International Journal of Computer Science and Applications
Vol. 6, No. 3, pp 43 – 56, 2009

A FAULT MANAGEMENT AND MONIROTING MECHANISM FOR SECURE MEDICAL SENSOR NETWORK

Hayoung Oh

Dept. of Computer Science and Engineering,
Seoul National University, Seoul 151-744, Korea
hyoh@popeye.snu.ac.kr

Inshil Doh, Kijoon Chae

Dept. of Computer Science and Engineering,
Ewha Womans University, Seoul 120-750, Korea
isdoh@ewhain.net, kjchae@ewha.ac.kr

Wireless Sensor Network (WSN) is a very attractive technique to support Ubiquitous Pervasive Computing(UPC) such as Medical Sensor Network (MSN) due to many merits such as compact form, low-power, and potential low cost. However, the more the sensor nodes exist, the more difficult the manager monitors sensor nodes individually, and faults of the sensing value are common due to the artificial attackers and the lack of physical protection. Therefore, we propose a key management and distributed abnormal area scanning scheme using spatial, temporal correlation and in-network aggregation for secure MSN. Simulations show that our scheme can clearly identify the abnormal sensors with high accuracy among the existing normal sensors, abnormal sensor, and event-detecting sensors. In addition, we show that the delivery ratio increases under various network environments through the key management scheme.

Keywords: *Medical Sensor Network (MSN), Ubiquitous Pervasive Computing(UPC), Sensor, Fault, Security, Key Management, Normal, Abnormal Sensor Nodes*

1. Introduction

In general, pervasive computing is also named as ubiquitous computing, connected computing devices in the environment [16][18]. Namely, pervasive computing is a convergence of wireless technologies and the Internet [14][15][17]. With the rapid development of wireless technologies and electronics devices, wireless sensor networks (WSNs) which consist of sensing, data processing, and communication components have been attracting technology for Ubiquitous Pervasive Computing (UPC) because of the miniaturization, low-cost, and low-power [1][2]. The tiny sensor nodes can easily be deployed into various environments to form a wireless network and perform environment and habitat monitoring, ecophysiology, condition-based equipment maintenance, disaster management, and emergency response [3]. Recently, for medical purpose, WSN is also applied for Medical Sensor Network(MSN) [22]. However, MSNs and their applications have not been developed with a proper secure management solution considering WSNs characteristics. One important feature that distinguishes sensor networks from traditional systems is unattended and ad hoc nature because of the compact form factor and potential

low cost. Another important feature is that sensor nodes become faulty and unreliable because the working environment where those sensor nodes are deployed might be unpredictable or even vulnerable. It can affect the performance of the network dramatically. It is much more important when the data the sensor devices carry is related to human life. Therefore, in MSN composed of WSNs, among the management function areas such as configuration, performance, fault, security, and bill, fault management considering the security is very important. Especially, since the data processing and communication components provide the targeted level of fault tolerance [5], we only consider the fault of the sensing component problem under the artificial attack.

In most previous fault management approaches, the manager monitors each individual sensor nodes in a centralized manner or each sensor node individually informs its wrong status to manager when it finds own status is wrong. However, due to the WSNs characteristics such as unattended nature, scalability, and limited energy, it is nearly impossible that the managers continuously monitor the explicit knowledge of the overall state of the sensor network. In special, it is very expensive for the manager to collect information from every sensor and identify faulty sensors in a centralized manner. Therefore, we propose a key management and distributed abnormal area scanning scheme using spatial, temporal correlation and in-network aggregation for secure MSN. It provides security for communications between sensor nodes, early warning of abnormal area, and aid in incremental deployment of sensors. This is an enhanced scheme of our previous work [12][13] for secure UPC. For example, sensor node exchanges the encrypted message using MCGA[13] to provide the security during communications between sensor nodes and then the aggregated information distributedly collected by sensor nodes is delivered to a manager. As a result, the manager can scan abnormal area if any part of the network has the problem based on the aggregated information. At last, our scheme can guide incremental deployment of sensors if the additional normal sensor nodes are needed.

In detail, after encrypting the sensing value using MCGA [13], each sensor node exchanges the encrypted sensing value with neighbors. When each sensor node receives the encrypted sensing values, it decrypts the encrypted messages using MCGA and applies the mutual testing method. It means that each sensor node compares the sensing values with neighbors to detect abnormal area using spatial and temporal correlation. Spatial correlation is performed using the value weight per distance weight. Namely, the more distance is near between each sensor node and neighbor, the more the value weight is influenced. As a result, each sensor decides its tendency such as normal or abnormal based on the result of the spatial correlation test step. And then, to distinguish abnormal sensors from event-detecting sensors and to improve the detection accuracy, we consider the temporal relationship between sensor node and neighbors using the variance of the variance according to the time. Finally, our proposed scheme applies an energy-efficient in-network aggregation algorithm for the manager to construct the abnormal area scanning. It may lose the detailed information about each individual node since a few normal sensor nodes may be included to the abnormal area. However, in the huge sensorNet, a little wrong decision is not important. Rather in aspect of scalable management of sensorNet, our abnormal scanning scheme can help managers to monitor sensorNet status at a look and induce to perform the proper execution for secure MSN.

The paper is organized as follows. We first review the related work in Section 2. Then, we define the network model in Section 3. A key management and distributed

abnormal area scanning scheme for secure MSN is proposed in Section 4. Performance evaluation results are presented in Section 5. Finally we conclude the paper in Section 6.

2. Related Work

2.1. *Fault management in sensor networks*

Various schemes to manage faults in wireless sensor networks have been studied. L.B. Ruiz and et al.[7] proposed the failure detection scheme based on the management architecture MANNA. In this scheme, every node checks its energy level and sends a message to manager whenever a change of states occurs. Using the collected information, the manager can determine which node is fault. Two-phase self monitoring system (TP) [8] is an efficient distributed self monitoring mechanism which utilizes two-phase timers for the local coordination and the active probing. In the first phase, a node waits for the updates from neighbors to recognize nodes which do not operate. In the second phase, a node collaborates with its neighbors to clarify a condition to make a more accurate management decision. On-line fault detection technique is proposed in [11] to classify faults in sensor networks. The key idea of this scheme is to consider the impact of readings of a particular sensor on the consistency of multi-sensors fusion. However, these techniques are is inefficient to the scalable sensorNet. The reason is that each sensor nodes should inform the wrong status to the manager individually. The more sensor nodes we deploy, the more cost a network spends for the notification of the status.

M. Ding and et al. [9] suggested a faulty sensor identification algorithm. In this algorithm, each node determines its status based on the difference between its own sensing value and its neighbors' median reading. However, it is possible that the algorithm cannot detect faults as expected when more than half of nodes are faulty or the number of sensor neighbors is even. In [10], J. Chen and et al. designed a distributed localized faulty sensor detection algorithm using the majority voting method. The algorithm consists of two steps. First step is that each sensor compares its own measurement value with neighbors and determines its tendency value (true or fault) based on the number of the sensor neighbors. Second step is that each sensor determines its final status value in the same way of the first step except using the opinions of true-tendency neighbors. However, the algorithm has problems about scalability and overhead due to exchange of information between neighbors. Besides the algorithm cannot detect the faults as expected, if itself and more than half of neighbors are faulty.

2.2. *Key management*

Most previous key management schemes in sensor network do not consider scalability. However, as previously stated, the more sensor nodes exist, the more addresses are needed for identifying each sensor node. In addition, during the communication between sensor nodes, each address of sensor nodes as well as the original message should be encrypted for the security. Therefore, we first apply Cryptographically Generated Addresses (CGA) to the sensor network for scalability and security purpose. CGA describes a method for binding a public signature key to an IPv6 address in the Secure

Neighbor Discovery (SEND) protocol. It is IPv6 address for which the interface identifier is generated by computing a cryptographic one-way hash function from public key and auxiliary parameters. The binding between the public key and the address can be verified by re-computing the hash value and by comparing the hash with the interface identifier. ICMPv6 message followed by IPv6 base header can be protected by the digital signature. Digital signature is performed by signing the ICMPv6 message with the corresponding private key and by attaching the public key and auxiliary parameters to the original ICMPv6 message [21]. The protection works without a certification authority or any security infrastructure [20]. That is to say, CGA specifies a method for securely associating a cryptographic public key with an IPv6 address in the Secure Neighbor Discovery (SEND) protocol [19]. The basic idea is to generate the interface identifier (i.e., the rightmost 64 bits) of the IPv6 address by computing a cryptographic hash of the public key. The resulting IPv6 address is called a cryptographically generated address (CGA). The corresponding private key can then be used to sign the ICMPv6 messages sent from the address. However, previous CGA proposed by SEND working group in IETF only provides authentication through digital signature using public key mechanism, it does not guarantee confidentiality of the ICMPv6 message. Therefore, the attacker still has the chance to modify the original ICMPv6 message and have the replay attack. Confidentiality means that the message is encrypted by the temporal session key to hide the whole message.

3. Network model

In this paper, we assume that our network is composed of several patients equipped with multiple portable body sensors and a lot of sensor devices with common transmission range to deliver the sensed data from the patient to HCC as shown in Figure 1. The dark circles in the figure represent abnormal sensors by attack and the white circles are normal sensors and red circles are also normal sensors with an event like a fire. There could be abnormal in a certain area [10]. Sensor nodes on mobile patients sense the signals from the body. A sensor is abnormal if the sensing value of sensor device deviates significantly from other sensing values of neighboring sensors because of the attack. Namely, sensor is called abnormal if sensor independently has an arbitrary sensing value without the correlation of neighbors. And the abnormal area means that sensors with arbitrary sensing value are nearly located in a certain area. The abnormal area can include a few normal sensors. Normal and abnormal area can exist at the mobile patient or somewhere from the patients to the Health Care Center(HCC). An event is a certain area composed of the sensors with the temporary similar sensing value. That is, the sensing values of event-detecting sensors have the correlation with each other while that in the abnormal area do not have any correlation with each other. However, the event area can also have a few abnormal/normal sensors.

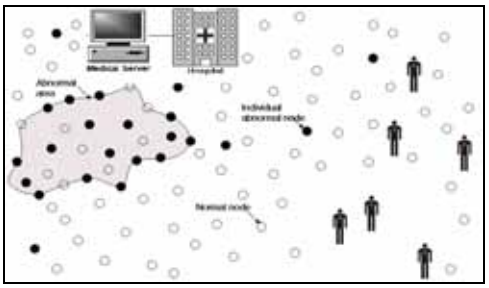


Figure 1. Network Model

We assume that each sensor has at least 2 neighbors because the proposed scheme utilizes the majority voting. We adopted multihop architecture from the patient to the HCC because usually multihop architecture has lower transmission power and higher delay when compared to star topology[23]. Namely, in the proposed scheme, each sensor collects the opinions from the neighbors and considers the gap of sensing values according to the distance and the time between sensors.

In sensor networks, various faults are common due to the malfunction of the sensor device itself and the harsh environment and artificial attacker. Faults occurring at different levels of the sensor are the physical layer fault, hardware fault, system software fault, and middleware fault [5]. In the proposed scheme, we focus on the faults of the sensing value under the attack by assuming all system hardware as well as the application software is already fault tolerant [10]. As a result, in the proposed scheme sensor node is still capable of receiving, sending, and processing even though it has the wrong sensing value due to the attacker.

4. A key management and distributed abnormal area scanning scheme for secure MSN

In this section, we first explain useful notations and present the proposed scheme.

Notations

- S_i: sensor node i;
- S_{ij}: the neighbors of S_i; j is the neighbor index of i
- x_i: sensing value of S_i;
- g_{ij}^t : gap between x_i and x_j at the time t, $g_{ij}^t = \left| x_i^t - x_j^t \right|$
- d_{ij}^t : distance difference btw S_i and S_j at the time t,
  $$d_{ij}^t = (x_i^t - x_j^t)^2 + (y_i^t - y_j^t)^2$$
- $m_k^{\Delta t, v}$: average of variance of neighbors, k, for a certain time Δ t;
- $v_k^{\Delta t, v}$: variance of variance of neighbors, k, for a certain time Δ t;
- c_{ij}: test between S_i and S_j , $c_{ij} \in \{0,1\}$, $c_{ij} = c_{ji}$;
- w_{ij}^v : sensing value weight between S_i and S_j
- w_{ij}^d : distance value weight between S_i and S_j
- T_s: tendency of a sensor considering spatial aspect,
  $T_s \in \{Normal, Abnormal\}$;

- T_t: tendency of a sensor considering temporal aspect,
  T_t □{*Normal, Abnormal*};
- T_r: real tendency of a sensor,
  T_r □{*Normal, Abnormal*};
- $x_{A\text{-}max}$: maximum sensing value;
- $r_{A\text{-}max}$: maximum transmission range;
- θ_s : allowed relative gap of sensing value; ex) 25%
- θ_t: allowed relative variance of sensing value according to the time

Key management

In the proposed scheme, each sensor encrypts its address and measured sensing data with MCGA before it regularly exchanges the message with neighbors. As previously stated, 128bit of IPv6 is composed of router's prefix 64bit and node's interface 64bit of MAC address. CGA provides secure communication by computing a cryptographic one-way hash function node's interface 64bit of IPv6 address and by digital signature the ICMPv6 message followed by IPv6 base header. However, previous CGA only provides authentication to the ICMPv6 message through digital signature using public key mechanism, it does not guarantee confidentiality of the ICMPv6 message. So we proposed the MCGA [13]. In this mechanism, the host can provide confidentiality to ICMPv6 message by hiding the whole message including the digital signature and the original message shown in Figure 2. KR_a and KU_a are private key and public key needed for authentication through digital signature. K_s is a session key needed for providing confidentiality to the message and it can be derived by the receiver using Sec bit value followed with CGA address. We omit the detail explain due to the space limit.

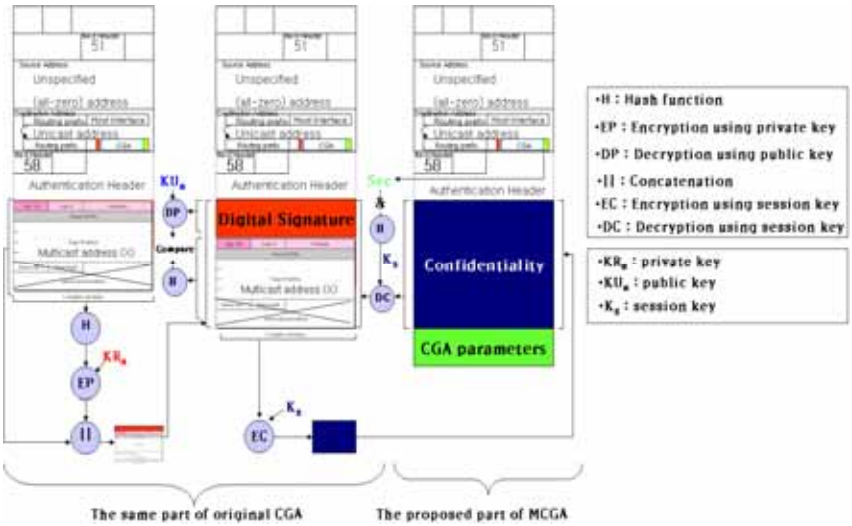


Figure 2.The total process of MCGA

Through MCGA, the node's interface 64bit of IPv6 address and the ICMPv6 message can be protected from the attacker, because the attacker can not manipulate the message during the communication between sensor nodes. To use MCGA in wireless sensor networks, we set the constant random bit to the router's prefix 64bit and sensor node ID to node's interface 64bit of MAC address. And we matches ICMPv6 message to the measured sensing value of sensor node. To know the MCGA generation and verification process in detail, III section of [13] can be utilized.

An abnormal area detection

After each sensor regularly exchanges its measured sensing value encrypted by MCGA with neighbors, it decrypts the encrypted measured sensing value using MCGA. And it determines its own status either normal or abnormal after it compares its own sensing value with the sensing values of neighbors. At that time, each sensor determines its status using two aspects. One is the spatial aspect and the other is the temporal aspect. And each sensor aggregates the network properties, sensorNet MIB, such as the location of sensor, tendency and mean of the sensing values when it receives the information from neighbors of the similar tendency. Finally, manager can monitor the sensorNet at a look through the scanning because he can receive the aggregated network properties, sensorNet MIB, from sensors.

1) Spatial aspect

To determine the sensor's status either normal or abnormal, in advance we consider the spatial aspect between sensors. In sensor networks, sensors usually have a similar sensing value in case they are nearly located each other. Specially, sensors located in the same sensing range have the similar tendency. The reason is that sensing values such as temperature, humidity and light cover the region to some degree. Usually, the sensing range is smaller than the transmission range. Therefore, each sensor node should differently consider 1-hop neighbors with the different value weights as (1) according to the distance weight as (2) even though 1-hop neighbors are within the same transmission range. Namely, we are interested in the weighted opinions of 1-hop neighbors considering the different value weight according to the spatial aspect to detect the abnormal sensor.

$$\begin{aligned} w_{ij}^{v}(Normal) &= 1-(g_{ij}^{t}/x_{A\_MAX})^{n},(n\geq 2),\ if\ g_{ij}^{t} \leq\ \theta_s * x_{A\_MAX} \\ w_{ij}^{v}(Abnormal) &= (g_{ij}^{t}/x_{A\_MAX})^{n},(n\geq 2),\ if\ g_{ij}^{t} \geq\ \theta_s * x_{A\_MAX} \end{aligned} \quad (1)$$

$w_{ij}^{v}(Normal)$ means the sensing value weight when the difference of tendency between sensor *i* and sensor *j* is small.

$w_{ij}^{v}(Abnormal)$ means the sensing value weight when the difference of tendency between sensor *i* and sensor *j* is significant. Therefore, the smaller the difference of tendency is, the lager the weight is acquired while the larger the difference of tendency is, the smaller the weight is acquired

$$w_{ij}^{d} = 1-(d_{ij}^{t}/r_{A\_MAX})^{n},(n\geq 2) \quad (2)$$

w_{ij}^{d} means the distance weight according to the distance between sensor *i* and sensor *j*. Surely, the nearer is the sensor node from each other, the larger the weight is acquired. The degree of weight, exponential n, can be chosen by the several functions such as $y = -x^n+1$ ($n\geq 2$), $y = -nx+1$ ($n\geq 2$) and $y = \log_n x$ ($0<n<1$). After each sensor measures its own

sensing value and collects the sensing values from neighbors, it divides neighbors into the same tendency group, c_{ij}=0, and the different tendency group, c_{ij}=1, through managing the tendency table. And it calculates both the weighted sum of the same tendency group and that of the different tendency group as (3). Finally it compares the weighted sum of the same tendency group with that of the different tendency group. As a result, if the weighted sum of the same tendency group is larger than that of the different tendency group, sensor node recognizes itself normal. Otherwise, sensor node recognizes itself abnormal.

$$\begin{aligned} T_s = Normal,\ if\ \frac{\sum w_{ij}^v}{\sum w_{ij}^d}\ for\ c_{ij}=0 > \frac{\sum w_{ij}^v}{\sum w_{ij}^d}\ for\ c_{ij}=1 \\ T_s = Abnormal,\ if\ \frac{\sum w_{ij}^v}{\sum w_{ij}^d}\ for\ c_{ij}=0 < \frac{\sum w_{ij}^v}{\sum w_{ij}^d}\ for\ c_{ij}=1 \end{aligned} \tag{3}$$

Namely, T_s means the tendency of each sensor node considering the spatial aspect.

2) Temporal aspect

Temporal aspect is needed to complement the limit of the spatial aspect by considering the change of the sensing value according to the time. In general, sensors constantly sense the value for a certain amount time. Specially, normal sensors including event-detecting sensors sense the consistent value within the uniform range and have a correlation of the sensing value with neighbors as the time passed. On the other hand, abnormal sensors arbitrary sense the value without the correlation with neighbors. Therefore, each sensor should consider a temporal correlation with neighbors to determine its status accurately through grasping the tendency of the group. Namely, each sensor senses the value several times for a certain time and calculates the variance as (4) and sends the result to all its neighbors. Finally, each sensor calculates the variance of the variance about neighbors to determine the final status as (5). As a result, if the variance of the variance is smaller than the specific threshold, θ_t, each sensor determines its final status as normal. Otherwise, it determines its final status as abnormal as (6).

$$\begin{aligned} m_i^{\Delta t} &= \sum_{t=1}^{n} x_i^t / n\ \ (n = \text{number of sensing per a sesnor } i) \\ v_i^{\Delta t} &= \sum_{t=1}^{n} (x_i^t - m_i^{\Delta t})^2 \end{aligned} \tag{4}$$

$$\begin{aligned} m_k^{\Delta t,v} &= \sum_{i=1}^{k} \sum_{t=1}^{n} (x_i^t - m_i^{\Delta t})^2 / k\ \ (k = \text{number of neighbors per a sensor i}) \\ v_k^{\Delta t,v} &= \sum_{i=1}^{k} (\sum_{t=1}^{n} (x_i^t - m_i^{\Delta t})^2 - m_k^{\Delta t,v})^2 \end{aligned} \tag{5}$$

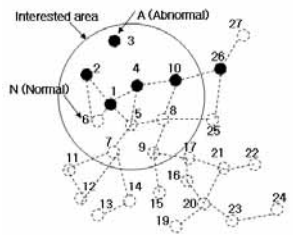
$$\begin{aligned} T_t = Normal,\ if\ v_k^{\Delta t,v} = \sum_{i=1}^{k} (\sum_{t=1}^{n} (x_i^t - m_i^{\Delta t})^2 - m_k^{\Delta t,v})^2 \le \theta_t \\ T_t = Abnormal,\ if\ v_k^{\Delta t,v} = \sum_{i=1}^{k} (\sum_{t=1}^{n} (x_i^t - m_i^{\Delta t})^2 - m_k^{\Delta t,v})^2 \ge \theta_t \end{aligned} \tag{6}$$

3) In-network aggregation

To reduce the direct communication overhead between each sensor and the manager and to provide the abstracted network properties, sensorNet MIB, to the manager, we applied the in-network aggregation to the proposed scheme. Namely, each sensor delivers sensorNet MIB to the neighbor with the highest weight when it calculates its tendency considering the spatial and temporal correlation. As a result, if sensor receives the same tendency, it aggregates sensorNet MIB and forwards the aggregated sensorNet MIB to the next node. However, if sensor receives the different tendency, it stops the aggregation and forwards the aggregated sensorNet MIB to the manager.

4) Example

Figure 3 shows the wireless sensor networks and the tendency table distributedly managed by each sensor node after decrypting the sensing value using MCGA. We exemplify the interested area including 5 abnormal sensors and 5 normal sensors in a wireless sensor networks. Tendency table is composed of 4 columns such as S_i, S_{ij} with c_{ij} = 0, S_{ij} with c_{ij} = 1, and tendency determined by the spatial aspect, temporal aspect and real situation. If c_{ij} is 0, S_i and S_j are most likely in same status either normal or abnormal. Otherwise, if c_{ij} is 1, S_i and S_j are most likely in different status.



S_i	S_{ij} with c_{ij} = 0	S_{ij} with c_{ij} = 1	Tendency		
			T_s	T_t	T_r
1	2,4	5,6	N	A	A
2	1	6	N	A	A
3			.	.	A
4	1,10	5	N	A	A
5	7,8	1,4	N	N	N
6		1,2	A	A	N
7	11,12,14,5		N	N	N
8	5,9,25	10	N	N	N
9	8,15,17		N	N	N

Figure 3. (a) A wireless sensor networks and (b) tendency table

For example, sensor node 1 marks the neighbor 2 and 4 as S_{ij} with c_{ij} = 0 in the tendency table because the sensing value of sensor node 1 is similar with that of sensor node 2 and that of sensor node 4. Whereas, sensor node 1 marks the neighbor 5 and 6 as S_{ij} with c_{ij} = 1 because the sensing value of sensor node 1 is different with that of sensor node 5 and that of sensor node 6. In the first step considering the spatial aspect, sensor node 1 determine its tendency as N(Normal) after applying equation (1), (2) and (3). However, in the second step considering the temporal aspect, it changes its tendency as A(Abnormal) after applying equation (4), (5) and (6). In fact, after the second step, its tendency is more same with the real tendency, T_r, because the second step considers the temporal aspect in addition. It is used to determine the detection accuracy through comparing T_t with T_r in the performance section. On the other hand, sensor node 3 and 6 shows the case of the false alarm rate because it decides its status, T_t, in different with its real tendency, T_r. However, this is few cases in a wireless sensor networks since most sensors is densely distributed and a few false alarm rate is not important in a scalable sensorNet. And MCGA additionally improved the accuracy of the proposed scheme by eliminating the manipulation of the attacker during the communication between sensor nodes.

5. Performance evaluation

Without MCGA

Fist of all, we simulated the proposed scheme without MCGA. For simulation we used Matlab as the tool. An example simulation scenario is composed of total 1000 sensor nodes randomly deployed in a region of size 30×30 units. The measurement parameter x_i is considered to be temperature. We set the values of x_i as normal including event and abnormal with ranges as follows, "Normal" = 70-75 degrees and "Abnormal" as 100-105 degrees. And we set both θ_s and θ_t to be 25. The weight of degree is chosen 2.

Figure 4 shows the result of an abnormal area scanning composed of the Normal (T) and Abnormal (F). As we can see, the most area with the similar temperature is expressed as T while sensor located in the boundary or sensor without correlation with neighbors as the time passed is expressed as F. Therefore, the manager can monitor the scalable sensorNet in a whole if any part of the network has the problem.

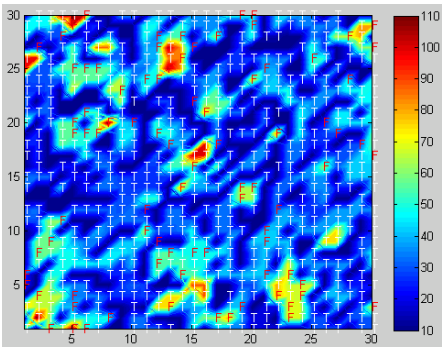


Figure 4. An abnormal area scanning in a wireless sensor networks

Abnormal sensor detection accuracy (ASDA) and abnormal alarm rate (AAR) are the two metrics. ASDA is defined as the ratio of the number abnormal sensor detected to the total number of abnormal sensors in the field. The AAR is the ratio of the number of abnormal sensor diagnosed as normal to the total number of abnormal sensors. In the simulation, sensors are randomly chosen to be abnormal with the probabilities of 0.05, 0.10, 0.15, 0.20 and 0.25 respectively under different average neighbors of 5 and 10.

Figure 5 show ASDA of the proposed scheme1 using spatial, temporal aspect and the proposed scheme2 using correlation coefficient as equation (7) and (8) and the previous scheme using the number of neighbors [10]. In (8), T_i is the tendency of sensor node i considering correlation coefficient between sensor node i and its neighbors.

$$m_i^{\Delta t} = \sum_{t=1}^{n} x_i^t / n \ \ (n = \text{number of sensing per a sesnor } i)$$
$$m_j^{\Delta t} = \sum_{t=1}^{n} x_j^t / n \ \ (n = \text{number of sensing per a sesnor } j) \tag{7}$$

$$
\begin{aligned}
&\textit{Correlation Coefficient}_{ij}(CC_{ij}) = \frac{\sum_{t=1}^{n}(x_i^t - m_i^{\Delta t})(x_j^t - m_j^{\Delta t})}{\sqrt{\sum_{t=1}^{n}(x_i^t - m_i^{\Delta t})^2 \sum_{t=1}^{n}(x_j^t - m_j^{\Delta t})^2}} \\
&T_i = \ \textit{Normal}, \ \sum_{j=1}^{k} CC_{ij} / k \ \ (k = \textit{number of neighbors per a sensor } i) \ \geq \ 0.5 \\
&T_i = \ \textit{Abnormal}, \ \sum_{j=1}^{k} CC_{ij} / k \ \ (k = \textit{number of neighbors per a sensor } i) \ < \ 0.5
\end{aligned} \tag{8}
$$

The detection accuracy for 5 neighbors decreases when the abnormal probability becomes larger. But the abnormal detection accuracy of the proposed schemes is still about 90% when there are about 25% of the sensors being abnormal. There are several abnormal sensors which are not diagnosed as abnormal because the random deployment of the sensors in the network results in very few neighbors for those sensors. When the average number of neighbors is greater than 10, the abnormal detection of the proposed scheme is very high than the previous scheme using the number of neighbors [10]. This is the reason that the proposed schemes can detect the event-detecting sensors as normal sensors using the spatial, temporal correlation. And almost all the abnormal sensors can be detected even under a high abnormal sensor probability.

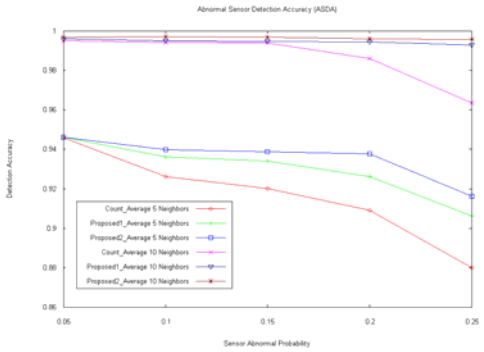


Figure 5.Abnormal Sensor Detection Accuracy (ASDA)

Figure 6 shows AAR of the proposed schemes and the previous scheme. It shows that for the 5 neighbors, the higher the abnormal probability, the higher AAR. This is because the large number of abnormal sensor tests normal sensors to be likely abnormal and these normal sensors are then diagnosed as abnormal sensors. However, when the average number of neighbors is greater than 10, AAR is low.

With MCGA

In addition, we simulated the proposed scheme with MCGA. As previously stated, MCGA provides the perfect confidentiality to the measured sensing value when each sensor node exchange the measured sensing value. Namely, attackers can not modify the measured sensing value during MCGA. As a result, the aggregated information collected

by sensor nodes is securely delivered to a manager. We do not show the simulation result graph because ASDA of the proposed schemes is 1 and AAR of that is 0 with MCGA.

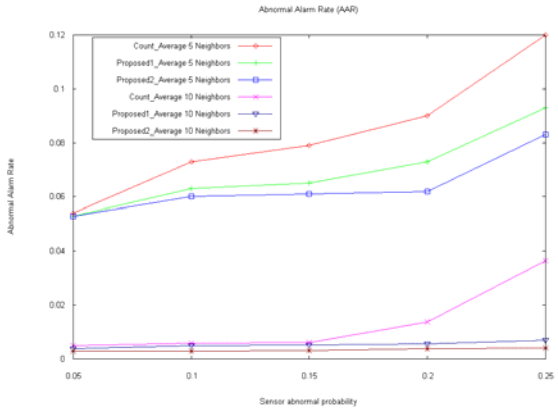


Figure 6. Abnormal Alarm Rate (AAR)

In fact, MCGA additionally increase the data delivery ratio because the intermediate sensor nodes have more chances of aggregating the sensing value with the same tendency under ASDA is 1 and AAR is 0. While in the proposed schemes without MCGA, the probability that sensor nodes meet the sensing value with different tendency because ASDA is smaller than 1 and AAR is larger than 0 is increased. Therefore, the sensor nodes stop aggregating the sensing value when they meet the sensing values with the different tendency and it decreases the delivery ratio. Figure 7 and Figure 8 shows the comparison of data delivery ratio according to the time, Sec and Mask value when attack manipulates the sensing data. Sec and MASK is an unsigned three-bit integer and is determined by the sender to prevent the enhanced attack. The more Sec and Mask is bigger, the more bits attacker must guess to know the original data. Therefore, the more Sec and Mask is bigger, the more data delivery ratio is increased. Additionally, data delivery ratio is larger in dense network than sparse network because the more sensor node is, the more sensor node can exchange the encrypted message and finally SensorMIB is delivered to the manager in MSN.

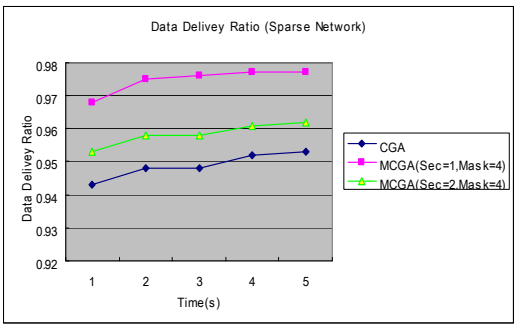


Figure 7. Data Delivery Ratio (Sparse Network)

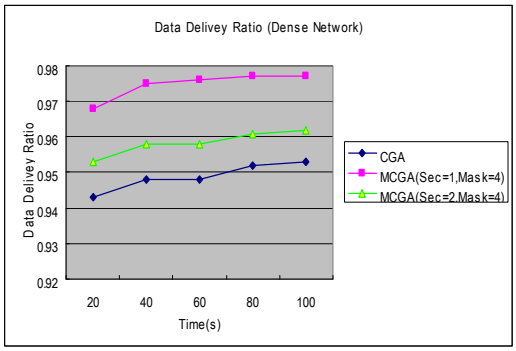


Figure 8. Data Delivery Ratio (Dense Network)

6. Conclusion

We proposed a key management and abnormal area scanning algorithm using spatial, temporal correlation and in-network aggregation for secure MSN. In the proposed scheme, each sensor identifies its own status to be either "normal" or "abnormal" using spatial, temporal correlation and in-network aggregation. It is tested and compared with the previous schemes under different number of abnormal sensors and neighbors in the same area. Our simulation results show that ASDA is over 99% even when 25% nodes are abnormal. And AAR is very accurate when the sensor abnormal probability is low. Namely, simulation results support and demonstrate that the proposed algorithm has high ASDA and low AAR in MSN composed of sensor nodes. In addition, we showed that the proposed scheme with MCGA provides the perfect confidentiality to the measured sensing value when each sensor nodes exchange the measured sensing values. In future work, we will simulate abnormal sensor detection accuracy (ASDA) and abnormal alarm rate (AAR) and data delivery ratio under the more various attack scenarios.

Acknowledgments

"This work was supported by the Korea Science and Engineering Foundation(KOSEF) grant funded by the Korea government(MEST) (NO. R01-2008-000-20062-0)."

References

1. J. M. Kahn, R. H. Katz, and K. S. J. Pister, "Next Century Challenges: Mobile Networking for "Smart Dust"," in Proceedings of the ACM/IEEE International Conference on Mobile Computing and Networking ACM, Seattle, WA, USA, Aug. 1999.
2. Deborah Estrin, Ramesh Govindan, and John Heidemann, "Embedding the Internet," *Communications of the ACM*, vol. 43, no. 5, pp. 39–41, May 2000, (special issue guest editors).
3. Jinran Chen, Shubha Kher, and Arun Somani, "Distributed Fault Detection of Wireless Sensor Networks," ACM DIWANS 2006.
4. Y. Zhao, R. Govindan, and D. Estrin, "Residual Energy Scans for Monitoring Wireless Sensor Networks," *IEEE WCNC'02*, pp.78-89.

5. F. Koushanfar, M. Potkonjak, and A. Sangiovanni-Vincentelli. "Fault-tolerance in sensor networks," In Handbook of Sensor Networks. CRC press, 2004.
6. A. K. Somani and V. K. Agarwal. "Distributed diagnosis algorithms for regular interconnected structures," IEEE Transactions on Computers, 41(7):899–906, July 1992.
7. L. B. Ruiz, I. G. Siqueira, L. B. e Oliveira, H. C. Wong, J. M. S. Nogueira, and A. A. F. Loureiro, "Fault management in event-driven wireless sensor networks," In MSWiM '04: Proceedings of the 7th ACM international symposium on Modeling, analysis and simulation of wireless and mobile systems, pages 149–156, New York, NY, USA, 2004. ACM Press.
8. Chihfan Hsin, Mingyan Liu, "Self-monitoring of wireless sensor networks," computer communications 2006.
9. M. Ding, D. Chen, K. Xing, and X. Cheng, "Localized fault-tolerant event boundary detection in sensor networks," In Proceedings of IEEE INFOCOM 2005.
10. Jinran Chen, Shubha Kher, and Arun Somani, "Distributed Fault Detection of Wireless Sensor Networks," ACM *DIWANS'06,* September 25, 2006.
11. F. Koushanfar, M. Potkonjak, and A. Sangiovanni-Vincentelli. "On-line fault detection of sensor measurements," Proceedings of IEEE Sensors, pages 974–979, 2003.
12. Hayoung Oh, Kijoon Chae, "An Abnormal Area Scanning for Scalable and Energy-Efficient and Secure SensorNet Management," Multimedia and Ubiquitous Engineering, 2008. MUE 2008. International Conference on, 24-26 April 2008 Page(s):592 – 596.
13. Hayoung Oh, Kijoon Chae, "An Efficient Security Management in IPv6 Network via MCGA," Advanced Communication Technology, The 9th International Conference on Volume 2, 12-14 Feb. 2007 Page(s):1179 – 1181.
14. Kabadayi, Sanem; Julien, Christine; "A Local Data Abstraction and Communication Paradigm for Pervasive Computing," Pervasive Computing and Communications, 2007. PerCom '07. Fifth Annual IEEE International Conference on 19-23 March 2007 Page(s):57 – 68.
15. Subramanian, Nalin; Yang, Chanjun; Zhang, Wensheng; "Securing Distributed Data Storage and Retrieval in Sensor Networks," Pervasive Computing and Communications, 2007. PerCom '07. Fifth Annual IEEE International Conference on 19-23 March 2007 Page(s):191 – 200.
16. Domaszewicz, J.; Roj, M.; Pruszkowski, A.; Golanski, M.; Kacperski, K.; "ROVERS: pervasive computing platform for heterogeneous sensor-actuator networks," World of Wireless, Mobile and Multimedia Networks, 2006. WoWMoM 2006. International Symposium on a 26-29 June 2006 Page(s):615 – 620.
17. Lin, J.; Song, C.; Wang, H.; "A Developing Approach of Information Acquisition System in Pervasive Computing Environment," Information Acquisition, 2006 IEEE International Conference on 20-23 Aug. 2006 Page(s):840 – 844.
18. Reddy, Y.V.; "Pervasive Computing: Implications, Opportunities and Challenges for the Society," Pervasive Computing and Applications, 2006 1st International Symposium on 3-5 Aug. 2006 Page(s):5 – 5.
19. J. Arkko, "RFC-3971: SEcure Neighbor Discovery (SEND)," March 2005.
20. T. Aura, "RFC-3972: Cryptographically Generated Addresses (CGA)," March 2005.
21. Subramanya, S.R.; Yi, B.K.; "Digital signatures," Potentials, IEEE Volume 25, Issue 2, March-April 2006.
22. Narasimha Challa, Hasan C¸ am, and Madhur Sikri, "Secure and Efficient Data Transmission over Body Sensor and Wireless Networks," EURASIP Journal on Wireless Communications and Networking Volume 2008, Article ID 291365.
23. Anirudh Natarajan, Mehul Motani, Buddhika de Silva, Kok-Kiong Yap & K. C. Chua, "Investigating Network Architectures for Body Sensor Networks," HealthNet'07 ACM, June. 2007.