http://dx.doi.org/10.6109/ijice.2011.9.6.676

Transmission Power Range based Sybil Attack Detection Method over Wireless Sensor Networks

HwaJeong Seo, Howon Kim*, *Member, KIICE*

***Abstract*— Sybil attack can disrupt proper operations of wireless sensor network by forging its sensor node to multiple identities. To protect the sensor network from such an attack, a number of countermeasure methods based on RSSI (Received Signal Strength Indicator) and LQI (Link Quality Indicator) have been proposed. However, previous works on the Sybil attack detection do not consider the fact that Sybil nodes can change their RSSI and LQI strength for their malicious purposes. In this paper, we present a Sybil attack detection method based on a transmission power range. Our proposed method initially measures range of RSSI and LQI from sensor nodes, and then set the minimum, maximum and average RSSI and LQI strength value. After initialization, monitoring nodes request that each sensor node transmits data with different transmission power strengths. If the value measured by monitoring node is out of the range in transmission power strengths, the node is considered as a malicious node.**

***Index Terms*— Sybil Attack, Wireless Sensor Network, Reduced Signal Strength Indicator, Link Quiality Indicator, Transmission power**

I. INTRODUCTION

WIRELESS Sensor Network (WSN) is the technology of enabling the ubiquitous environment such as surveillance system, home automation and structure integrity monitoring, etc. These WSN applications provide many conveniences to us. However it can also easily be abused by malicious users because the WSN applications are basically dependent on wireless network, which is easily attackable communication media. The communication data in WSN are easily captured and modified by a malicious user for its purposes.

The malicious user can impersonate authorized users by modulating its transmission power strength. To detect or prevent the Sybil attack, two kinds of methods have been proposed. One is using cryptography scheme to verify the user, but this method is not suitable to the resource constrained devices because cryptography algorithms need to compute the complex computation. The other type of Sybil attack detection method is location based verification method, in which we need to compute the localization algorithm to determine the sensor's location. The localization techniques are mostly using the values of Time of Arrival(TOA), Time difference of Arrival(TDOA), AOA(Angle of Arrival) or RSSI(Received Signal Strength Indicator).

The TOA based method exploits signal propagation time between source and destination nodes. The drawback of TOA is necessity of high clock resolution. Transmitter and recipient are required to synchronize the clock, which cause much more overhead than the other methods [1].

Second, TDOA based method uses the arrival time of a signal obtained from at least three nodes. The difference of signal arrival information among three nodes determines the source location [2].

Third, AoA based method is a method for determining the direction of propagation of a radio-frequency wave incident on an antenna array [3].

Last, received signal strength (RSS) is measured in each received packet, which can be quantized into the RSSI which is linearly reduced getting distance between recipient and sender. Therefore, the information presents the distance between source and destination nodes. The drawback of RSS is irregular signal propagation and multipath fading causing the inaccuracy on range estimation [4].

Among these localization methods, many researches have been done based on the RSSI value. This is because other methods except the RSSI based Sybil attack detection method requiring an additional module on sensor node or additional computations.

However, previous research works on RSSI based Sybil attack detection methods assumed that the malicious node does not change the transmission power strength in Sybil attack processes. But in real attack scenario, the malicious node can change their transmission power strength for its purposes. This is the main motivation of this research work.

Contributions of the paper: In the paper, we present a new method for Sybil attack detection using range of transmission power strengths. Also we provide the novel approach in determination of signal interference case using proposed method.

Outline: This paper is organized as follows. In section 2, we give an introduction to Sybil attack and previous Sybil attack detection. In section 3, we present our proposal. In section 4, we analyze the result of implementation.

Manuscript received September 9, 2011; revised November 4, 2011; accepted November 15, 2011.

Hwajeong Seo is with the Department of Computer Engineering, Pusan National University, Pusan, 609-735, Korea (Email: hwajeong@pusan.ac.kr)

Howon Kim* (Corresponding author) is Professor in the Department of Computer Engineering, Pusan National University, Pusan, 609-735, Korea (Email: howonkim@pusan.ac.kr)

Finally, the conclusion is drawn in the last section.

II. RELATED WORKS

A. Sybil attack

The Sybil attack is introduced in [5] to denote an attack where Sybil node tries to impersonate multiple identifications in sensor network. It is easier to perform than traditional network medium in sensor network where messages are communicated through the air with same frequency among all nodes. Sybil nodes, which forge broadcast messages, disrupt sensor network to make group based decisions. The following is the important protocols affected by Sybil attack.

Distributed Storage: Sybil node can disrupt the architecture where data is replicated or fragmented on several nodes. The hash table for authentication of reality data will be stored in Sybil nodes.

Routing: Routing mechanisms where nodes are disjointed the network are affected by Sybil nodes because it has various identifications and locations at the same time.

Data Aggregation: Sensor nodes usually aggregate the data into one node, because sensor device has lack of resources, computation capabilities. Sybil node can change the aggregated data if it is selected as an aggregation node.

Voting: In sensor network, decisions which are made using voting are easily controlled by Sybil node using multiple polls from multiple virtual identities.

B. Sybil attack detection

Since sensor nodes are designed to small and low computing device, existing solutions for Sybil attack detection using cryptography algorithm are infeasible in terms of computation cost and hardware capability which imposes an excessive computation and data transmission overheads on sensor nodes.

For this reason, location based Sybil attack detection using a received signal strength indicator (RSSI) is more proper method as it is not required to compute the complex computations, which makes decision by location and distance between sender and recipient.

RSSI based Sybil attack detections are comprised of a single monitoring node and multiple monitoring nodes. A single monitoring node based algorithm such as disc based detection [6] divides the area into the sub-area, called disc, depending on distance. Sensor nodes are allocated to the disc. After initialization of disc allocation, monitoring node determine the suspect or normal node based on disc number. The method is required to compute a simple operation and deploy single monitoring node which is efficient in terms of computation cost and the number of monitoring node. However, if Sybil nodes are located in the same disc with ordinary nodes, monitoring node cannot distinguish the Sybil nodes and ordinary nodes. This area is defined as indistinguishable section illustrated in figure 1. (B).

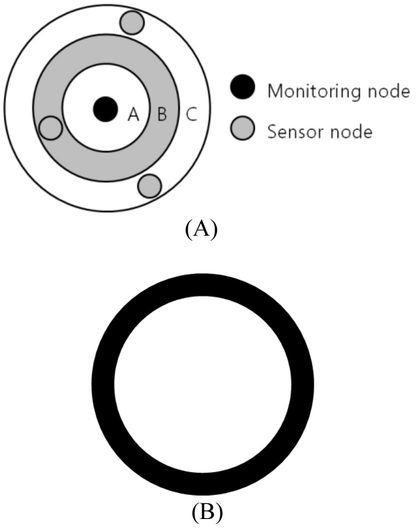


Fig. 1. (A) Disc based Sybil attack detection.
(B) Indistinguishable section.

The multiple monitoring nodes detection, called cooperative RSS-based Sybil detection [7, 8], is installing the multiple nodes to get the more accurate distance relation information from the area. In the CRSD, multiple monitoring nodes measure the RSS ratio depending on each position of node. Then monitoring nodes periodically report the RSS ratio to the root node, by which the Sybil attack judgment is decided through comparisons of RSS relations. Compared to the single node detection, indistinguishable section decreases as the number of monitoring node increases, which is illustrated in Figure 2.

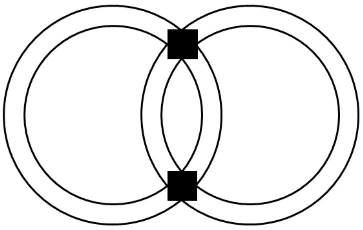


Fig. 2. Indistinguishable section in case of two mon itoring nodes

However, the method is vulnerable to transmission power modulation. If malicious node equipped with directional antenna modulates the transmission power and sends the message, monitoring node cannot distinguish the modified and normal message. This is illustrated in Figure 3. If Sybil node wants a short distance with monitoring node, it transmits the messages with high transmission power. On the contrast, if Sybil node wants a long distance, it transmits the data with low transmission power. Through the Sybil attack mechanism, Sybil node can cheat the monitoring node and disrupt the Sybil attack detection system.

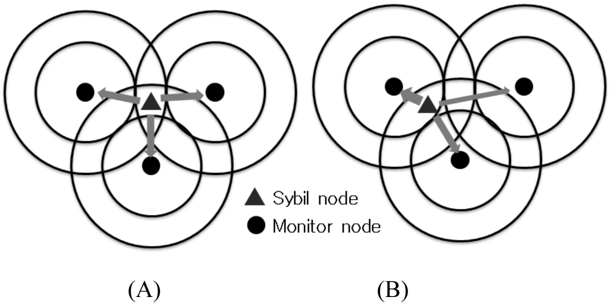


Fig. 3. (A) Actual position (B) Sybil attack using signal strength modification.

C. RSSI and LQI

Current platforms including micaZ, Telos and Intel Mote2 use the same radio chip the CC2420 [9, 10, 11] which provides two useful measurements: RSSI and LQI. RSSI is the estimate of the signal strength and is expressed with 8-bit and stored in the RSSI_VAL register. Chipcon specifies the formula to compute the received signal power in dBm: RSSI_VAL+RSSI_OFFSET, where RSSI_OFFSET is about -45. RSSI is unreliable and time-varying in general and radio transmission is non-isotropic [12].

LQI can be viewed as chip error rate and is expressed with 8-bit which is usually between 110 and 50, and correspond to maximum and minimum quality frames respectively.

Radio chip CC2420 provides eight transmission power modes which are determined and programmed using TinyOS [13] which is operating system designed for low-power wireless devices. Adjusting the transmission power, we can transmit the data with different output power.

TABLE I
EIGHT TRANSMISSION POWER MODES AND CURRENT CONSUMPTION

Output Power [dBm]	Current Consumption [mA]	Output Power [dBm]	Current Consumption [mA]
0	17.4	-1	16.5
-3	15.2	-5	13.9
-7	12.5	-10	11.2
-15	9.9	-25	8.5

In source code of tinyos (/opt/tinyos-2.x/tos/chips/cc2420/transmit/CC2420TransmitP.nc), programmers easily adjust the transmission power when installing the program with modified tx_power. In the Table 2, transmission power is obtained from cc2420packet. If there is no settlement on power, it will put the default power to the tx_power. When we put the transmission power to the tx_power, the eight power values including (31, 27, 23, 19, 15, 11, 7 and 3) are determined, which are matched with output power in Table 1.

TABLE II
TRANSMISSION POWER ADJUSTMENT PART IN TINYOS

```
void loadTXFIFO() {
cc2420_header_t* header = call
CC2420PacketBody.getHeader( m_msg );
uint8_t tx_power = (call
CC2420PacketBody.getMetadata( m_msg ))->tx_power;
if ( !tx_power ) {
tx_power = CC2420_DEF_RFPOWER;
}
call CSN.clr();
//The rest is omitted.
```

III. PROPOSAL

Our proposal detects the Sybil attack by measuring the range of RSSI and LQI in terms of different transmission power strengths. To utilize the proposal we need to follow the four procedures comprised of deployment, setup, monitor and detection.

Deployment: To collect the information of RSSI and LQI, the monitoring nodes are deployed to the designated area. Depending on detection methods (single or multiple monitoring nodes) we can choose the number of monitoring node. If we deploy the more monitoring nodes to the designated area, we can get the more accurate collaborated information.

Setup: Whenever sensor node joins the network, the monitoring nodes measure the range of transmission power. To measure the capability of transmission power, monitoring nodes ask the sensor node to send the message with the different transmission power strengths. The transmission is started from the lowest transmission power to the highest transmission power, as first received message presents the lowest transmission power of the sensor node. From that transmission power, monitoring nodes gather the RSSI and LQI value, increasing the transmission power. As a result of the procedure, we can get the range of transmission power and more detailed RSSI and LQI value depending on different transmission power.

Monitor: Monitoring nodes compute a relation of the transmission power and location using average RSSI and LQI. Then the monitoring nodes compare the data with the former RSSI and LQI data. The average value is set depending on variable α which is a constant smoothing factor in weighted average mechanism between 0 and 1. Since RSSI and LQI values are instable and irregular in the reality, we also use the standard deviation of the value to make decision accurately considering the irregularity. When the measured value is out of range (average value ± standard deviation), the sensor node is regarded as Sybil node.

Detection: When Sybil attack is detected in the WSN, monitoring nodes inform root monitoring node that location and identification number of the suspect and then isolate the sensor node from network to prevent foreseeable additional attacks.

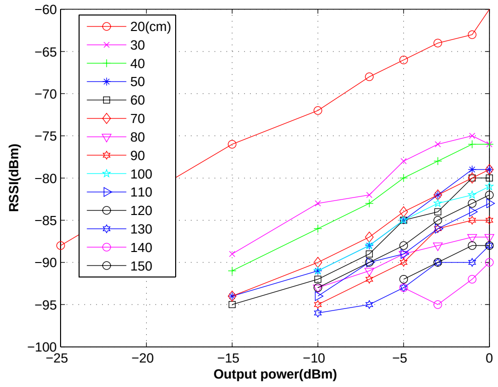
IV. EVALUATION AND DISCUSSION

Compared to the previous one, proposal has strong features in terms of transmission power modulation and signal interference. To evaluate the method, we first deployed the monitor and sensor node and then measured the RSSI and LQI, increasing the distance between the monitoring and sensor node. The RSSI and LQI are measured per 100 times by each distance and transmission power.

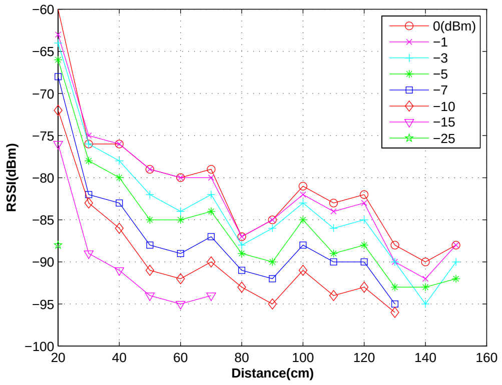
A. Transmission power modulation

Figure 4(A), 5(A) illustrate that the RSSI and LQI are linearly reduced as propagation distance increases or transmission power decreases. If malicious node, deployed in a long distance from monitoring node, generates the messages with high transmission power, the node can impersonate an ordinary sensor node in a short distance. To detect the Sybil attack, we used the range of transmission power and RSSI and LQI depending on different transmission power.

In Figure 4(B), 5(B), we found that every node has the unique range of transmission power associated with their location. Even though malicious node can impersonate the others in RSSI and LQI, it is impossible to impersonate the range of transmission power. In a short distance, variation of RSSI is wider than nodes in a long distance. On the contrast, in a long distance, variation of LQI is wider than nodes in a short distance. Therefore, unique location determines the range and unique variation of RSSI and LQI value.

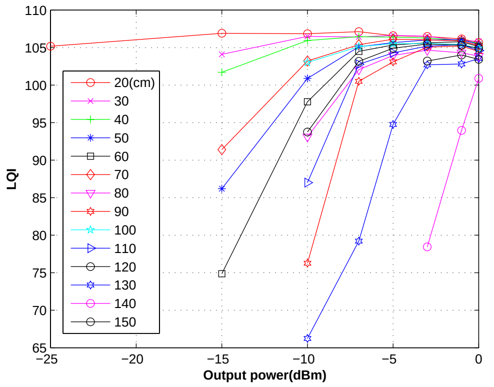


(A)

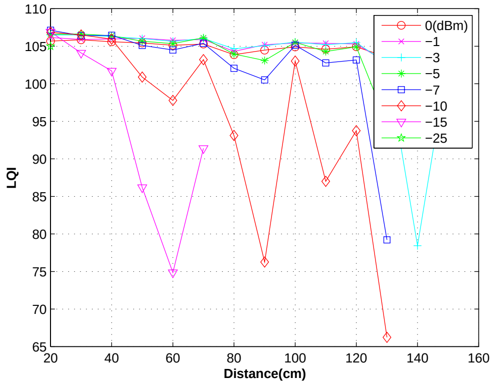


(B)

Fig. 4. Measured RSSI value with different transmission power and distance. (A) is illustrated depending on transmission power , (B) on distance basis.

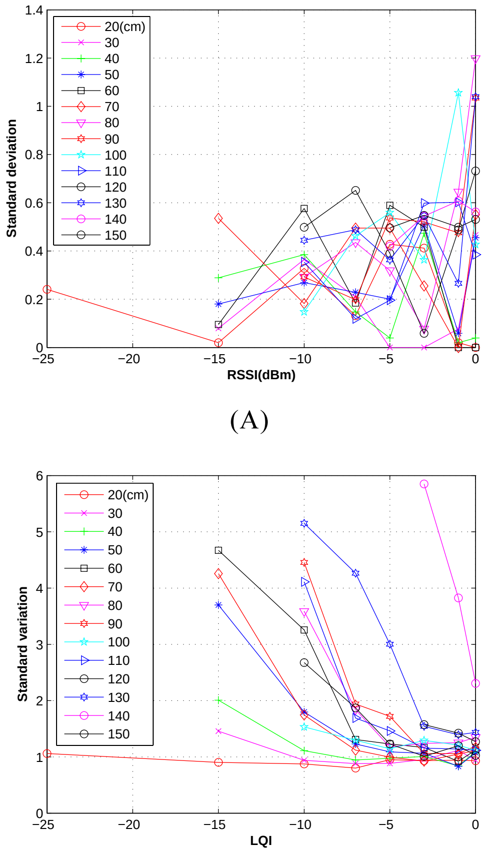


(A)



(B)

Fig. 5. Measured LQI value by different transmission power and distance. (A) is illustrated depending on transmission power, (B) is on distance.



(A)

(B)

Fig. 6. Standard deviation of RSSI (A) and LQI (B).

The standard deviation of RSSI and LQI is illustrated in Figure 6. RSSI and LQI are easily influenced by environment so an error is added to the measured information. Therefore, we need to set an acceptable error range and determine the Sybil node with range of RSSI, LQI based on their standard deviation.

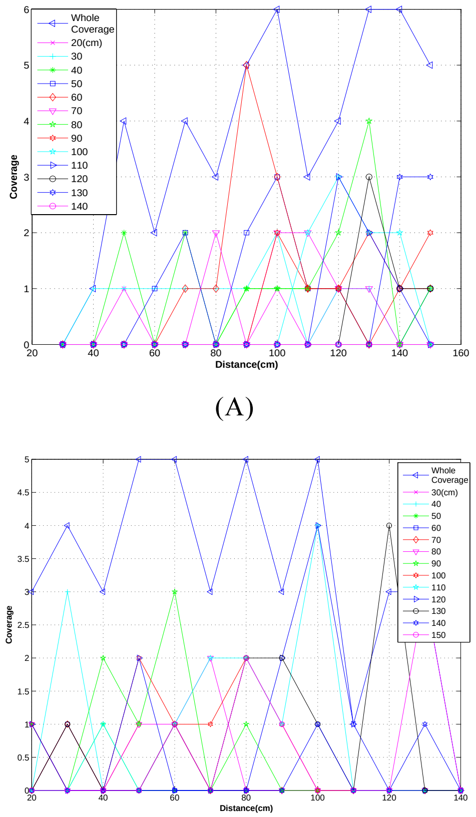
We set the two Sybil attack models to evaluate the proposal. We judged the success of impersonation depending on following procedures.

TABLE III
SYBIL ATTACK DETECTION PROCEDURE.

```
If((Estimated RSSI-Sybil RSSI)<standard deviation of RSSI
and (Estimated LQI-Sybil LQI)< standard deviation of LQI)
                    Sybil_Attack_is_occured;
Else{}
```

Firstly, Sybil node is placed between monitoring and ordinary node and generates seven transmissions with different power. (8th transmission power is not used in the experiment because it does not show proper transmission rate) In the case, we can test the situation that Sybil node located in a short distance generates the sensor node's transmission in a long distance. The Figure 7(A) shows the results. The maximum number of success is six and all nodes failed in impersonating the ordinary sensor node at different location.

Secondly we placed the Sybil node in a long distance and tried to impersonate the sensor node in a short distance. The results are illustrated in Figure 7(B). In this case, the possibility of impersonation is much lower than the first case. The results show that impersonating the range of transmission power is difficult in different locations.



(A)

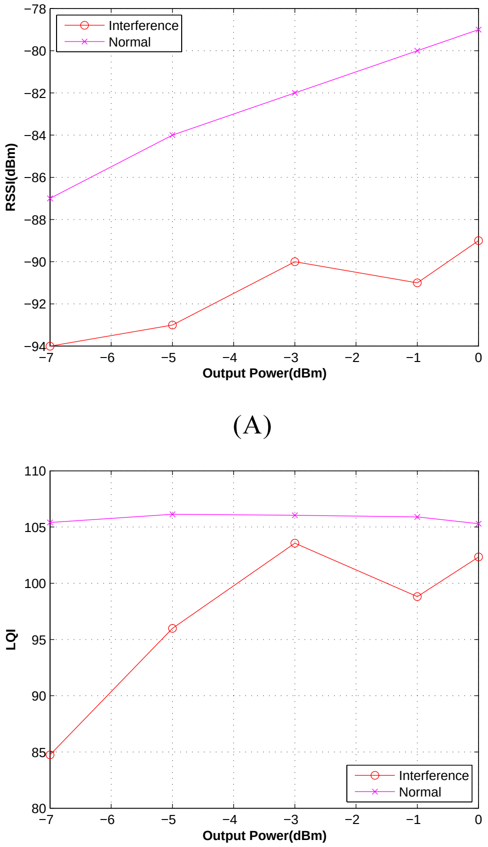
(B)

Fig. 7. Coverage of the transmission power based on distance between monitor and sensor node. (A) is a coverage when Sybil node impersonate the ordinary node in a long distance. (B) is a coverage when Sybil node impersonate the ordinary node in a short distance.

B. Signal interference

Figure 8 (A, B) shows comparison of the RSSI and LQI value depending on ordinary and signal interference case. To make a signal interference case, we installed the obstacles around node. When signal interference occurred, RSSI and LQI values fluctuated. Therefore, the detection algorithm in signal interference case is prone to misjudge the Sybil node due to irregularity of signal strength. However even though RSSI and LQI are changed, their variations are maintained in constant value so we can aware the situation that is signal interference or ordinary case through following equation.

$$Difference = Difference + |Normal\_variation - interference\_variation| \quad (1)$$



(A)

(B)

Fig. 8. Measured RSSI and LQI value in case of normal and signal interference. (A), (B) describe the RSSI and LQI value depending on transmission power respectively.

We measured RSSI and LQI at both cases, the ordinary and signal interference in case of 70cm. The experiment results are illustrated in Figure 9. We found that the results do not provide the perfect information of signal interference but through the information, we can predict the sensor node because difference of variation in RSSI and LQI present the average of results.

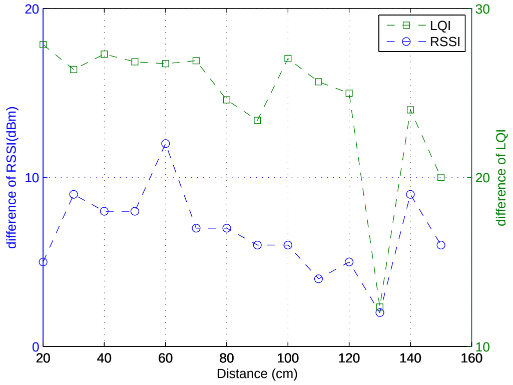


Fig. 9. Difference of variation in RSSI and LQI.

V. CONCLUSION

The paper presents the novel approach in Sybil attack detection based on different transmission power strengths and range of transmission power strengths. Previous proposals do not consider about transmission power modulation for impersonating the ordinary sensor nodes. For this reason, existing methods are vulnerable to the Sybil attack. On the contrast, our proposal distinguishes the Sybil attack which conducts the transmission power modulation, checking the range of transmission capability and each node's RSSI and LQI value depending on its' unique location.

The method is also effective to checking the signal interference case. If we determine the Sybil attack based on RSSI and LQI value in case of signal interference, we are prone to misjudge the Sybil attack because the values easily fluctuated due to influence of obstacles and environment. To determine the condition, we compared the difference between ordinary and interference condition because the variation of RSSI and LQI values are maintained. However, signal interference detection is not proper level for practical implementation in terms of accuracy. Therefore, we need to enhance the method to determine the case more accurately.

ACKNOWLEDGMENT

"This work was supported by the National Research Foundation of Korea(NRF) grant funded by the Korea government(MEST) (No.2010-0026621)."

REFERENCES

[1] T. Karalar and J. Rabaey., An rf tof based ranging implementation for sensor networks, in Communications, 2006. ICC '06. IEEE International Conference on, (2006), 3347–3352

[2] S. Gezici, Z. Tian, G. Giannakis, H. Kobayashi, A. Molisch, H. Poor, and Z. Sahinoglu, Localization via ultra-wideband radios: a look at positioning aspects for future sensor networks, Signal Processing Magazine, IEEE, (2005), 70–84.

[3] A. Nasipuri and K. Li, A directionality based location discovery scheme for wireless sensor networks, in WSNA ’02: Proceedings of the 1st ACM international workshop on Wireless sensor networks and applications. (2002), 105–111

[4] R.-H. Wu, Y.-H. Lee, H.-W. Tseng, Y.-G. Jan, and M.-H. Chuang, Study of characteristics of rssi signal, in Industrial Technology, 2008. ICIT 2008. IEEE International Conference on, (2008), 1–3.

[5] J. R. Douceur., The sybil attack, In IPTPS ’01:Revised Papers from the First International Workshop on peer-to-peer systems, (2002), 251-260.

[6] Fereshteh Amini, Jelena Mišic, and Hossein Pourreza., Detection of Sybil attack in beacon enabled IEEE 802.15.4 Networks., Wireless Communications and Mobile Computing Conference, 2008. IWCMC’08. International, (2008), 1058-1063.

[7] M. Demirbas and Y. Song., An RSSI-based Scheme for Sybil Attack Detection in Wireless Sensor Networks., International Symposium on a World of Wireless, Mobile and Multimedia Networks, (2006), 564-570.

[8] L. Shaohe, W. Xiaodong, Z. Xin, Z. Xingming, Detecting the Sybil Attack Cooperatively in Wireless Sensor Networks, Computational Intelligence and Security, 2008. CIS ’08. International Conference on, (2008), 442-446.

[9] ChipCon Inc. http://www.chipcon.com

[10] J.L. Hill, D.E. Culler, Mica: A wireless platform for deeply embedded networks,IEEE Micro 22 (6) (2002) 12‐24.

[11] M. Corporation, Tmote sky:Ultra low power IEEE 802.15.4 compliant wireless sensor module data sheet, (2006).

[12] G.Zhou, T.He, S. Krishnamurthy, and J. A. Stankovic. Impact of radio irregularity on wireless sensor networks., In MobiSys ’04: Proceedings of the 2nd international conference on Mobile systems, applications, and services, (2004), 125-138

[13] TinyOS, http://www.tinyos.net/

Hwajeong Seo He received the BSEE degree from Pusan National University, Pusan, Republic of Korea in 2010 and he is in MS degree in Computer engineering from Pusan National University. His research interests include sensor network, information security, Elliptic Curve Cryptography and RFID security. He is a member of IEEE.

Howon Kim He received the BSEE degree from Kyungpook National University, Daegu, Republic of Korea, in 1993 and the MS and PhD degrees in electronic and electrical engineering from the Pohang University of Science and Technology (POSTECH), Pohang, Republic of Korea, in 1995 and 1999, respectively. From July 2003 to June 2004, he studied with the COSY group at the Ruhr-University of Bochum, Germany. He was a senior member of technical staff at the Electronics and Telecommunications Research Institute (ETRI), Daejeon, Republic of Korea. He is currently working as an assistant professor with the Department of Computer Engineering, School of Computer Science and Engineering, Pusan National University, Busan, Republic of Korea. His research interests include RFID technology, sensor networks, information security, and computer architecture. Currently, his main research focus is on mobile RFID technology and sensor networks, public key cryptosystems, and their security issues. He is a member of the IEEE, and the International Association for Cryptologic Research (IACR).