논문 2007-44CI-3-11

센서 인증과 충돌 방지를 위한 USN 채널 확립 알고리즘

(USN Channel Establishment Algorithm for Sensor Authentication and Anti-collision)

이 강 현*

(Kang Hyeon RHEE)

요 약

전자와 컴퓨터 기술의 발전은 무선 센서 네트워크 증대의 토대를 마련하였다. 이에 따라, 센서 네트워크상의 충돌 방지와 인증 기술의 필요성이 증대되어 지고 있다. 센서 네트워크의 충돌 방지를 위해 개발될 알고리즘은 무선 센서 네트워크 플랫폼상에 쉽게 적용될 수 있으며 또한 동시에 분산 연산, 분산 저장, 데이터 강인성, 센싱된 데이터를 자동 분류할 수 있어야한다. 그리고 무선 센서 네트워크에서 보안을 유지하기 위하여 여러 센서 간에 안전하게 채널을 확립할 수 있어야한다. 본 논문 우리는 센서의 인증과 충돌 방지를 위하여 유비쿼터스 센서 네트워크 채널 확립 알고리즘을 제안하였다. 본 논문에서는 두 가지 다른 형태의 구조를 제안하였으며, 각 구조에서는 센서 노드 사이에서 채널을 확립하기위하여 웨이블렛 필터를 사용한 알고리즘과 센서의 충돌 방지를 위하여 BIBD(Balanced Incomplete Block Design) 코드를 사용하였다. 결과적으로, BIBD와 웨이블렛 필터 기반으로 제안된 알고리즘은 이상적인 환경에서 98% 충돌 검출율을 가졌다.

Abstract

Advances in electronic and computer technologies have paved the way for the proliferation of WSN(wireless sensor networks). Accordingly, necessity of anti-collusion and authentication technology is increasing on the sensor network system. Some of the algorithm developed for the anti-collision sensor network can be easily adopted to wireless sensor network platforms and in the same time they can meet the requirements for sensor networks like: simple parallel distributed computation, distributed storage, data robustness and auto-classification of sensor readings. To achieve security in wireless sensor networks, it is important to be able to establish safely channel among sensor nodes. In this paper, we proposed the USN(Ubiquitous Sensor Network) channel establishment algorithm for sensor's authentication and anti-collision. Two different data aggregation architectures will be presented, with algorithms which use wavelet filter to establish channels among sensor nodes and BIBD (Balanced Incomplete Block Design) which use anti-collision methods of the sensors. As a result, the proposed algorithm based on BIBD and wavelet filter was made for 98% collision detection rate on the ideal environment.

Keywords : USN Channel Establishment, BIBD, Anti-collision, Wavelet filter

I. Introduction

Wireless sensor networks (WSNs) have recently emerged as a premier research topic. Sensor networks pose a number of new conceptual and optimization problems such as location, deployment and tracking. Wireless ad-hoc sensors are self-creating, self-organizing, and self-administering [1,2]. Those parts are important in sensor networks since the data obtained with them are massive and with high dimensionality, which could easily break down the processing and storage capacity of a centralized data collection system. On the other hand, the data obtained by the sensor networks are often self-correlated over time, space and different sensor inputs. This is a consequence of the nature of the

* 정회원, 조선대학교 전자정보공과대학 전자공학과
(Dept. of Electronic Eng., College of Elec-Info Eng., Chosun University, Korea)
접수일자: 2007년4월6일, 수정완료일: 2007년5월7일

phenomena being sensed which is usually changing gradually. It is also due to the redundant sensor nodes dispersed near each other and the fact that often the sensor readings are correlated over different modalities sensed at one node [3].

Sensor networks usually consist of a large number of ultra-small autonomous devices. Each device, called a sensor node, is battery powered and equipped with integrated sensors, data processing, and short-range radio communication capabilities. And sensor networks are being deployed for a wide variety of applications, including military sensing and tracking, environment monitoring, patient monitoring and tracking, smart environments, etc. When sensor networks are deployed in a hostile environment, security becomes extremely important as they are prone to different types of malicious attacks [4]. An open research problem is how to bootstrap secure communications among sensor nodes. To provide security, communication should be encrypted and authenticated.

In this paper, the author proposed the Ubiquitous Sensor Network channel establishment algorithm for sensor's authentication and anti-collision. Allocating communication channel in each sensor to used wavelet filter for channel establishment between deployed sensors and sink node. Therefore we solved the problem of extension channel using wavelet filter character which is scalability of 2^n. Also, BIBD code was assigned in each sensor for using Ack signal between sensors and sink node to prevent/avoid data collision that is produced in WSN, that is, the proposed algorithm has robustness about collusion attack and collision between channels using the anti-collision property of BIBD code. And two different data aggregation architectures will be presented with algorithms which transmit data from a base station to sensors and from base station to sink nodes.

The remainder of the paper is organized as follows: The recent work on channel establishment algorithm in Section Ⅱ. In Section Ⅲ, theoretical background is explained for wavelet filter and BIBD code, the author proposed the USN channel establishment algorithm for sensor's authentication and anti-collision in Section Ⅳ. The proposed algorithm's performance analysis and simulation results are presented in Section Ⅴ and the conclusion is drawn in Section Ⅵ.

Ⅱ. Recent works

There exists some research to study the Channel establishment algorithm in WSN[5-7] in recent years. In these papers, the information theoretical aspects of the correlation are explored in depth. In other words, these studies aim to find the optimum rate to compress redundant information in the sensor observations. More recently, the relation between distortion, spatio-temporal bandwidth and power for large sensor networks is investigated [8]. Moreover, none of the above solutions develop communication network protocols. In [9], spatial and temporal correlation is exploited to eliminate the acknowledgment in the communication. While the number of acknowledgments is considerably reduced, the number of redundant packets is still high in the network. The joint routing and source coding is introduced in [10] to reduce the amount of traffic generated in dense sensor networks with spatially correlated records. While joint routing and source coding reduces the number of transmitted bits, the number of transmitted packets remains unchanged from the network point of view. In [11], the number of transmitted packets can be further minimized by regulating the network access based on the spatial correlation between the sensor nodes. Moreover, the relation between spatial and temporal sampling rate on the overall network delay and energy consumption is studied in [12]. However, the spatial and temporal correlation between sensor observations is not investigated. Current studies on medium access in WSN focus mainly on the energy-latency tradeoffs. S-MAC[13] aims to decrease the energy consumption by using sleep schedules with virtual clustering. T-MAC[14], a variant of S-MAC, incorporates variable

sleep schedules to further decrease the energy consumption. However, in both protocols, sensor nodes keep sending redundant data with increased latency due to periodic sleep durations. In [15], an energy-aware TDMA-based MAC protocol is presented where the sensor network is assumed to be composed of clusters and gateways. Each gateway acts as a cluster-based centralized network manager and assigns slots in a TDMA frame. The protocol assumes a cluster-based topology, which requires significant additional processing complexity and overhead in the overall sensor network. An energy-efficient collision-free MAC protocol, which is based on a time-slotted structure, is presented in [16]. Each node determines its own time slot using a distributed election scheme based on traffic requirements of its every two-hop neighbor. Although the protocol achieves high delivery ratio with tolerable delay, the performance of the protocol depends on the two-hop neighborhood information in each node. Since this information is collected through signaling, in the case of high density sensor networks, the signaling cost increases significantly resulting in either incomplete neighbor information due to collisions or high energy consumption due to signaling costs.

III. Theoretical backgrounds

1. balanced incomplete block design

Combinational problems can generate the matrix that satisfies a restricted condition using a matrix model. The BIBD code generates Incidence Matrix which satisfies the restricted condition of anti-collision and can thus analyze a partly matrix symmetry. That is, the anti-collision code has robustness against collusion attack. Among ncode vectors, the combination of less than $(n-1)$ code vectors differ each other and can therefore detect less than $(n-1)$ colluders.

The BIBD code is generated with 5 parameters (v, b, r, k and λ)

Where :

v: Number of treatments

b: Number of blocks

r: Number of times each treatment is run

k: Number of treatments per block

λ: Number of times a pair of elements of v appear in the same block.

$$vr = bk \tag{1}$$

$$r(k-1) = \lambda(v-1) \tag{2}$$

Five parameters satisfy a restrict condition of Eq. (1) and (2) and simply present Incidence Matrix $v \times b$ represented with (v, k, λ) using Eq. (3) and (4).

$$b = \frac{v(v-1)\lambda}{k(k-1)} \tag{3}$$

$$r = \frac{\lambda(v-1)}{k-1} \tag{4}$$

In Incidence Matrix, if $b=v$ or $r=k$, then the BIBD code is to be a symmetric square matrix. Incidence Matrix M with $v \times b$ is defined by Eq. (5) and satisfied in Eq. (6)

$$M = [m_{ij}]$$
$$m_{ij} = \begin{cases} 1 \text{ if } j_{th} \ blocks \in i_{th} \ elements \\ 0 \ otherwise \end{cases} \tag{5}$$

$$MM^t = (r-\lambda)I + \lambda J \tag{6}$$

I : $v \times v$ Identity Matrix

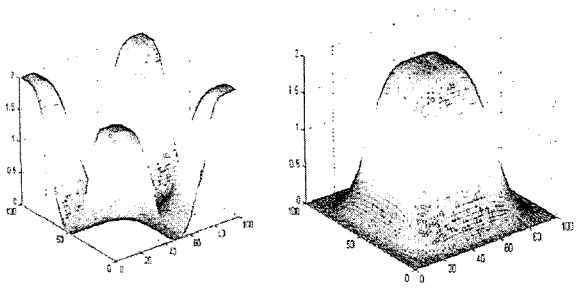
J : $v \times v$ Unit Matrix

As a result, the row vector of Incidence Matrix M will be a fingerprint code and given to b users and this Incidence Matrix M can be used as an anti-collision code.

2. Wavelet filter

Wavelet function is satisfied condition of Eq. (7) and (8).

$$\int_{-\infty}^{\infty} \varphi(t)dt = 0 \tag{7}$$



(a) Wavelet synthesis filter (b) Wavelet decomposition filter

그림 1. 웨이블렛 필터 응답.
Fig. 1. The response of wavelet filter.

$$\int_{-\infty}^{\infty} |\varphi(t)|^2 dt < \infty \tag{8}$$

Eq. (9) is presented discrete wavelet. Compression of time axis achieved changing coefficient i included in Eq. (9).

$$\varphi_{j,k}(t) = 2^{\frac{j}{2}} \varphi(2^j t - k) \quad i,j \in Z \tag{9}$$

Eq. (10) is wavelet synthesis equation that is used in transmission data modulation and Eq. (11) is wavelet decomposition equation that is used in detection of transmit data.

$$c_{j+1}(n) = \sum_{k=0}^{N-1} h(n-2k)c_j(k) + \sum_{k=0}^{N-1} g(n-2k)d_j(k) \tag{10}$$

$$\begin{aligned} c_j(n) &= \sum_{k=0}^{N-1} h(k-2n)c_{j+1}(k) \\ d_j(n) &= \sum_{k=0}^{N-1} g(k-2n)c_{j+1}(k) \end{aligned} \tag{11}$$

Fig. 1 shows that the response of wavelet in frequency domain

IV. Proposed algorithm

The proposed algorithm established communication channel between cluster and sensors using wavelet filter bank and prevented the collision of channels used BIBD code. In this paper, there is two type of structure. One is that a base station can collect data from all of the sensors and the other structure is extended cluster head model. Each of these two architectures can use a wavelet transformation on each sensor signal, treated as a one dimensional time series. Different wavelet transformation methods have been developed, more or less complex. In this paper, we have chosen one of the simplest methods Haar wavelet transform.

1. One cluster head collecting all sensor data

The proposed structure, base station had filter bank(channel number), BIBD code and the allocated code values of each sensor. If selection signal transmits through filter bank of the sensor which wants to do communication, the sensor which was allocated filter bank channel transmits BIBD code to the base station. This structure can select sensor efficiently because of using wavelet filter bank and base station can check external collusion attack or collision between sensors by having code. Fig. 2 shows that total block diagram of the proposed algorithm.

In the Fig. 2, '1' is a part of filter bank to selects channel of each sensor by using wavelet. Fig. 3 shows that channel selection module using wavelet.

Sensor transmits data to base station using

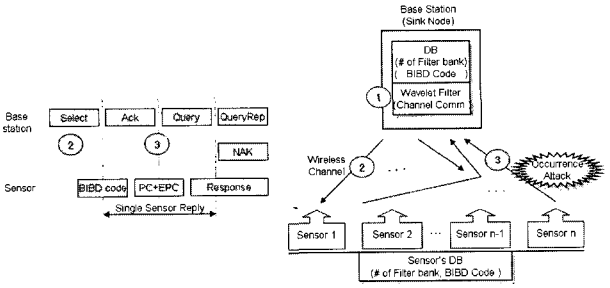


그림 2. 모든 센서 데이터로부터 수집되는 Cluster head.
Fig. 2. Cluster head collecting all sensor data.

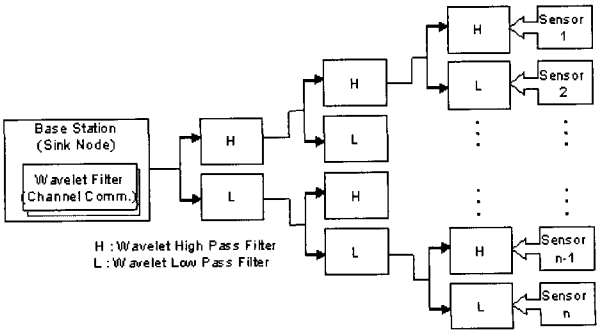


그림 3 웨이블렛을 이용한 채널 선택 모듈.
Fig. 3. Channel selection module using wavelet.

channel that is selected through Fig. 3 and base station can establish channel without collision or collusion attack by detecting BIBD code.

2. Extended cluster head model

The author proposed the extended cluster head model that was extended from one cluster head model. This model is possible to communicate between sink node and base station. Fig. 4 shows that the extended cluster head model.

The proposed model had structure that allocate each channel using filter bank to transmit data between base station and sink node and in the Fig. 5, this algorithm shows that can detect data collision and collusion attack.

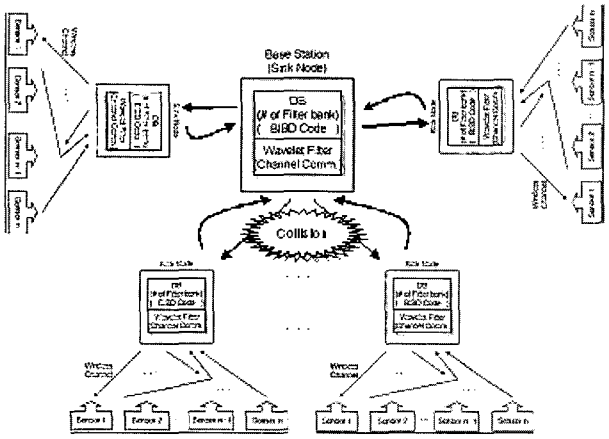


그림 4. 확장된 cluster head 모듈.
Fig. 4. Extended cluster head model.

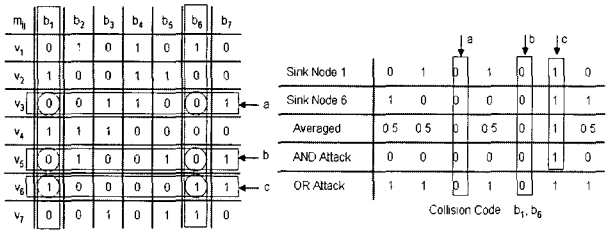


그림 5. BIBD 코드의 Anti-collision.
Fig. 5. Anti-collision BIBD code.

V. Experimental result

The platform for the experiments, from which the data analyzed in this paper were obtained, is a collection of 'USN-AP-Zigbee'. One that this unit embodies a sensor module (audio), and a

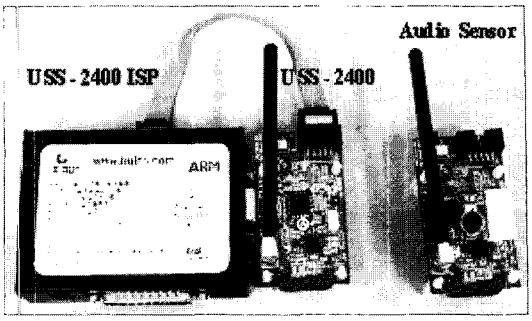


그림 6. 시뮬레이션에 사용된 Hardware architecture.
Fig. 6. Hardware architecture used in simulation.

표 1. 여러 공모자에 의한 공모 상황들.
Table 1. The collusion cases by the number of colluder.

Number of colluders	Number of collusion cases			
	{7,3,1} code	{15,7,3} code	{22,11,5} code	{31,15,7} code
2	21	105	231	465
3	35	455	1540	4495
4	35	1365	7315	31465
5	21	3003	26334	169911
6	7	5005	74613	736281

communication module, which are interconnected. Fig. 6 shows the hardware architecture which used in simulation.

In simulation, the condition of BIBD code parameter { v, k, λ} is generated with {7,3,1}, {11,5,2}, {15,7,3}, {19,9,4}, {23,11,5}, {31,15,7}, {39,20,9} and {47,24,11}. As collusion/collision attack, a collusion/collision number of possible combination is presented in Table 1. The collusion/collision detection of experiment, measured the robustness of anti-collision and channel establishment.

The correlation coefficient of collision code and codebook in the base station is computed, that result is upper critical value then it defines collision. Correlation coefficient is computed by Eq. (12).

$$r = \frac{\frac{1}{n}\sum_{i=1}^{n}(x_i-\bar{x})(y_i-\bar{y})}{\sigma_x \sigma_y}, \quad -1 \le r \le 1 \tag{12}$$

$\bar{x}, \bar{y}$: Average

σ_x, σ_y : Standard deviation

Table 2 shows the result of collision code detection

표 2. 통신채널에서의 공격에 대한 검출된 공모자의 수.

Table 2. The number of the detected collision by attack on communication channel.

	Number of Collisions							
BIBD code	6	10	14	18	22	30	38	46
{7,3,2}	5.86	-	-	-	-	-	-	-
{11,5,2}	5.86	9.2	-	-	-	-	-	-
{15,7,3}	5.88	9.3	13.4	-	-	-	-	-
{19,9,4}	5.91	9.4	13.5	17.4	-	-	-	-
{23,11,5}	5.92	9.5	13.6	17.5	21.4	-	-	-
{31,15,7}	5.92	9.5	13.7	17.6	21.5	29.3	-	-
{39,20,9}	5.92	9.6	13.8	17.7	21.6	29.4	37.1	-
{47,24,11}	5.92	9.7	13.9	17.8	21.7	29.5	37.2	45.1

against collision averaging attack by means of the algorithm proposed in this paper. As a result, collision was 98% detected only for the collision averaging attack.

VI. Conclusion

This paper presents a ubiquitous sensor network channel establishment algorithm for sensor's authentication and anti-collision in the field of wireless. The positive features of the proposed algorithm such as simple parallel distributed computation, distributed storage, data robustness and auto-classification of sensor readings are demonstrated within two different proposed architectures.

Ones of the proposed architectures with one cluster head collecting only clustering outputs from the other units provides a big dimensionality reduction and in the same time additional communication saving, since only classification IDs (small binaries) are passed to the cluster head instead of all input samples.

As a result, we confirmed that the proposed algorithm base on BIBD code has 98% detection of collision of sensor. Also, filter bank using wavelet transform can be incorporated as a preprocessing unit of the USN giving the ability to extract important features in the data like abrupt changes at various scales.

In our future work, we will study channel establishment algorithm using other ACC (Anti Collusion Code) and how the accuracy of deployment modeling affects these results.

References

[1] Kang-Hyeon RHEE, "Detection of Colluded Multimedia Fingerprint using LDPC and BIBD,"IEEK Journal CI, pp. 68-75, 2006. 9

[2] W. Jia and J. Wang, "Analysis of connectivity for sensor networks using geometrical probability," IEE Proc.-Commun. Vol 153, No. 2, April 2006.

[3] A. Kulakov, D. Davcev and G. Trajkovski, "Application of Wavelet Neural-Networks in Wireless Sensor Networks," IEEE Proc. of the Sixth International Conf. on Sofware Eng., 2005.

[4] Wenliang Du, Jing Deng, Yunghsiang S. Han and Pramod K. Varshney, "A Key Predistribution Scheme for Sensor Networks Using Deployment Knowledge," IEEE Trans. on dependable and secure computing, Vol. 3, No. 1, January 2006.

[5] M. Gastpar and M. Vetterli, "Source-channel communication in sensor networks," Proc. 2nd Int. Workshop on Information Processing in Sensor Networks (IPSN'03), vol. 219, pp. 162-177, 2003.

[6] S. S. Pradhan, J. Kusuma, and K. Ramchandran, "Distributed compression in a dense microsensor network," IEEE Signal Process. Mag., vol. 19, no. 2, pp. 51-60, Mar. 2002.

[7] A. Scaglione and S. D. Servetto, "On the interdependence of routing and data compression in multi-hop sensor networks," in Proc. ACM MobiCom, Atlanta, GA, Sep. 2002, pp. 140-147.

[8] "Power, spatio-temporal bandwidth, and distortion in large sensor networks," IEEE J. Sel. Areas Commun., vol. 23, no. 4, pp. 745-754, Apr. 2005.

[9] L. Zhong, R. Shah, C. Guo, and J. Rabaey, "An ultra-lowpower and distributed access protocol for broadband wireless sensor networks," presented at the Networld + Interop: IEEE Broadband Wireless Summit, Las Vegas, NV, May 2001.

[10] A. Scaglione and S. D. Servetto, "On the interdependence of routing and data compression

in multi-hop sensor networks," in Proc. ACM MobiCom, Atlanta, GA, Sep. 2002, pp. 140-147.
[11] Mehmet C. Vuran and Ian F. Akyildiz, "Spatial Correlation-Based Collaborative Medium Access Control in Wireless Sensor Networks," IEEE/ ACM Transactions on networksing, Vol 14, No. 2, APRIL 2006.
[12] S. Bandyopadhyay and E. J. Coyle, "Spatio-temporal sampling rates and energy efficiency in wireless sensor networks," in Proc. IEEE INFOCOM, Mar. 2004, vol. 3, pp. 1728-1739.
[13] W. Ye, J. Heidemann, and D. Estrin, "Medium access control with coordinated adaptive sleeping for wireless sensor networks," IEEE/ACM Trans. Netw., vol. 12, no. 3, pp. 493-506, Jun. 2004.
[14] T. van Dam and K. Langendoen, "An adaptive energy-efficient MAC protocol for wireless sensor networks," in Proc. ACMSenSys 2003, Los Angeles, CA, Nov. 2003, pp. 171-180.
[15] K. A. Arisha, M. A. Youssef, and M. Y. Younis, "Energy-aware TDMA-based MAC for sensor networks," Comput. Netw. J. (Elsevier), vol. 43, no. 5, pp. 539-694, Dec. 2003.
[16] V. Rajendran, K. Obraczka, and J. J. Garcia-Luna-Aceves, "Energy-efficient, collision-free medium access control for wireless sensor networks," in Proc. ACM SenSys 2003, Los Angeles, CA, Nov. 2003, pp. 181-192.

저 자 소 개

이 강 현(평생회원)
1979년, 1981년 조선대학교 전자공학과 공학사 및 석사
1991년 아주대학교 대학원 공학박사
1977년～현재 조선대학교 교수
1991년, 1994년 미 스탠포드대 CRC 협동연구원.
1996년 호주 시드니대 SEDAL 객원교수
2000년～현재 한국 멀티미디어기술사협회 이사
2002년 영국 런던대 객원 교수
2002년 대한전자공학회 멀티미디어연구회 전문위원장
2003년 한국 인터넷 방송/TV 학회 부회장
2003년～현재 대한전자공학회 상임이사
2005년～현재 조선대학교 RIS 사업단장
<주관심분야 : 멀티미디어 시스템설계, Ubiquitous convergence>