Sensors & Transducers, Vol. 172, Issue 6, June 2014, pp. 61-66

Sensors & Transducers

Orthogonal Code Based Anonymity Communication Protocol for Wireless Sensor Networks

[1] Jiangang Deng, [2] Zhiming Zhang
[1] Science and Technology Research Place, Jiangxi Normal University, Jiangxi, Nanchang, 330022, China
[2] School of Software, Jiangxi Normal University, Jiangxi, Nanchang, 330022, China
[1] E-mail: zzm_9650@163.com

Received: 11 April 2014 /Accepted: 30 May 2014 /Published: 30 June 2014

Abstract: In some environments, the security of the wireless sensor networks (WSNs) involves not only the security of sending data, but also the anonymity and privacy during data delivery, how to design a secure efficient anonymity communication scheme for wireless sensor networks has became an important research topic. The proposed schemes can provide efficient anonymous communication, but some of the schemes need more overheads on computation, storage and bandwidth consumption. In this paper, an anonymous secure communication protocol for wireless sensor network is proposed based on orthogonal code and symmetric secret key, comparing with the previous anonymous communication schemes for wireless sensor networks, this scheme not only can satisfy the basis require of anonymity communication, but also improve distinctly in storage and bandwidth consumption, and is more suitable for the wireless sensor networks. *Copyright © 2014 IFSA Publishing, S. L.*

Keywords: Wireless sensor networks, Anonymous communication, Orthogonal code, Anonymity, Bandwidth consumption.

1. Introduction

With the development of more advanced sensor technology, wireless sensor networks are widely used in various fields, such as health care [1], military, environmental, target tracking [2], etc. Wireless sensor network is composed by many low-cost sensors, the computing and storage capacity of each sensor node is limited. Sometimes, wireless sensor network is deployed in unprotected or hostile environment, and it is vulnerable to be attacked by the adversary. The security of WSNs is not only involved in the confidentiality, integrity and authentication of the communication content, but also the anonymity and privacy during data delivery. The adversary can locate and compromise some important nodes by eavesdropping on the identities of the communication nodes, and the adversary can launch many attacks through the compromised nodes. Therefore, an efficient anonymous communication scheme is essential for WSNs to hiding the real identities of communication nodes. Anonymous communication of WSNs is that the communication relationship between the sensor nodes is hidden by a certain method, and the eavesdropper can not know or infer the identity of any sensor node and the communication relations of both.

In order to prevent the adversary from eavesdropping on the identities of the communication nodes, a variety of anonymous routing schemes were proposed for mobile ad hoc

networks that are closely to wireless sensor networks [3-7], but the mobile ad hoc networks are different from the wireless sensor networks, and these schemes can not be applied straight to the resource-constrained WSNs. Recently, there are some works on anonymous routing schemes for wireless sensor networks [8-12]. The proposed schemes can prevent the adversary form getting the identities of the communication, but some of the schemes need more overheads on computation, storage and bandwidth consumption.

In this paper, an anonymous secure communication protocol for wireless sensor network is proposed based on orthogonal code and symmetric secret key. In our scheme, each sensor node is assigned to an orthogonal code as the unique identity, the Summation of all the identities of intermediate forwarding routing nodes is transmitted with the packet, according to the additive property of orthogonal code, any intermediate routing node in the routing path can confirm that it is part of the routing path, but do not know the real identities of the communication sender and receiver, and the destination node i do not know the real identities of the intermediate routing nodes also. This scheme not only can satisfy the basis require of anonymity communication, but also improve distinctly in storage and bandwidth consumption.

The organization of the lecture is as follows. The related work is introduced in Section 2, in Section 3 briefly introduces The Orthogonal Code, the Section 4 is the description of anonymity communication protocol for wireless sensor networks, anonymity, security, and performance analysis of the new scheme are discussed in Section 5 and 6, Section 7 is the conclusion.

2. Related Work

Recently, anonymity communication in wireless sensor has become an important topic, there are some anonymous routing schemes are proposed for wireless sensor networks.

S. Misra and G. Xue [9] proposed an anonymous scheme (SAS) for clustered wireless sensor networks. To ensure concealment of its true identifier (ID), the SAS uses a range of pseudonyms as identifiers for a node in the network, and the ranges are non-contiguous and chosen uniformly at random from a pseudonym space. After deployment, neighboring nodes in the network share their individual pseudonyms and use them to ensure that the communication is anonymous and that a node's true ID is kept private. Even when many nodes in a given neighborhood of the network are compromised and are colluding, The SAS ensures that non-compromised nodes are still guaranteed complete anonymity.

In [10], Yi Ouyang, *et al*. proposed two schemes for protecting anonymity of sensors in wireless sensor networks based on hash function chain, HIR and RHIR. The basic idea of HIR is for each individual sensor node to use a one-way keyed hash chain for producing a sequence of hash values as its IDs. The anonymity of a message's sender is protected as long as the key is not compromised. A sensor node can delete its previous ID and generate a new one after sending a message. In RHIR method, it uses a one-way hash chain in reverse-in other words, it assigns a sensor node's ID backwards from the end of the hash chain to the beginning. This change improves the security properties of HIR method. Both schemes can provide better anonymity than previous solutions when the secret keys are compromised. But two schemes require each node maintains a routing information table, with the increasing of number of nodes, it required storage space is increasing dramatically, and is not suitable for large-scale distributed wireless sensor networks.

In [11], an efficient Anonymous Communication (AC) protocol for sensor networks was proposed. The AC protocol was composed by anonymous one-hop communication and anonymous end-to-end communication scheme. In the protocol, each sensor node finds the link direction (towards the base station) between itself and its neighbors during the deployment stage by a broadcast from the base station. Then the sensed data can be sent to the base station hop-by-hop by the link direction. After that, the AC protocol utilizes an anonymous one-hop communication scheme and an anonymous end-to-end communication scheme to achieve the source anonymity, the communication relationship anonymity and the base station anonymity.

In [8], to protect sources against the local adversary and global adversary, P. Pengjun and V. Boppana proposed an anonymous communication protocol for WSNs. In the protocol, Each node transmits exactly one fixed-size packet in an active period regardless of whether it has useful data to send/forward or not. Upon a reception of a real packet, a sensor node buffers it, processes it, and relays it when next transmission is fired. If a dummy packet is received, it is discarded immediately. If a sensor node has a real packet in its buffer (its own injected packet or a received relay packet) when next transmission is fired, it sends the packet immediately. If not, a dummy packet with the same size will be generated and sent. In the case when the sensor node has multiple real packets, data aggregation may be used to make sure only one packet is sent.

In [12], a lightweight anonymous on-demand routing scheme (LANDER) was proposed, the LANDER first uses Bloom filter to hide the identities of the routing sensor nodes, and thereafter generates per-hop pseudo-link identifiers based on the elliptic curve cryptosystem for accomplishing private information exchange in WSNs. In the LANDER scheme, after path establishment, each pair of neighbor nodes authenticate each other anonymously, and establish a pseudo-link identifier with an associated pair-wise key. This pair-wise key and pseudo-link identifier are used for anonymous

data forwarding. This scheme not only conceals the node and the link identities in data packets, but also helps to achieve traffic anonymity due to content analysis.

3. Preliminary

3.1. The Orthogonal Code

Orthogonal code [13] is widely used in the field of wireless communications and information hiding [14-15]. The orthogonal code has the following three properties.

1) Any two dissimilar orthogonal codes do inner product computing, the result of the operation is zero. For example, if A and B are two distinct orthogonal code, then,

$$A \cdot B = 0$$

2) One orthogonal code and itself do inner product computing, the result of the operation is one. For example, if A is an orthogonal code, then,

$$A \cdot A = 1$$

3) The Orthogonal codes have the property of additive, the sum of K orthogonal codes remains the characteristics of (1), (2). For example, if there are four orthogonal codes A, B, C and D, the S is the sum value of the three orthogonal codes A, B and C, then,

$$\begin{aligned} S &= (A+B+C) \\ S \cdot A &= (A+B+C) \cdot A \\ &= A \cdot A + B \cdot A + C \cdot A \\ &= 1 \end{aligned} \quad \text{(i)}$$

$$\begin{aligned} S \cdot D &= (A+B+C) \cdot D \\ &= A \cdot D + B \cdot D + C \cdot D \\ &= 0 \end{aligned} \quad \text{(ii)}$$

It can be determined from the formula (i), the A is contained in S, and it can be determined from the formula (ii), the D is not included in S.

4. Description of Anonymity Communication Protocol for Wireless Sensor Networks

4.1. System Model and Notations

The wireless sensor network consists of the base station and a large of sensor nodes. The base station is not resource constrained, and can not be compromised. The base station will receive sensed data sent from the sensor nodes, and send some security operation instructions to the sensor nodes. The base station saves the whole network topology information. Each sensor node i have a unique identity ID_i, each sensor node i is preloaded a secret key $K_{i,BS}$ shared with the base station. We assume that the adversary can eavesdrop on and analyze the package transmitted in the network, and get the identities of the communication nodes and their communication relationships. The adversary can locate and compromise some important nodes by the identities of the communication nodes, and launch many attacks through the compromised nodes.

This paper defines anonymous communication to achieve the following objectives.

1) Identity confidentiality. Any intermediate routing nodes do not know the real identities of the communication sender (source) and receiver (destination), and the sender and the receiver do not know the real identities of the intermediate routing nodes also.

2) Position confidentiality. The location of the sender and the receiver will not be known by the other nodes, intermediate routing node can not get the distance between the source and destination, in other words, intermediate forwarding node can not judged to the hops from the sender to the receiver.

3) Routing anonymity. The adversary can not find the sender and the receiver by tracking sending packets, in other words, the third party is difficult to extrapolate the transfer mode of communication between the source and destination.

Since many notations are used in our proposed protocol, in order to easy to inquire, compare and reference, we list the notations used in proposed protocol in Table 1.

Table 1. Notations of proposed protocol.

Notation	Definition
BS	The base station
ID_{BS}	The identity of the base station
S_i	the node i
ID_i	The identity of the node i
$K_{i,BS}$	The secret key shared between the node i and base station
$E_K(M)$	A message M encrypted with the key k
T	A timestamp
$\|\|$	The concatenation operation
$\oplus$	Addition operation
$\odot$	Inner product operation

4.2. System Initialization

Each sensor node is preloaded a secret key $K_{i,BS}$ shared with the base station. The system generates a series of mutually different orthogonal codes according to the paper [4], each sensor node is assigned to an orthogonal code as the unique identity ID_i. The system deploys the sensor nodes to the target area. We consider only the static network, and it means that the sensor nodes can not move after deployment.

4.3. Anonymity Communication Protocol

If the base station wants to communicate anonymously with the sensor node i, it will perform the following steps.

1) The base station selects a path from base station to node S_i (BS, S_1, S_2, …, S_{i-}, S_i).

2) The base station computes the SumID = $ID_1 \oplus ID_2 \oplus \ldots \oplus ID_{i-1} \oplus ID_i$, a communication sequence number RPID, and a timestamp T.

3) The base station generates the routing packet RP=< RPID||SumID|| $E_{Ki,BS}$(data||T) >, and broadcast to the network, where the data denotes the security operation instruction is sent to the destination node i, and the $E_{Ki,BS}$(data) denotes the data is encrypted by the secret key $K_{i,BS}$.

4) After receiving the routing packet RP, each node j will check if the packet has already been received using the unique RPID, if it has been in the memory, the packet will be dropped, if not, each node j will do inner product computing with it's ID_j and SumID, $L=SumID \odot ID_j = (ID_1 \oplus ID_2 \oplus \ldots \oplus ID_{i-1} \oplus ID_i) \odot ID_j$, if the result of the operation is zero, which means the node j is not in the routing path, it will drop the packet right now, if the result of the operation is one, which means the identity of the node j is contained in the SumID, in other words, the node j is in the routing path, it will saves the RPID to its memory, and attempts to decrypt the $E_{Ki,BS}$(data) with the secret key shared by the node j and the base station. If it can decrypt correctly the $E_{Ki,BS}$(data) and the timestamp T is within a reasonable range, the node j is the destination node, and anonymous communication is over, if can not, the node j is a intermediate routing node in the routing path, it will broadcast this packet to other nodes within its wireless transmission range.

5. Anonymity and Security Analysis

5.1. Anonymity Analysis

1) Identity confidentiality. In our scheme, each sensor node is assigned to an orthogonal code, as the unique identity ID_i. All the identities of intermediate routing nodes are embedded in the SumID of the routing packet RP, any intermediate routing nodes do not know the real identities of the communication sender (source) and receiver (destination), and the destination node i do not know the real identities of the intermediate routing nodes also.

2) Position confidentiality. In our scheme, when the intermediate routing nodes receive the routing packet, each node j will do inner product computing with it's ID_j and SumID, if the result of the operation is one, which means the node j is in the routing path, it can not get the distance from the source to destination, in other words, any intermediate forwarding node can not judged to the hops between the sender and the receiver.

3) Routing anonymity. All the identities of intermediate routing nodes are embedded in the SumID, only the nodes in the routing path can know itself is in the routing path, any other node or the adversary is difficult to extrapolate the transfer mode of communication between the source and destination.

5.2. Security Analysis

1) Against passive attack. The adversary can get the routing packet RP=< RPID||SumID|| $E_{Ki,BS}$(data|| T) >, but it has no the secret key shared between the node i and the base station, it can not get the data from the $E_{Ki,BS}$(data). Although the adversary can get the SumID, but it has no any node identity in the routing path, it can not get any correct routing information.

2) Minimum information disclosure. The sensor node in the routing path only can confirm itself is in the routing path, it can get any routing information of other nodes.

3) Verifiability. Any intermediate routing node in the routing path can confirm that it is part of the routing path, because only the SumID and the node identity in routing path do inner product computing, the result of the operation is one.

6. The Performance Analysis

6.1. Storage Requirements

In this section, we analysis the storage requirements of our scheme and the other schemes. We assume that the base station has unlimited computation ability and storage, we do not take the memory cost of the base station.

In order to achieve the purpose of anonymous communication, in scheme [2], the amount of memory required by each node is $6k + 7kN$, where k represents the size of the k-bits of the pseudo-name space, N is the number of the adjacent node of the current node, if there are 1000 sensor nodes in the wireless networks, the pseudo-name space is 64-bit, and the adjacent node of each node is 100, the amount of memory required by each node is 6*64+7*64*100=45184 bits≈5.6 KB. In scheme [3], each node needs to maintain an information table of neighboring nodes. The table includes (HT, HHT(x), Link), where HHT(x) denotes the keyed hash values of neighboring nodes' IDs, the HT denotes the number of hash operation and the Link denotes the direction of the data flow, the total storage requirement at each node is (HT+HHT(x)+Link)N, let k=128 bit, HHT(x)=k=128 bit, HT=k/2=64 bit, Link=k/2=64 bit and the number of neighboring nodes is 100, the amount of memory required by each node is $(k+k/2+k/2)\times N$=100*(128+64+64)=25600 bits≈

≈3.125 kB. In scheme [7], the total storage requirement at each node is 4k+3kN+2, where N denotes the average number of neighbors for each node, and k represents the size of the k-bits of the hashing value. For instance, in a WSN with1000 nodes, let k=128 bit and each node has an average of 100 neighbors. The memory requirement shall be, 4*128+3*128*30+2=12,034 bits ≈ 1.5 kB. For a WSN with 5,000 nodes and a neighbor size of 100 nodes, the memory requirement is: 4*128+3*128*100+2=38,914 bits=4.8 kB. In our scheme, each immediate routing node needs to store the RPID to its memory for one anonymity communication. In order to save storage space, each node will delete all the RPID after period of time. The total storage requirement at each node is k/2*N during a period of time, where k represents the size of the k-bits of the RPID, N is the number of the RPID, if there are 100 RPID in each immediate routing node during a period of time, and let k=64 bit, the amount of memory required by each node is 64*100=6400 bit≈0.78 kB.

Table 2 compares the storage costs of our scheme with several existing anonymous communication protocols [2, 3, 7]. Table 2 shows that our scheme needs little memory burden.

Table 2. The comparison of the storage costs.

Anonymous communication schemes	The storage costs (bits)
Scheme[2]	6k +7 k*N
Scheme[3]	(k+k/2+k/2)*N
Scheme[7]	4k+3k*N+2
Our scheme	k/2*N

6.2. Bandwidth Consumption

In this section, we analyze the bandwidth consumption of our scheme and the other schemes.

Let L_{RPID}, L_{SumID} denote the length of the RPID and SumID, and L_e denotes the length of the data by encrypted. The format of the report packet is RP=< RPID||SumID|| $E_{Ki,BS}$(data|| T) >, so, the length of a report packet is L_p= L_{RPID}+ L_{SumID} + L_e. In scheme [3], the message that a sensor node received and sent is $M=H_{Kij}^{HTj}(ID_j) \| H_{Ki}^{t}(ID_i) \| t \| D_t$, where ID_j means the identity of node j, the ID_i means the identity of node i, the $H_{kij}^{HTj}(ID_j)$ means using K_{ij} as a key to hash ID_j for HT_j times, the $H_{ki}^{t}(ID_i)$ means using K_i as a key to hash ID_i for t times, the D_t is a encrypted data block collected by the sender. Let L_{H1}, L_{H2} denote the length of the $H_{kij}^{HTj}(ID_j)$ and $H_{ki}^{t}(ID_i)$, let L_t denote the length of the t, and L_D denotes the length of D_t, so, the length of a report packet is L_p'= L_{H1}+ L_{H2} + L_t + L_D. In scheme [7], the message that a sensor node received and sent is $M=OHAI_{ij}||E_{kij}(AI_i||\ E_{ki}(D)||AAI_{ij})$ + AAI_{ij} $||D_{rand}$, where $OHAI_{ij}$ means One-hop anonymous identity shared between node i and node j, AI_i means the global anonymous identity of node i shared between i and the base station, AAI_{ij} means an anonymous acknowledgement identity shared between node i and node j, D_{rand} means an anonymous acknowledgement identity shared between node i and node j, and $E_{kij}(D)$ means Data D encrypted by pair-wise key k. Let L_{OHAI}, L_{AAI} denote the length of the $OHAI_{ij}$ and AAI_{ij}, Let L_{Drand}, L_e denote the length of the $E_{kij}(AI_i||\ E_{ki}(D)||AAI_{ij})$ and D_{rand}, so, the length of a report packet is L_p''= L_{OHAI} + L_{AAI} + $L_{e'}$ + L_{Drand}. Let e_r, e_s, denote the energy consumption of receiving and sending 1 byte report packet, when a intermediate routing node receives a report packet from another node, it will forward the report packet to the other nodes, so, the energy consumption in our scheme is E_p=n* L_p *(e_r+e_s), the energy consumption in scheme [3] is E_p'=n* L_p' *(e_r+e_s), the energy consumption in scheme [7] is E_p''=n* L_p'' *(e_r+e_s), where n denotes the average number of hops from the source node to the destination node.

Let e_r=12.5 μJ, e_s=16.25 μJ, L_{RPID}=64 Bits, L_{SumID} = 64 Bits, L_{H1} = L_{H2} = L_{OHAI} =128 bit, L_t = L_{AAI} = L_{Drand} =64 bits, L_e = L_D = $L_{e'}$ =24 Bytes, the figure1 depicts the bandwidth consumption of our scheme, scheme [3] and scheme [7].

The Fig. 1 shows that our scheme is lower in energy consumption than scheme [3] and scheme [7] with the increasing of the number of hop from the source to destination.

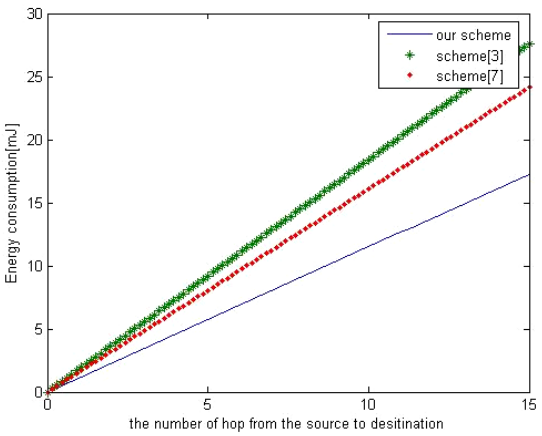

Fig. 1. The bandwidth consumption comparison of our scheme and scheme [3, 7].

7. Conclusions

In this paper, we proposed a novel security anonymity communication scheme for wireless sensor networks based on orthogonal code and symmetric secret key. All the identities of intermediate routing nodes are embedded in the SumID, any intermediate routing node in the routing

path can confirm that it is part of the routing path, but do not know the real identities of the communication sender and receiver, and the destination node i do not know the real identities of the intermediate routing nodes also. The anonymity, security and performance analysis show that our scheme not only can satisfy the basis require of anonymity communication, but also improve distinctly in storage and bandwidth consumption, and is more suitable for the wireless sensor network.

Acknowledgements

This work was financially supported by National Natural Science Foundation of China (61363077) and education office project of Jiang Xi province (GJJ13206).

References

[1]. Bae Wan D., Narayanappa Sada, Alkobaisi Shayma, Liu Cheng C., Real-time health monitoring system for evaluating environmental exposures, *Journal of Software*, Vol. 8, Issue 4, 2013, pp. 791-801.

[2]. Makki S. Kami, Sun Bo, Guidry Ricky, Hill Jeffery, Efficient Monitoring Strategy for Active Environments, *Journal of Software*, Vol. 6, Issue 4, April 2011, pp. 536-543.

[3]. A. Boukerche, K. El-Khatib, L. Xu, L. Korba, An Efficient Secure Distributed Anonymous Routing Protocol for Mobile and Wireless Ad Hoc Networks, *Computer Communications*, Vol. 28, Issue 10, 2005, pp. 1193-1203.

[4]. Y. Zhang, W. Liu, W. Lou, Anonymous Communications in Mobile Ad Hoc Networks, in *Proceedings of the Annual IEEE Conference on Computer Communications (INFOCOM'05)*, 13-17 March 2005, pp. 1940-1951.

[5]. A. Boukerche, Y. Ren, ARMA: An Efficient Secure Ad Hoc Routing Protocol, in *Proceedings of the IEEE Global Communications Conference (GLOBECOM'07)*, Washington, DC, 26-30 November 2007, pp. 1268-1272.

[6]. J. Kong, X. Hong, M. Gerla, An Identity-Free and On-Demand Routing Scheme Against Anonymity Threats in Mobile Ad Hoc Networks, *IEEE Transaction on Mobile Computing*, Vol. 6, Issue 8, 2007, pp. 888-902.

[7]. L. Bao, R. Chen, D. Sy, ODAR: On-Demand Anonymous Routing in Ad Hoc Networks, in *Proceedings of the IEEE International Conference on Mobile Adhoc and Sensor Systems*, Vancouver, 09-12 October 2006, pp. 197-206.

[8]. Pengjun Pan, Boppana R. V., ACP: Anonymous communication protocol for wireless sensor networks, in *Proceedings of the IEEE Consumer Communications and Networking Conference (2011CCNC)*, Las Vegas, NV, 9-12 January 2011, pp. 751-755.

[9]. S. Misra, G. Xue, SAS: A Simple Efficient anonymity schemes for clustered wireless sensor networks, in *Proceedings of the IEEE International Conference on Communications (ICC'06)*, Istanbul, June 2006, pp. 3414-3419.

[10]. Yi Ouyang, Zhengyi Le, Yurong Xu, Triandopoulos N., Sheng Zhang, Ford J., Makedon F., Providing Anonymity in Wireless Sensor Networks, in *Proceedings of the IEEE International Conference on Pervasive Services*, Istanbul, 15-20 July 2007, pp. 145-148.

[11]. Juan Chen, Hongli Zhang, Binxing Fang, Xiaojiang Du, Lihua Yin, Xiangzhan Yu, Towards Efficient Anonymous Communications in Sensor Networks, in *Proceedings of the Global Telecommunications Conference (GLOBECOM'11),* Houston, TX, USA, 5-9 December 2011, pp. 1–5.

[12]. Muhammad Bashir Abdullahi, Guojun Wang, A Lightweight Anonymous On-Demand Routing Scheme in Wireless Sensor Networks, in *Proceedings of the IEEE International Conference on Trust, Security and Privacy in Computing and Communications (TrustCom'12)*, Liverpool, 25-27 June 2012, pp. 978–985.

[13]. R. C. S. Chauhan, R. Asthana, Y. N. Singh, A General Algorithm to Design Sets of All Possible One Dimensional Unipolar Orthogonal Codes of Same Code Length and Weight, in *Proceedings of the IEEE International Conference on Computational Intelligence and Computing Research (ICCIC),* Coimbatore, 28-29 December 2010, pp. 1-7.

[14]. M. Son, Y. Lee, C. Pyo, Design and Implementation of mobile RFID technology in the CDMA networks, *RFID/USN Research Group, Electronics and Telecommunications Research Institute,* Daejeon, Korea, February 2006, pp. 1033-1036.

[15]. Wuu L. C., Chen Y. J., Kuo W. C., Hung C. H., Zero-Collision RFID Tags identification based on CDMA, in *Proceedings of the Fifth International Conference on Information Assurance and Security*, Xi'an, China, 2009, pp. 513-516.