EAI Endorsed Transactions
on Industrial Networks and Intelligent Systems
Research Article EAI.EU

A Secure Authentication Scheme based on Brownian Motion in hierarchy Wireless Sensor Networks

Minh Hoang Trong*, Ngoc Le Van, Nguyen Lang Tuan, Hai Hoang Dang[1]

[1]Posts and Telecommunication Institute of Technology, Hanoi, Vietnam hoangtrongminh@ptit.edu.vn

Abstract

In the last few years, the Internet of Things (IoT) has experienced exponential advancements. In IoT infrastructures, Wireless Sensor Network (WSN) has been considered as one of the crucial technologies to support a lot of amazing services. To fulfill new requirements of deployed network environments, the security issue in wireless sensor networks has to be met new challenges such as secured and lightweight requirements simultaneously. Hence, in this paper, an authentication scheme based on the watermarking technique is proposed to secure the sensory data in hierarchy wireless sensor networks. Especially, natural movement characteristics of a sensor node are exploited to provide a conveniently watermarked data, that can be used to validate and detect data integrity attacks in familiar methods. The proposed authentication scheme is evaluated by numerical results and theoretically analyzed to prove a proposal efficiency.

Received on 06 September 2019; accepted on 19 September 2019; published on 24 September 2019

Keywords: wireless sensor networks, authentication, Brownian motion, watermark technique

Copyright © 2019 Minh Hoang Trong *et al.*, licensed to EAI. This is an open access article distributed under the terms of the Creative Commons Attribution license (http://creativecommons.org/licenses/by/3.0/), which permits unlimited use, distribution and reproduction in any medium so long as the original work is properly cited.

doi:10.4108/eai.13-7-2018.160389

1. Introduction

Wireless sensor network (WSN) is a vital technology for IoT applications since it is widely applied to collect and monitor various physical parameters[1][2]. In a distributed sensor networks, a sensor node is normally constrained by the power supply and physical size that leads to a poor security capacity [3][4][5]. Furthermore, Security of wireless sensor networks becomes a critical issue in some practical cases such as scientific exploration in civil operations, battlefield surveillance in military, security monitoring, target tracking or health care system [4][5].

To save network energy, a WWSN is regularly configured in a hierarchy topology. In this network type, several sensor nodes are formed to a cluster to aggregate sensed data before forwarding to the sink node. Unfortunately, attackers can have a chance to attack either data link between a cluster head and the sink node or sensor nodes[6]. In literature, watermarking has been recognized as a promising approach for ensuring authentication, privacy, and digital copyrights protection in WSN environment due to its lightweight processing as compared with the other conventional approach [7][8]. This approach helps to hide useful information in sensed data sources appeared on an image form, then is easily processed by varied image processing methods[12].

In this paper, a novel lightweight authentication scheme based on watermarking techniques is proposed. In which, the watermark data for authentication is extracted naturally from Brownian motion characteristic of the sensor agent node. Because every collected sensory data is reflected as a pixel intensity, the watermarked data is created as an image matrix which is secured for data transmissions. The proposed scheme is validated by both numerical results and theoretical analysis.

The rest of this paper is organized as follows. Section 2 presents typical related work for watermarking and authentication in WSNs. In Section 3, we present the background for our new method. Section 4 devotes to the proposed watermarking scheme. Section 5 provides a performance evaluation and Section 6 concludes the paper.

2. Related work

Security for wireless sensor networks has received much attention in recent years due to their important roles in IoT area [3][1][13]. In which, authentication has been evolved to many security mechanisms such as network access control, key distribution or data protection. In [13]-[18], authentication has been emphasized as a key protection mechanism for controlling network/device access. it enables sensor nodes to verify themselves and ensures that authorized devices are given appropriate right to access to devices/networks. Authentication

process combining with access control is proposed to enhance device protection features in heterogeneous sensor networks [15] [16]. An identity authentication model was proposed in [17], which composes both a public key distribution technique and a lightweight protocol for securing device communications. In IoT environments, the lightweight property of a secure mechanism tends to the critical point of energy saving aims in case of multiple constrained conditions such as transmission technology limitations and computational capacity of IoT devices[18] [14]. To reach this aim, the authors in [20] proposed a cooperation concept, in which mobile sensors act with static nodes to handle failures of static sensor networks by filling faulty gaps. According to the indicated works, network topology for authentication scheme can be derived, in which a mobile node can act as agent node that cooperates with other static nodes to get local authentication information in passive ways. This information will be a part of watermarked data that can be used for secure authentication.

On the other hand, watermarking techniques can be used for many applications that require some degree of security such as tamper detection, ownership protection, etc. The authors in [21] proposed using watermarking to recognize the authorship by imposing additional constraints during data acquisition processes and/or data processing. In this paper, the authors show that the spread spectrum technique can be used for the watermarking progress by various transformations and simple embedding operations. The watermarking approach in [22] is proposed for data authenticity and integrity targets. This proposal focuses on reducing watermark payload and computational complexity through the semi-blind technique. The watermark can be embedded directly into the original data in order to reduce the complexity of this scheme. However, any mediated node can check authentication by comparing original watermark and extracted watermark, thus, the watermark can be exploited by attackers. Especially, the authors in [23] presented a method for visualizing gathered data as an image. In this scheme, sensor nodes collect data from the whole network at a certain time snapshot. Each sensor node presents a pixel on the image with its collected data representing the pixel intensity. The watermark bits are spread based upon orthogonal pseudo-random modulation pulses to avoid interfering. However, watermark data is chosen randomly that needs to comfort with the network's image matrix.

Intuitively, one of the shortcomings of watermark-based authentication is the provision of two-way authentication. Sensor nodes are recognized by the database, but they cannot verify whether or not their data accurately reaches the expected database. This problem can be mitigated by a lightweight authentication scheme that combines both initial authentication phase and final authentication phase in a sensor node and base station respectively [24], where key generation is the important criterion for a securing model. Key generated from dynamic and random properties is well suited to cryptographic key generation in IoT applications [25]. Thanks to the strongly random characteristic of Brownian motion, this information is utilized to create an appropriated dynamic key for authentication schemes [26]. Hence, in this paper, the watermark data is extracted from average distance between a Brownian node and the virtual root in a geographic network area. Since local sensor nodes have only known a part of location information of the Brownian node, the scheme can provide enhanced security protection for watermark data. Moreover, an appropriate two-way authentication scheme is proposed to protect the Brownian node itself which is validated by overall security analysis.

3. Preliminaries

3.1. Assumptions

Without loss of generality, we assume a wireless sensor network is deployed in a planar area where static sensor nodes are assumed to be distributed in a grid network topology. In a hierarchy configuration, several sensor nodes are formed into a cluster which has an aggregation node called a cluster head. It is responsible for collecting sensory data from its group for keeping network energy-efficiency. A Brownian sensor node is called an agent node that moves in the planar as a two-dimensional Brownian motion model [27]. This moving action is commonly in dynamic environments such as underwater or molecular sensor networks. Assume that the examined WSN is a k-covered and homogeneous network [28]. As depicted in Fig.1, a transmission range of the sensor node is $r = l\sqrt{2}$ and the distance between two sensor nodes is estimated by a practical power measurement.

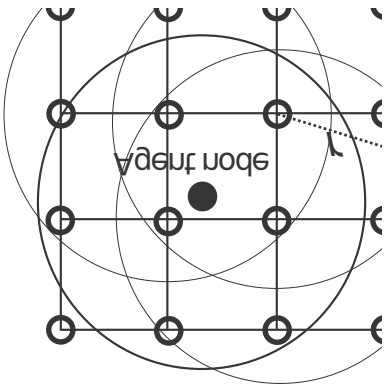

Figure 1. The exampled grid network topology

According to [29] [30], we assume that only the sink node has a location information database of sensor nodes which come from a physical system such as a global position system (GPS).

3.2. Characteristics of the agent node

An agent node has moved freely in a planar of wireless sensor network deployed. Let an agent sensor movement be presented as $m(t) = (w_1(t), w_2(t))$, where $w_1(t)$ and $w_2(t)$ represent the position of a point m in the Cartesian coordinates (x-axis and the y-axis) at time t. We assume that $w_1(t)$ and $w_2(t)$ is the one-dimensional Wiener processes that satisfy the following characteristics:

1. $w_t = 0$ almost surely;
2. w_t has independent increments, i.e. with $0 \leq t_1 \leq t_2 \leq ... \leq t_n$, the increments $w_{t_n} - w_{t_{n-1}}, w_{t_{n-1}} - w_{t_{n-2}}, ..., w_{t_2} - w_{t_1}$ are independent random variables;
3. w_t has Gaussian increments. Thus, $w_{t+h} - w_t, h \geq 0$ is normally distributed with mean 0 and variance h, i.e. $w_{t+h} - w_t \sim \mathcal{N}(0, h)$;
4. w_t has a continuous path; it is continuous in t almost surely.

As specified in [31], the wiener process that specifies Brown motion is closely linked to the normal distribution. Since the probability distribution function follows the normal distribution with $(\mu = 0, t)$, we have the probability distribution function of the wiener process as follows.

$$F_{w_t}(x) = \mathrm{P}(w_t < x) = \frac{1}{\sqrt{2\pi t}} \int_{-\infty}^{x} e^{-\frac{u^2}{2t}} du, \tag{1}$$

for all $x \in \mathbb{R}$. Therefore, the coordinates of an agent node m within a time interval are the random variables. their probability distribution function is formed to a Gaussian distribution. Moreover, we can recognize that the maximum variable of its coordinates is approximated a Gaussian distribution too. This is proven by a lemma 1 bellows.

Lemma 1: Let $X \sim \mathcal{N}(\mu_1, {\sigma_1}^2)$ and $Y \sim \mathcal{N}(\mu_2, {\sigma_2}^2)$ are two normal distributed variables. Then $Z = \max\{X, Y\}$ is approximated a Gaussian distribution.

Proof:

Let X and Y be two independent random variables, we can determine the cumulative distribution function of Z as follows:

$$\begin{aligned} F_Z(x) &= \mathrm{P}(Z < x) = P(X < x \cap Y < x) \\ &= P(X < x).P(Y < x) = F_X(x).F_Y(x). \end{aligned} \tag{2}$$

Since X and Y follows the Gaussian distribution, thus

$$\begin{aligned} F_Z(x) &= F_X(x).F_Y(x) \\ &= \left(1 - \Phi(\tfrac{x-\mu_1}{\sigma_1})\right).\left(1 - \Phi(\tfrac{x-\mu_2}{\sigma_2})\right). \end{aligned} \tag{3}$$

where $\Phi(x) = \int_x^{+\infty} \frac{1}{\sqrt{2\pi}} e^{-\frac{t^2}{2}} dt$. According to [32], the probability density function of Z is given by

$$\begin{aligned} f_Z(x) &= \tfrac{1}{\sigma_1}\Phi(\tfrac{x+\mu_1}{\sigma_1}).\Phi(-\tfrac{x+\mu_2}{\sigma_2}) \\ &+ \tfrac{1}{\sigma_2}\Phi(\tfrac{-x+\mu_2}{\sigma_2}).\Phi(-\tfrac{-x+\mu_1}{\sigma_1}). \end{aligned} \tag{4}$$

We can calculate the expected value of Z as follows:

$$\begin{aligned} E_Z(x) &= \textstyle\int_R x f_Z(x) dx = \mu_1 \Phi(\tfrac{\mu_1-\mu_2}{\sqrt{{\sigma_1}^2+{\sigma_2}^2}}) + \\ &\mu_2 \Phi(\tfrac{\mu_2-\mu_1}{\sqrt{{\sigma_1}^2+{\sigma_2}^2}}) + \sqrt{{\sigma_1}^2 + {\sigma_2}^2}\Phi(\tfrac{\mu_1-\mu_2}{\sqrt{{\sigma_1}^2+{\sigma_2}^2}}). \end{aligned} \tag{5}$$

We can determine the second moment of Z as

$$\begin{aligned} &\textstyle\int_{x^2 f_Z(x) dx} = \sqrt{{\sigma_1}^2 + {\mu_1}^2}\Phi(\tfrac{\mu_1-\mu_2}{\sqrt{{\sigma_1}^2+{\sigma_2}^2}}) + \\ &\sqrt{{\sigma_2}^2 + {\mu_2}^2}\Phi(\tfrac{\mu_2-\mu_1}{\sqrt{{\sigma_1}^2+{\sigma_2}^2}}) + \\ &(\mu_1 + \mu_2)\sqrt{{\sigma_1}^2 + {\sigma_2}^2}\Phi(\tfrac{\mu_2-\mu_1}{\sqrt{{\sigma_1}^2+{\sigma_2}^2}}). \end{aligned} \tag{6}$$

The variance of Z is given by the following expression:

$$V_Z(x) = \int_{x^2 f_Z(x) dx} - E_z^2(x). \tag{7}$$

We can conclude that the variance of $Z = \max\{X, Y\}$ is the approximated Gaussian distribution with main parameters in equations (4) (5) (6). Moreover, the cumulative distribution function of Z simulated by numerical results that validates these similar characteristics (Fig.2).

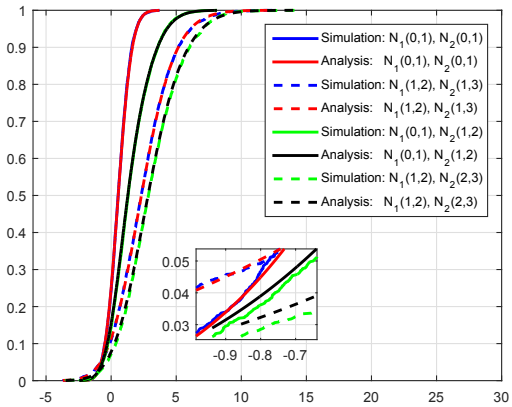

Figure 2. The CDF with varied parameters of Z

4. The proposed secure authentication scheme

4.1. Watermark process

The proposed watermark process based on image processing composes two parts as shown in Fig.3. On the cluster head side, an image reflected sensor data of

its group is created as a data image, its size is depended on a number of sensors in the cluster. In reality, to enhance energy-efficient utility, a cluster is formed as equal cluster size or unequal cluster size that depends on a practical routing strategy. The watermark data generated by measuring the maximum distance of agent nodes and sensor nodes is embedded in the data image that forms a watermarked data. On the sink node side, watermark data is extracted to verify the agent node authentication and sensory data integrity.

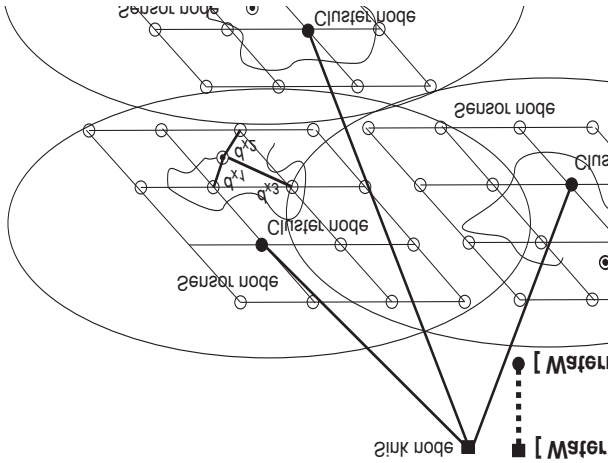

Figure 3. Illustration of a watermarking process

In this scheme, only the sink node has known a real position of the agent node while every sensor node having a part of three coordinated parameters. Hence, by a simple embedding procedure, the watermark data is secured overtime then against masquerade attacks. Moreover, the cluster head can use advantage transform techniques to reduce data size for saving data transmit energy. Denote $d\,(x, y)$ the embedded watermark data at the cluster node, we have $d\,(x, y) = o_i + b_i \times p(x, y) \times d_t$. In this equation, o_i represents an original data value of a static WSN node, b_i presents the watermark bit, $p(x, y)$ is a pseudo-random value, and d_t is a watermark data that presents the coordinates of the mobile WSN node at time t, $d_t = \max\{X_t, Y_t\}$. To detect the watermark, we follow the approach proposed in [23]. This method considers watermark presence conditions based on the statistical characteristics of the correlation coefficients. Using this approach, we investigate all transform cases to reveal the conditions for watermark detection through the following formula:

$$\sum_{i=1}^{L} b_i r_i \leq\geq erfc^{-1}(p_f)\sigma\sqrt{L}, \tag{8}$$

where r_i are the correlation coefficients, b_i are watermark bits, $erfc$ is the complementary error function, p_f is the fixed false alarm probability and L is the length of the watermark sample.

4.2. The proposed two-way authentication procedure

To prevent counterfeit attacks by releasing malicious motion nodes into the network, assume that the Brownian motion node has a unique identification (id) which can be detected by the sink node and sensor nodes. Obviously, adverse conditions with the misbehavior of spurious motion nodes will cause a falseness in the distance measured by each fixed node. Thus, at each round, the agent node needs to send its id value and the distance value of the communicated nodes simultaneously. This information will match with the collected information at the cluster head node and be authenticated at the sink node as analyzed above.

However, it is a disturbing matter to authenticate the agent node because it can be completely forged, and the agent node itself can not validate the static sensor node which it wants to exchange information. This is the drawback of the proposed watermark mechanism when two-way data authentication is not provided. To overcome this limitation as well as reduce the cost authentication by the third party, the agent node and other sensor nodes should establish the session keys compromised to authenticate each other. As pointed out before, keys generated from characteristic features of the naturally dynamic channels such as wireless sensor networks are appropriate to low-cost devices. Therefore, we propose modified key generation algorithms which encoding bits are based on mean and standard deviation values [34].

For the sake of simplicity, we assume that the agent node is more powerful than conventional sensor nodes in terms of energy, memory and computational ability when it can be self-locating at all times. Firstly, we use a data value which relied on the position of the agent node at the s^{th} session to generate keys (Algorithm 1, INPUT). Proximity thresholds are based on expected values and deviation values of the received data (Algorithm 1, line 1-2), with the threshold adjustment coefficient, α. Accordingly, the encryption bits for a session key are quantized (Algorithm 1, line 3-6). The location information of the agent node in the s^{th} session is the basis for key generating for the $(s+1)^{th}$ session, as this information is only known by such pair of nodes through authentication and getting information from the sink node. The computational complexity of calculating the mean and variance is $O(n)$.

Algorithm 1: Key generation Algorithm
INPUT: $Z_s = \max\{X_s, Y_s\}$ (Agent node coordinators)
OUTPUT: k_s (Session Key)
1: $\eta_+^u = E(Z_s) + \alpha\sqrt{V_Z^s}$ (η_+^u: a positive threshold)
2: $\eta_-^u = E(Z_s) - \alpha\sqrt{V_Z^s}$ (η_-^u: a negative threshold)
- - - - - - - - - - - - - - (V_Z^s is a variance of Z_s)
3: for $i \leftarrow 1$ to n do

4: if $Z_s(i) \geq \eta_+^s$ then $k_s = 1$
5: else if $Z_s(i) \leq \eta_-^s$ then $k_s = 1$
6: else $k_s = 0$ (Key dropped)
7: End if
8: End for

In the proposed scheme, a session key is generated in every round and verified by Algorithm 1. Assume every node has a unique identification (id); a pairwise key between a sensor node and the sink node is predefined, k_p [35]. k_p is a symmetric key reserved for examining a trusted sensor node in an authenticate phase. Note that, a cluster head is voted in every round that depends on how is better energy than its members. In the data collection phase, sensory data is aggregated at the cluster head. The whole process is described by the schema as in Fig.4.
(1) At the first step, the agent node a (mobile node) sends its identification (id_a) and its distance d_{na} of the node a and a sensor node wanted to connect, node n. the distance can be estimated by received signal power. $M(1) = a \rightarrow n : (id_a \| d_{na})$.
(2) a sensor node n compares its distance value d_{an} with its d_{na} received. If $d_{an} = d_{na}$ then it is validated the exact sensor node which communicates to. Node n does the XOR operand of the node id_a and the node id_n before encoding by predefined key (k_p), this message is sent to the sink node. $M(2) = n \rightarrow S : k_p(id_n \oplus id_n) \| d_x$.
(3) The sink node has already k_p,id_a and id_n in its database, it can verify an agent node id_a. Moreover, the location information of a agent node is determined by several sensor nodes in this round s, Z. Based on location parameter Z, the sink node generates a new session key k_s as presented in logarithm 1. The sink node sends its id_s and watermark threshold to agent node through a sensor node n. $M(3) = s \rightarrow n : k_p(id_s, Z)$.
(4) a sensor node n authenticates the sink node id_s, then passes the location information to an agent node.$M(4) = n \rightarrow a : Z \| (id_n \oplus id_s)$. The agent node a uses received value Z to generate a session key k_s.
(5) Node a grants this communication path between an agent node, a sensor node and the sink node is safety. It sends back a session key k_s to sensor node n to use as new session key to protect data between the node n and the node s.

5. Security analysis and validation

5.1. Numerical results

To simulate our proposed watermark scheme, a Gaussian generation function in Mathlab tools is used to create a sensory data matrix, ($8x8$) [12]. The average values of 10.000 Gaussian random processes are formed to a normal distribution. A watermark data is extracted from movement characteristic of the agent node. Assume that it has a random coordination

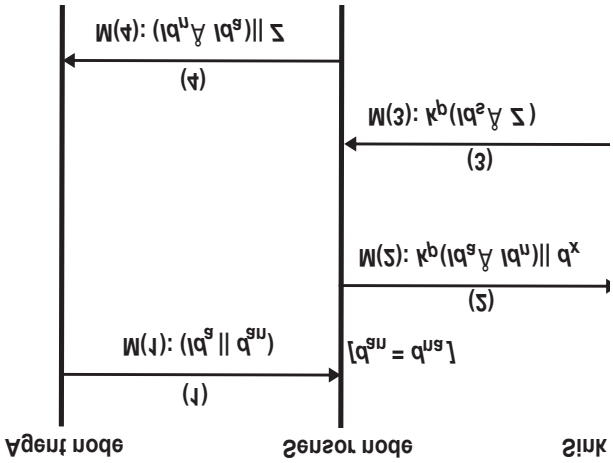

Figure 4. Two-way authentication scheme

without drift following time t, $dx(t) = \sigma_x dw_1(t)$ and $dy(t) = \sigma_y dw_2(t)$. In this context, $w_1(t)$ and $w_2(t)$ are independent Wiener processes in one dimension. σ_x and σ_y are diffusion coefficients of the Brownian motion coordinators, respectively.
Figure 5 shows the intensity of the watermark data versus diffusion coefficients of the agent node, the surface plot represents the case in which these diffusion coefficients are different in the coordinate (i.e. $\sigma_x \neq \sigma_y$) and the other represents the symmetric case, it means that they have the same diffusion coefficient (i.e. $\sigma_x = \sigma_y$). The results show that with a diffusion coefficient of less than 20, the watermark intensity does not exceed 12.

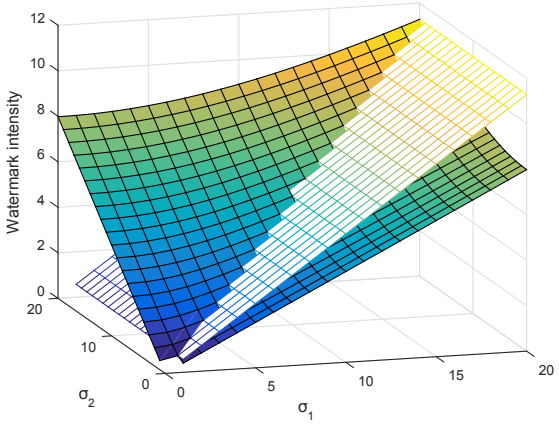

Figure 5. Watermark detection probability vs diffusion coefficients

5.2. Watermark vulnerable detection analysis

A fundamental limitation of the traditional authentication scheme based on watermark data is that the sink node can not accurately detect the attacked nodes which

watermarked data is modified across an entire network. Instead, the sink's database only detects whether data is being tapped or not based on the probability of watermark detection. Therefore, we propose a method for determining interfered nodes relied upon the random characteristics of Brownian motion in the watermark-based authentication model.

Definition 1: Let $d_i(s)$ is the deviation of the probability density function of original data and received data, then we have:

$$\begin{array}{ll} d_i(s) > T_h & \text{node i is attacked} \\ \mathrm{d_i(s)} \le \mathrm{T_h} & \text{otherwise.} \end{array} \tag{9}$$

where T_h is a detection threshold.

Proclamation 1: Modified watermark data can be detected by Definition 1.

Proof would be presented by Lemma 2.

Remark 1: Suppose that a function $f(x)$ is infinitely differentiable on R, then $f(x)$ can be rewritten as

$$f(x) = P_n(x) + R_n(x) \tag{10}$$

In which, $P_n(x) = \sum_{k=0}^{n} a_k(x-\mu)^k$ *and* $R_n(x) = \frac{f^{(n+1)}(c)}{(n+1)!}(x-\mu)^{n+1}$ with $c \in R$ is between μ and x.

Lemma 2: If $\varepsilon > 0$ and $f(x) = \frac{1}{\sqrt{2\pi}\sigma} e^{-\frac{(x-\mu)^2}{2\sigma^2}}$, then existing $g(x) := \frac{1}{\sqrt{2\pi}\sigma} - \frac{1}{2\sqrt{2\pi}\sigma^3}(x-\mu)^2$ satisfies $|f(x) - g(x)| < \varepsilon$, for all x $\in R$.

Proof:

Because the $f(x)$ function follows a normal distribution, it can be perturbed as follows:

$$f(x) \approx g(x) = a_0 + a_1(x-\mu) + a_2(x-\mu)^2 \tag{11}$$

Equation (11) is equivalent to

$$f(x) = g(x) + R_2(x). \tag{12}$$

We have,

$$\begin{aligned} a_0 &= f(\mu) = \frac{1}{\sqrt{2\pi}\sigma} \\ a_1 &= \frac{f'(\mu)}{1!} = 0 \\ a_2 &= \frac{f''(\mu)}{2!} = -\frac{1}{2\sqrt{2\pi}\sigma^3} \\ R_2(x) &= \frac{f'''(c)}{3!}(x-\mu)^3 \end{aligned} \tag{13}$$

in which

$$f'''(c) = \frac{(c-\mu)(3-(c-\mu)^2)}{\sqrt{2\pi}\sigma^5} e^{-\frac{(c-\mu)^2}{2\sigma^2}}.$$

and $c \in R$ is between μ and x.

We have

$g(x) = a_0 + a_1(x-\mu) + a_2(x-\mu)^2$

$= \frac{1}{\sqrt{2\pi}\sigma} - \frac{1}{2\sqrt{2\pi}\sigma^3}(x-\mu)^2.$

From equation (12), we have:

$$\begin{aligned} R_2(x)| &= \left|\frac{f'''(c)}{6}(x-\mu)^3\right| < \varepsilon \\ \varepsilon &= \begin{cases} \frac{f'''(c)\mu^3}{6} \text{if} x < \mu \\ \frac{f'''(c)x^3}{6} \text{otherwise} \end{cases} \end{aligned} \tag{14}$$

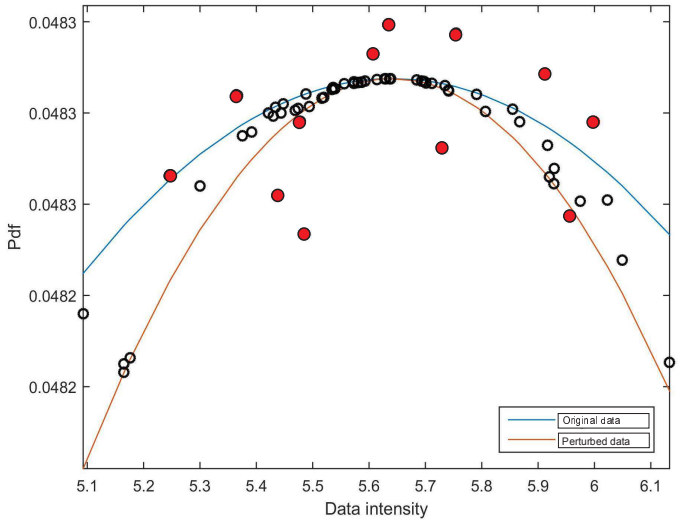

Figure 6. Watermark vulnerable probability

Recall that, the original watermark data is created by Brownian motion characteristic. Hence, the probability density function of original watermark data is illustrated as the green line in Fig.6. The diffusion coefficients of the Brownian motion node are demonstrated its behavior, they affect directly to maximum perturbation of the watermark data change. In this example, the diffusion coefficient is set as 10 and presented by the red line. As proven in Lemma 2, the green line is illustrated upper bound of the received watermarked data and the red line is illustrated lower bound of the received watermark data. As shown in Fig.6, the watermark data has been attacked when its probability density function is outside of two lines. In other word, the watermark data in the allowable threshold if the probability density function of its intensity lies in the radius perturbations of original data.

5.3. Complexity evaluation

As mentioned above, in many IoT applications, sensor nodes are often restrained by power, memory and computing capacity. According to common mechanisms, in every round, the agent node needs to send its distance information to the sink node. It seem to be unreasonable for a larger network when an agent node sends a request to join the session every time it wants to communicate. Instead of sending multiple requests for multiple sessions, the agent node just only communicates with a

sensor node which is located in its transmission range. When a agent node moves to a new location, a newly sensible sensor node becomes a new candidate sensor to make a new communication process. As the result, the cost for sending communication requests is ameliorated.

In Brownian motion case, the time interval which an object firstly goes out of a circular area is called first hitting time of circle. In our model, first hitting time $t_h = t_L(a, r_t)$ is defined as the first time the Brownian motion node a reaches out the transmission area radius r_t of a sensor node, n.

Lemma 3: With an agent node a,

$$\begin{aligned} &E[t_L(a, r_t)] < \infty; \\ &t_L(a, r_t) \stackrel{\Delta}{=} \inf\{t > t_0 \geq 0 : d(t) \geq r_t | d(t_0) < r_t\} \end{aligned} \tag{15}$$

in which $d(t)$ and $d(t_0)$ are the distances between the agent node a and the sensor node n at time t_0 and t.

Lemma 4: If $\sigma_a > 0$ is the diffusion coefficient of a Brownian node a then,

$$E[t_L(a, r_t)] = \frac{r_t^2 - d(t_0)}{2\sigma_a^2} \tag{16}$$

Proof:

In [36], the authors presented the result of joint distribution of the first hitting time and its location of a Brownian motion rambling in a sphere, which is represented by Lemma 5 below.

Lemma 5: If $0 < x < r_t$ and $s > 0$ then,

$$E\left(e^{-st_h}\right) = \frac{I_0(x\sqrt{2s})}{I_0(r_t\sqrt{2s})} \tag{17}$$

in which $I_0(.)$ is the modified Bessel function of the first kind of order zero.

Applying Lemma 5, it follows

$$E[t_h] = -\frac{\partial}{\partial s} \frac{I_0(\frac{d(t_0)\sqrt{2s}}{\sigma_a})}{I_0(\frac{r_t\sqrt{2s}R_t}{\sigma_a})} | s = 0 \tag{18}$$

Let $\alpha = \frac{d(t_0)}{\sigma_a}$ and $\beta = \frac{r_t}{\sigma_a}$. We have,

$$\begin{cases} I_0(0) = 1 \\ \frac{\partial I_0(z)}{\partial z} = I_1(z); z \in \\ I_0(\alpha\sqrt{2s}) = \frac{2I_1(\alpha\sqrt{2s})}{\alpha\sqrt{2s}} \\ I_0(\beta\sqrt{2s}) = \frac{2I_1(\beta\sqrt{2s})}{\beta\sqrt{2s}} \end{cases} \tag{19}$$

From (18) and (19) we obtain,

$$\begin{aligned} E[t_h] &= \lim_{s\to 0} \frac{\frac{\beta I_1(\beta\sqrt{2s}) I_0(\alpha\sqrt{2s})}{\sqrt{2s}} - \frac{\alpha I_0(\beta\sqrt{2s}) I_1(\alpha\sqrt{2s})}{\sqrt{2s}}}{\left(I_0(\beta\sqrt{2s})\right)^2} \\ &= \lim_{s\to 0} \frac{b^2 I_0(\beta\sqrt{2s}) - \alpha^2 I_0(\alpha\sqrt{2s})}{2} \\ &= \frac{\beta^2 - \alpha^2}{2} \end{aligned} \tag{20}$$

From Lemma 4 we find that the Brownian node will minimize the requesting process as it is closest to a sensor node. Therefore, each time exchanging information with the database the Brownian node needs to select the closest neighbor acting as the forwarding node, and keep the connection with this node until it exits the transmission range of this WSN node, thereby the computational complexity of communication processes is considerable reduced not only for intentional deployment scenarios but also random distribution ones.

6. Conclusion

Authentication is one of the main problems for security assurance in IoT infrastructure, especially in wireless sensor networks. This paper focuses on the security issues of wireless sensor networks under the conditions of limited resources and the heterogeneity of the devices. Using watermarking techniques, we propose a novel lightweight secure authentication scheme for sensor nodes. Our scheme utilizes the natural movement of a Brownian sensor node in order to build the convenience watermark data in a passive way. As the result, our scheme can hide watermark information from local sensor nodes when only the sink node can examine the accuracy of random location parameters. Moreover, a session key is generated from the watermark data that enhance data secure in this network. Beside that, a theoretical analysis and reasonable lemmas to find out the suitable method for realizing a lightweight authentication scheme are presented. Finally, we examine a watermark vulnerable detection analysis for protecting the watermark data through numerical results. In our future work, the proposed authentication scheme can be integrated to a clustered routing protocol to approach to new optimization criteria.

Acknowledgement

This work is the output of the ASEAN IVO project: A Hybrid Security Framework for IoT Networks (http://www.nict.go.jp/en/aseanivo/index.html) and financially supported by NICT (http://www.nict.go.jp/en/index.html)

References

[1] N. Khalil, M. R. Abid, D. Benhaddou and M. Gerndt. Wireless sensors networks for Internet of Things. *IEEE Ninth International Conference on Intelligent Sensors, Sensor Networks and Information Processing (ISSNIP)* **2014**, Singapore, 2014; pp. 1-6.

[2] M. Kocakulak and I. Butun. An overview of Wireless Sensor Networks towards internet of things. *IEEE 7th*

Annual Computing and Communication Workshop and Conference (CCWC) **2017**, Las Vegas, NV, 2017; pp. 1-6.

[3] Y. Zhou, Y. Fang and Y. Zhang. Securing wireless sensor networks: a survey. In *IEEE Communications Surveys & Tutorials*, vol. 10, no. 3, Third Quarter 2008; pp. 6-28.

[4] Li, Mo, et al . A survey on topology control in wireless sensor networks: Taxonomy, comparative study, and open issues. *Proceedings of the IEEE*, 101(12), 2013; pp. 2538-2557.

[5] Sheng, Z., et al. A survey on the ietf protocol suite for the internet of things: Standards, challenges, and opportunities. *Wireless Communications, IEEE*, 20(6), 2013; pp. 91-98.

[6] A. S. Panah, R. van Schyndel, T. Sellis, and E. Bertino. In the shadows we trust: A secure aggregation tolerant watermark for data streams. In *Proc. 16th IEEE Int. Symp. World Wireless, Mobile Multimedia Netw. (WoWMoM)*, Jun, 2015; pp. 1-9.

[7] Ping ping, Y., Suying, Y., Jiangtao, X., Yu, Z. and Ye, C. Copyright protection for digital image in wireless sensor network. In *proceeding of 5th International conference on wireless communications, networking and mobile computing*, 2009; pp. 1-4.

[8] Ingemar J. Cox, Gwenael Doerr and Teddy Furon. Watermarking is not cryptography, digital watermarking. In *Lecture Notes in Computer Science*, 4283, 2006; pp. 1-15.

[9] Farid Lalem, Muath AlShaikh, Ahcene Bounceur, Reinhardt Euler, Lamri Laouamer, Laurent Nana, Anca Pascu. Data Authenticity and Integrity in Wireless Sensor Networks Based on a Watermarking Approach. *FLAIRS Conference* **2016**; pp. 282-287.

[10] X. Sun, J. Su, B. Wang, et al. Digital Watermarking Method for Data Integrity Protection in Wireless Sensor Networks. *International Journal of Security and Its Applications*, vol. 7, no. 4, 2013 July; pp. 407-416.

[11] Y. Ren, Y. Cheng, J. Wang and L. Fang. Data protection based on multifunction digital watermark in wireless sensor network, *International Carnahan Conference on Security Technology (ICCST)* **2015**, Taipei, 2015; pp. 37-41.

[12] H. T. Minh, L. T. Nguyen, N. T. Tra and H. D. Hai, "A study on the sensor network authentication by utilizing a Brownian motion behavior," 2017 International Conference on Information and Communication Technology Convergence (ICTC), Jeju, 2017, pp. 14-18.

[13] C. Vorakulpipat, E. Rattanalerdnusorn, P. Thaenkaew, H.D. Hai, Recent Challenges, Trends and Concerns of IoT Security: An Evolutionary Study. *Proc of IEEE IACT 2018*. Korea, Feb 2018. Best paper award.

[14] H.D.Hai, N.H.Duong, A PCA-based Method for IoT Network Traffic Anomaly Detection, *Proc of IEEE ICACT 2018*. Korea, Feb 2018. Best paper award.

[15] J.Gubbi, R.Buyya, S.Marusic, M.Palaniswami, Internet of Things (IoT): A vision, architectural elements, and future directions, *Future Generation Computer Systems*, 29(7), 2013, pp.16451660.

[16] B.Ndibanje, HJ.Lee, SG.Lee, Security analysis and improvements of authentication and access control in the Internet of Things, *Sensors*, 14(8), **2014**, pp.1478614805.

[17] R.Neisse, G.Steri, IN.Fovino, G.Baldini, SecKit: A Model-based Security Toolkit for the Internet of Things, *Computers and Security*, 54, **2015**, pp.6076.

[18] A.Al-Fuqaha, M.Guizani, etal., Internet of things: A survey on enabling technologies, protocols, and applications, *IEEE Communications Surveys and Tutorials*, 17(4), **2015**, pp.2347-2376.

[19] D.G.Costa, S. Figueredo, G. Oliveira, Cryptography in Wireless Multimedia Sensor Networks: A Survey and Research Directions. *Cryptography* **2017**; pp. 1-4.

[20] E. Pignaton de Freitas et al. Handling Failures of Static Sensor Nodes in Wireless Sensor Network by Use of Mobile Sensors. *IEEE Workshops of International Conference on Advanced Information Networking and Applications* **2011**, Biopolis, 2011; pp. 127-134.

[21] A. Soltani Panah, R. Van Schyndel, T. Sellis and E. Bertino. On the Properties of Non-Media Digital Watermarking: A Review of State of the Art Techniques. In *IEEE Access*, vol. 4, no. , 2016; pp. 2670-2704.

[22] Wang, B., Su, J., Zhang, Y., Wang, B., Shen, J., Ding, Q., & Sun, X. A copyright protection method for wireless sensor networks based on digital watermarking. *International Journal of Hybrid Information Technology*, 8(6), 2015; pp. 257-268.

[23] W. Zhang, Y. Liu, S. K. Das, and P. De. Secure data aggregation in wireless sensor networks: A watermark based authentication supportive approach. *Pervas. Mobile Comput*, vol. 4, no. 5, 2008; pp. 658-680.

[24] Riaz, R., Chung, T. S., Rizvi, S. S., & Yaqub, N. BAS. The Biphase Authentication Scheme for Wireless Sensor Networks. *Security and Communication Networks*, 2017.

[25] Zenger, C.T., Chur, M.J., Posielek, J.F., Paar, C., Wunder, G. A Novel Key Generating Architecture for Wireless Low-Resource Devices. *In Proceedings of the 2014 International Workshop on Secure Internet of Things (SIoT)*,Wroclaw, Poland, 10 September 2014; pp. 26-34.

[26] Zhang, J., Duong, TQ., Woods, R. Marshall, A. Securing Wireless Communications of the Internet of Things from the Physical Layer. *An Overview. Entropy*, 2017 Aug 18;19(8); pp. 420.

[27] Nguyen T, Hoang TM, Lang TN. A study on link quality in single hop sensor networks with Brownian motion. InRecent Advances in Signal Processing, Telecommunications & Computing (SigTelCom), International Conference on 2017 Jan 9 ; pp. 235-239. IEEE.

[28] C.-F. HUANG, Y.-C. TSENG, and L.-C. LO. The Coverage Problem in Three-Dimensional Wireless Sensor Networks. *J. Interconnect. Networks*, vol. 8, no. 3, 2007; pp. 209-227.

[29] N. Bulusu, J. Heidemann, and D. Estrin. GPS-less low-cost outdoor localization for very small devices. *IEEE Pers. Commun.*, vol. 7, no. 5, 2000; pp. 28-34.

[30] D. Niculescu and B. Nath. Ad hoc positioning system (APS). *GLOBECOM'01. IEEE Glob. Telecommun. Conf. (Cat. No.01CH37270)*, vol. 5, 2001; pp. 2926-2931.

[31] Y. Peres. Brownian Motion. *Colloids Surfaces A Physicochem*. Eng. Asp., vol. 106, 2008 pp. 230601.

[32] S. Nadarajah and S. Kotz. Exact distribution of the max/min of two Gaussian random variables. *IEEE Trans. Very Large Scale Integr. Syst.*, vol. 16, no. 2, 2008; pp. 210-212,.

[33] R.C. Gonzalez, R.E. Woods. Digital Image Processing, *Prentice Hall* **2002**.

[34] Mathur, S., Trappe, W., Mandayam, N., Ye, C., Reznik, A. Radio-telepathy: Extracting a secret key from an unauthenticated wireless channel. *In Proceedings of the 14th ACM International Conference on Mobile Computing and Networking (MobiCom)*, San Francisco, CA, USA, 14-19 September 2008; pp. 128-139.

[35] R, Riaz. A Unified Security Framework for IP Based Wireless Sensor Networks [Ph.D. thesis], 2008.

[36] Wendel, J. G. Hitting spheres with Brownian motion. *The annals of probability* **1980**; pp. 64-169.