption * Header}{Transfer\ \ Rate} \qquad -(3)$$

The result of energy efficiency test per packet is shown in **Table 3**. From the result, we can see that our proposed hybrid adaptive security framework has only a 4% increased overhead in comparison with the default IEEE 802.15.4 network without security. In case of IEEE 802.15.4 with security, it spent 0.28 mJ energy with a 16.7% increased overhead. Thus, the proposed approach can achieve about a four-fold decrease in energy consumption compared to the IEEE 802.15.4 security system.

Table 3. Energy Efficiency per Packet

	Energy Consumption (*mJ*)	Increasing Rate (%)
IEEE 802.15.4 (No Security)	0.24*mJ*	-
IEEE 802.15.4 (Security)	0.28*mJ*	16.7%
Proposed Approach (HAS Framework)	0.25*mJ*	4.2%

In addition, we designed an experiment to evaluate the performance of cryptographic algorithms based on existing approaches. The performance evaluation was designed for AES and RC-5 algorithms based on a sensor node with MSP 430 [11]. In case of using a MSP 430 micro-controller unit, it spends 1.26 nJ per cycle and needs 26 cycle operations per byte. The HAS framework has an AES-based encryption system and a security overhead of 4.7 bytes from the above expected overhead estimation. On the other hand, the Crossbow sensor node based on the TinySec architecture requires an additional 5 byte security overhead and an RC-5 encryption algorithm. **Table 4** shows the performance comparison of three kinds of sensor nodes; the IEEE 802.15.4-based system with no security, the proposed HAS framework, and the TinySec-based approach. Although the difference is not significant, we can see that the proposed HAS framework outperforms the TinySec-based approach. If the proposed approach can be ever better tuned to minimize the expected overhead size, it can present a much better performance.

4.2. Implementation Result

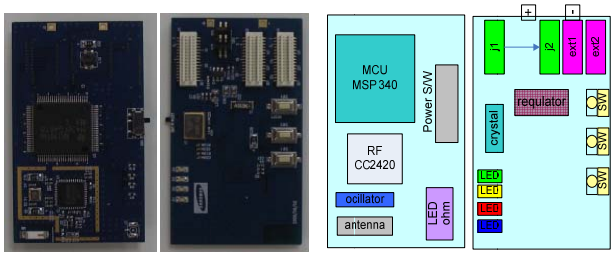
Fig. 8 shows the wireless sensor node and the prototype of its debugging board we built in order to verify the proposed HAS framework. In **Fig. 8**, the sensor node has a connector to extend the sensing modules. The prototype sensor node is composed of Chipcon's CC2420 RF chip [10] and TI's MSP430 MCU [11]. The CC2420 has a 250Kbps maximum speed and a -95 dbm receive sensitivity and operates in the 2.4 GHz bandwidth. Built on a 16 bit RISC

structure CPU, the MSP430 has a 12 bit AD (Analog-to-Digital) converter. Additionally, this 60x32 mm^2 sized sensor node has 116KB fresh memory and 8Kb RAM. Also, its operating system is Tiny OS 2.0 based on NesC.

Table 4. Energy Efficiency using Expected Security Overhead

	Encryption Algorithm	Security (Overhead)	Total Size (bytes)	Cycle	Energy (nJ,mJ)	Increase
IEEE 802.15.4 (No Security)	None	0	97	2522	3177	-
Proposed Approach (HAS Framework)	AES	4.7	101.7	2644	3331	4.8%
TinySEC-based Approach	RC-5	5	102	2652	3342	5.2%

a) IEEE 802.15.4-based sensor node and debugging Board



b) Sensor node layout (head and tail)

Fig. 8. IEEE 802.15.4-based sensor node and debugging board

In order to present a demonstration of a WSN application using the HAS framework, we have deployed a wireless sensor network with various sensors as illustrated in **Fig. 9**. Sensor nodes using various sensors such as sound, motion, vibration, gas, and photo are installed in our institute's office. About 10 sensor nodes are deployed, which basically send periodic data when a sensing timer is used and an event occurs. The sensed data is collected for a UMPC (Ultra Mobie PC) in order to provide office monitoring information. Also, the sensor network is used in combination with a network camera in order to show more realistic data to users. In this application, our deployed WSN was configured with a default setup such as the "Pub" network type and the "Periodic" data type. And then, we tested the HAS framework using two additional kinds of security level scenarios. The HAS framework tests are used to identify network attributes (public, commercial, private) and data (application, control) types from incoming and outgoing packets, and then confirm an appropriate security suite from the

decision matrix. In **Table 5**, the network type of the first example case was public and the data type was from an application using periodic data (a default configuration). Thus, security suite #1, which supports data confidentiality mode using AES-128, was selected. In the next two cases, we can see that security suite #2 and #7 were chosen separately. Thus, we could confirm the usability and potential of the proposed HAS framework that reflects the network and data features of an office surveillance application through a practical demonstration.

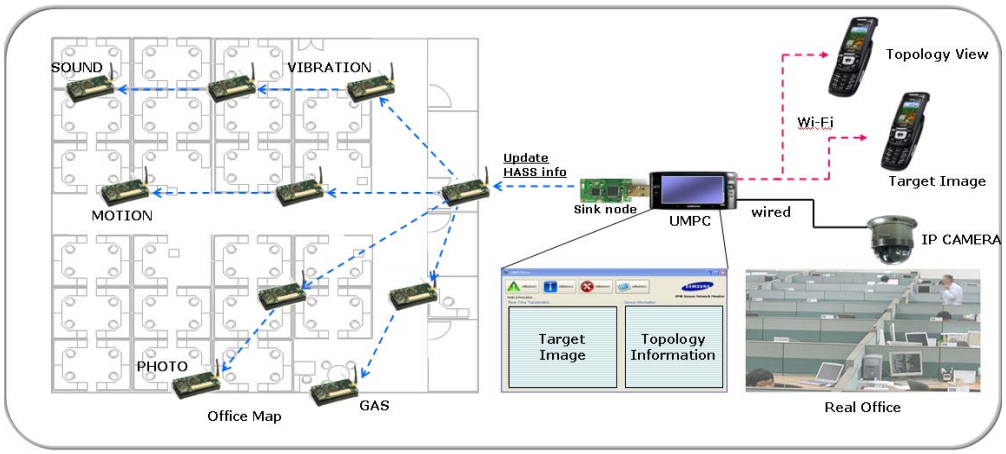


Fig. 9. WSN Demonstration with HAS Framework

Table 5. HAS Framework for Demonstration

	Net Type	Data Type		HAS Decision	HAS Description		
		App	Ctrl		Auth	Conf	Auth Conf
1	Pub	Periodic	-	Suite #1	X	O	X
2	Com	Event	-	Suite #2	O	X	X
3	Priv	-	OTA	Suite #7	X	X	O

5. Conclusion

In this paper we have designed a HAS (Hybrid Adaptive Security) framework to solve the trade-off issue between energy and security through employing a flexible security suite to packets dynamically. Based on this idea, we evaluated the proposed HAS approach and compared its performance to those of the IEEE 802.15.4 and related security schemes. The experimental results showed that the proposed HAS Framework approach had better energy efficiency. The energy consumption is increased only by about 4% in comparison with the IEEE 802.15.4 security scheme (4% versus 16%). In case of the energy efficiency experiment using the expected security overhead, the hybrid adaptive security suite framework shows a slight superiority over the TinySec-based Crossbow (4.8% versus 5.2%). Although the energy consumption efficiency difference of the experiment result is small, it can be improved through adjusting the weighted security header ratio, because the small difference is mainly dependent on the derived size by the expected overhead size equation. Moreover, we designed a real test-bed in order to deploy our own proto-type nodes with the proposed HAS architecture. This shows the potential to apply the architecture to a real site.

Therefore, in this paper, we presented a novel security framework which can be practically used in wireless sensor networks and this will be a vehicle for reliable and robust WSN services with reduced energy consumption supporting differentiated and appropriate security levels.

Furthermore, in the near future we plan to study a more efficient method to find the optimized characteristics of wireless sensor networks for more energy efficiency and enhanced security capability.

References

[1] Institute of Electrical and Electronics Engineers, Inc., IEEE Std. 802.15.4-2003, "Wireless Medium Access Control (MAC) and Physical Layer (PHY) Specifications for Low Rate Wireless Personal Area Networks (LR-WPANs)," New York, IEEE Press, Oct. 2003.
[2] ZigBee Alliance, ZigBee Specifications, version 1.1, Nov. 2006.
[3] Paolo Baronti, Prashant Pillai, Vince W.C. Chook, Stefano Chessa, Alberto Gotta and Y. Fun Hu, "Wireless sensor networks: A survey on the state of the art and the 802.15.4 and ZigBee standards," *Computer Communications*, vol. 30, no. 7, pp. 1655-1695, May 2007.
[4] I. F. Akyildiz, W. J. Su, Y. Sankarasubramaniam, E. Cayirci, "Wireless sensor networks: a survey," *Computer Networks*, vol. 38, pp. 393–422, 2002.
[5] N. Sastry, D. Wagner, "Security Consideration for IEEE 802.15.4 Networks," *WiSe'04 Proceeding*, pp. 32-42, 2004.
[6] Johann Großschädl, "TinySA: a security architecture for wireless sensor networks," *Proceedings of the International Conference on Emerging Networking Experiments And Technologies Archive*, Lisboa, Portugal, 2006.
[7] T. Zia and A. Zomaya, "A security framework for wireless sensor networks," *Proceeding of the Sensors Applications Symposium*, pp. 49- 53, 2006.
[8] N. R. Prasad and M. Alam, "Security Framework for Wireless Sensor Networks," *Wireless Personal Communications*, vol. 37, no. 3-4, pp.455-469, 2006.
[9] S. Slijepcevic, M. Potkonjak, V. Tsiatsis, S. Zimbeck, M. B. Srivastava, "On communication security in wireless ad-hoc sensor networks," *Proceedings of Eleventh IEEE International Workshops on Enabling Technologies: Infrastructure for Collaborative Enterprises*, pp. 139-144, 2002.
[10] Chipcon, Chipcon Products from Texas Instruments, http://www.chipcon.com.
[11] MSP430, Texas Instruments, http://www.ti.com.

Taeshik Shon is a senior engineer in the Convergence Device Lab, DMC R&D Center of Samsung Electronics Co., Ltd. He received his Ph.D. degree in Information Security from Korea University, Seoul, South Korea and his M.S. and B.S. degree in computer engineering from Ajou University, Suwon, South Korea. While he was working toward his Ph.D. degree, he was awarded a KOSEF scholarship to be a research scholar in the Digital Technology Center, University of Minnesota, Minneapolis, USA, from February 2004 to February 2005. He was awarded the Gold Prize for the Sixth Information Security Best Paper Award from the Korea Information Security Agency in 2003, the Honorable Prize for the 24th Student Best Paper Award from Microsoft-KISS, 2005, the Bronze Prize for the Samsung Best Paper Award, 2006, and the Second Level of TRIZ Specialist certification in compliance with the International TRIZ Association requirements, 2008. He is also serving as an editorial staff and review committee of the Journal of The Korea Institute of Information Security and Cryptology, IAENG International Journal of Computer Science, and other journals. His research interests include Mobile/Wireless Network Security, WPAN/WSN Network Security, network intrusion detection systems, and machine learning.

Yongsuk Park received his Ph.D. and M.S degrees in computer science from the Polytechnic Institute of New York University, New York, USA and his B.S. degree in computer science from Sogang University, Seoul, South Korea. Dr. Park is a head researcher at SAMSUNG Electronics Co, Ltd., Korea where he is focusing on Wireless Networks and Mobile Device Security. Previously, he was with AT&T Laboratories at Middletown, NJ, USA as a senior technical staff member from 1999 to 2003, where he conducted various research and development about network optimization and management for data networks and IP services. Since 1995, he has occasionally also been with the City University of New York, New York, USA as a research and teaching staff member working on wireless networks and teaching CS courses. He served as editor for several journals and conferences such as the Journal of SAMSUNG and published a number of papers and patents. His current research interests include broadband wireless cellular networks and utility computing with an emphasis on secure, seamless, cognitive aspects. He is a member of IEEE.