■ 2006년도 학생논문 경진대회 수상작

신뢰도 평가를 통한 무선 센서 네트워크에서의 거짓 데이타 제거

(Trust-Based Filtering of False Data in Wireless Sensor Networks)

허 준 범 † 이 윤 호 †† 윤 현 수 †††
(Junbeom Hur) (Younho Lee) (Hyunsoo Yoon)

요 약 무선 센서 네트워크는 자연재해 탐지 시스템, 의료 시스템, 그리고 군사적 응용분야 등의 다양한 환경에서 유용한 해결책을 제시하고 있다. 그러나 센서 네트워크의 구성 환경 및 자원 제약적인 본질적인 특성으로 인해 기존의 전통적인 보안기법을 그대로 센서 네트워크에 적용하기에는 무리가 있다. 특히 네트워크를 구성하는 센서 노드들은 제한된 배터리를 사용하기 때문에 센서 네트워크에 거짓 데이타가 유입되는 경우 서비스 거부 뿐만 아니라 센서 노드의 제한된 에너지를 소모시키는 등의 심각한 문제를 야기할 수 있다. 기존의 전통적인 암호학적 인증 및 키 관리 방법 등을 통한 보안 기법은 센서 네트워크의 물리적인 노드탈취 공격에 대한 취약성으로 인해서 이러한 거짓 데이타 판별에 대한 해결책을 제시하지 못한다. 본 논문에서는 기존의 평판기반 기법과 달리 각 센서 노드의 위치에 따른 센싱 결과에 대해 일관성 등의 요소를 기반으로 신뢰도를 평가하고, 거짓 데이타를 주입하는 내부 공격에 대한 보안기법을 제안한다. 분석 결과에 따르면 제안한 신뢰도 평가 기반의 데이타 통합 기법은 기존의 중앙값보다 견고한 데이타 통합 결과를 보여준다.

키워드 : 무선 센서 네트워크 보안, 신뢰도 평가, 안전한 데이타 통합

Abstract Wireless sensor networks are expected to play a vital role in the upcoming age of ubiquitous computing such as home environmental, industrial, and military applications. Compared with the vivid utilization of the sensor networks, however, security and privacy issues of the sensor networks are still in their infancy because unique challenges of the sensor networks make it difficult to adopt conventional security policies. Especially, node compromise is a critical threat because a compromised node can drain out the finite amount of energy resources in battery-powered sensor networks by launching various insider attacks such as a false data injection. Even cryptographic authentication mechanisms and key management schemes cannot suggest solutions for the real root of the insider attack from a compromised node. In this paper, we propose a novel trust-based secure aggregation scheme which identifies trustworthiness of sensor nodes and filters out false data of compromised nodes to make resilient sensor networks. The proposed scheme suggests a defensible approach against the insider attack beyond conventional cryptographic solutions. The analysis and simulation results show that our aggregation scheme using trust evaluation is more resilient alternative to median.

Key words : trust evaluation, security, secure aggregation, resilient sensor networks

· This research was supported by the MOST(Ministry of Science and Technology) / KOSEF(Korea Science and Engineering Foundation) through the AITrc(Advanced Information Technology Research Center) and the MIC(Ministry of Information and Communication), Korea, under the ITRC(Information Technology Research Center) support program supervised by the IITA(Institute of Information Technology Assessment). (IITA-2006-C1090-0603-0015)

† 학생회원 : 한국과학기술원 전산학과
jbhur@nslab.kaist.ac.kr
†† 정 회 원 : 한국과학기술원 전산학과
yhlee@nslab.kaist.ac.kr
††† 종신회원 : 한국과학기술원 전산학과 교수
hyoon@kaist.ac.kr

논문접수 : 2006년 5월 18일
심사완료 : 2007년 11월 21일

정보과학회논문지: 정보통신 제35권 제1호(2008.2)

1. 서 론

Wireless sensor networks suggest a promising approach for various applications including safety monitoring of environments, freeway traffic measuring, and many other military applications [1]. A major feature of these systems is that a large number of resource-limited sensor nodes in networks assist each other by passing data, in-network process and control packets from one node to another. It is often termed an infrastructure-less, self-organized, or spontaneous network [2].

Wireless sensor networks tend to be organized in open environment; thus, they are susceptible to a variety of attacks, such as node capture, eavesdropping, denial of services, wormhole, and Sybil attack [3]. Especially, node compromise is a severe security threat, upon which the adversary might obtain the secret keys and use them to launch insider attacks. A compromised node is able to successfully authenticate bogus reports to its neighbors in its communication range. In addition, if the adversary can obtain his own commodity sensor nodes and induce the networks to accept them as legitimate nodes, it is hard to distinguish legitimate nodes from illegitimate ones just through the current network security mechanisms [4]. Although cryptographic authentication schemes are effective for preventing outsider attacks injecting or spoofing packets, they cannot prevent insider attacks since a compromised node has secret keys.

Therefore, developing a malicious nodes detection and an efficient false data filtering scheme is necessary for resilient wireless sensor networks because false reports can drain out the finite amount of energy resources in battery-powered sensor networks and even a small amount of compromised nodes can influence the whole networks critically [5]. In this paper, we propose a novel secure aggregation scheme based on the trustworthiness of each sensor node without any utilization of cryptographic approaches that may put a heavy processing load on resource-constrained sensor nodes. To evaluate the trustworthiness, each node analyzes behaviors of its neighbor nodes based on several trust evaluation factors. The result of the trust evaluation is utilized to identify compromised nodes and thwart malicious behaviors of them.

Specifically, the trustworthiness of a sensor node is evaluated by investigating that how straightforwardly the node forwards sensing results and how consistent data the node reports compared with those of its neighbor nodes. The consistency check is performed by gathering multiple and redundant sensing data, and crosschecking them using spatial correlations of them. More precisely, a node computes a boundary of expected sensing value of its neighbor node in consideration of its own sensed value and distances among the nodes and an event, and checks that a reported value of the neighbor node is within the boundary. If a node cooperates with its neighbor nodes straightforwardly and its reported data are estimated to be consistent within the boundary, it gets a high trust value as an incentive; otherwise, it gets a low trust value as a penalty. The evaluated trust value is then used as a standard which indicates the trustworthiness of a node and determines an aggregating proportion of data reported from the node for an event.

The contributions of this paper are as follows. First, we propose a novel and non-cryptographic trust evaluation scheme designed for detection of malicious nodes in wireless sensor networks beyond the capability of cryptographic security. Second, we develop a secure and hierarchical aggregation mechanism using trust values of each node. The cryptographic approaches for authentication can defend just against the outsider attack, whereas the proposed scheme can defend against the insider attack using accumulated analysis for the behaviors of sensor nodes. The evaluated trustworthiness of a node affects data aggregation policy in return. To the best of our knowledge, this is the first effort that establishes a trust evaluation scheme for secure aggregation in wireless sensor networks. The best we can hope for in the presence of insider adversaries is a graceful degradation of wireless sensor networks. According to our analysis, the proposed aggregation scheme could be a more resilient alternative to median, which is known to be the robustest conventional aggregation

function [5]. The breakdown point of median, which means a fraction of nodes that can be compromised before security down, is estimated to 1/2, whereas that of our scheme is $(2m-1)/2m$ in the best case, where m is an average number of sensor nodes in a grid, which is a unit area for local data aggregation. In addition, simulation results show that the deviated error rate of the aggregated result of our scheme goes down 90% when a half of nodes are compromised, whereas the error rate of median exceeds 340%.

The rest of the paper is organized as follows. Section 2 describes some related works. Section 3 describes goals and assumptions of our scheme. Section 4 details an overall process of the trust evaluation and secure aggregation scheme. Section 5 analyzes the performance evaluation, and Section 6 shows the simulation results. Section 7 discusses further security issues. Section 8 remarks conclusion of the paper.

2. Related Work

One of the most vexing issues facing sensor networks is how to provide resiliency against node capture attacks. In most applications, sensor nodes are likely to be deployed in open environment readily accessible to attackers. Such exposure raises the possibility of nodes compromising. That is, an adversary might capture sensor nodes, extract cryptographic secrets, modify programming, or replace them with malicious nodes under the control of him or her. The adversary may affect their readings, then it cannot be prevented, neither detected by cryptographic mechanisms. This is called *stealthy attack* [6].

Recent studies proposed several solutions for sensor networks to authenticate and prevent false data injection by an outsider attacker [7-10]. Their basic approaches are using cryptographic mechanisms such as Message Authentication Codes (MACs), or probabilistic key predistribution schemes such as [13] and [14] for a probabilistic attack detection or en-route filtering. These approaches prevent naive impersonation of a sensor node, however, they cannot prevent an injection of false data from malicious or compromised insider nodes which have already been authenticated as legal ones in the networks because the data acceptance policies are mainly based on the cryptographic authentication process.

Secure aggregation schemes can be one solution to the insider attack. According to the resiliency analysis of primitive aggregation functions by D. Wagner, some of the widely used aggregation functions such as average, minimum, and maximum are inherently insecure [5]. Wagner proposed to use a median instead of an average as a robust aggregation function. Before the aggregation function is called, to analyze unexpected deviations of received sensor readings can help to upper bound a distortion of them [15]. Another approach against the stealthy attack is an interactive proof method using random sampling such as SIA [6]. The SIA enables a user to verify that the reported value given by an aggregator is a good approximation of true values at the cost of an additional commitment construction and communication overhead. Other studies proposed several secure in-network aggregation methods which make a network resilient even when a fraction of sensor nodes are corrupted [8-12]. These schemes, however, mainly focus on detecting and excluding fictive data which are significantly different from the true values so that they cannot determine the corruption of the nodes themselves, neither differentiate malicious nodes and temporarily malfunctioning nodes. The proposed trust management scheme is concerned with this problem so that it analyzes the behavior of a sensor node accumulatively in addition to sensing values reported from it.

Some studies discussed the trust evaluation in ad hoc networks [2,16]. However, the trust evaluation mechanisms developed for ad hoc networks cannot be directly adopted to sensor networks because the trust evaluation policy in ad hoc networks requires each node to manage all trust values of other nodes in the network. Such a global computation of trust values is an impractical approach in wireless sensor networks that consist of a large number of resource-constrained sensor nodes. Therefore, a novel trust evaluation scheme is necessary for resilient wireless sensor networks.

3. Goals and Assumptions

3.1 Threat Model

In this paper, we do not consider attacks against the physical layer such as frequency jamming. Also, we do not consider any attack against the Medium Access Control (MAC) protocol that may lead to a denial-of-service (DoS). Several mechanisms such as spread spectrum [17] and coding [18] are known to be efficient to shield wireless sensor networks against such attacks. Rather, the attackers may compromise a node to obtain security information to launch various insider attacks, especially false data injection. A compromised node can also block legitimate reports passing through it, or neglect its duty of generating reports for real events selfishly for the sake of battery saving.

3.2 Goals

We focus on making resilient wireless sensor networks which work normally even though some fraction of sensor nodes might be compromised, that is graceful degradation of performance. For this goal, we propose a novel trust evaluation scheme for secure aggregation suited to wireless sensor networks. The proposed scheme is designed to detect compromised nodes, thwart malicious behaviors, and filter out false data from the malicious nodes.

3.3 Assumptions

We have several assumptions in our scheme as follows: (1) Each sensor node knows deployed geographic coordinates of itself and its neighbor nodes. This can be accomplished by several localization schemes such as [19-21], and a location claims verification scheme such as [22]. (2) Sensor nodes are deployed in separate locations densely enough to be able to sense a same event redundantly with their neighbor nodes.

4. Trust Evaluation for Secure Aggregation

In this section, a trust-based secure aggregation scheme is proposed. An overview of the scheme is described as follows: First, the sensing area is divided into a number of logical grids (Section 4.1). Each sensor node deployed in the grid then estimates its location and verifies location claims of its neighbor nodes. Second, each sensor node evaluates trustworthiness of its neighbor nodes by analyzing behaviors and consistency level of reported data of them. Inconsistent data from malicious nodes can be detected in this step (Section 4.2). Third, an aggregator per each grid aggregates sensing data of the grid, and a representative value is computed from the aggregated results and transmitted to a sink node, which is a data collection node with sufficient computation and storage capabilities. Inconsistent data from malicious nodes can be excluded in this step (Section 4.3).

4.1 Grid Division

The sensing area is divided into a number of logical grids in proportion to the sensing range s of a sensor device so that one sensor device's sensing range can cover a grid entirely it belongs to regardless of its deployed location. So, a grid size is set to $\frac{s}{\sqrt{2}} \times \frac{s}{\sqrt{2}}$ as in Fig. 1, which is the maximum size that a grid can extend to while satisfying the whole coverage by s. This guarantees that any sensor node can detect an event happened in the grid in which it is deployed. Each sensor node deployed in the sensing area then determines its grid and geographic coordinate as well as locations of its one-hop neighbor nodes. A grid of ith row and jth column in the sensing area is identified with $Grid_{i,j}$.

Node n_i located in (x_i, y_i) determines its grid G_i in the sensing area of which a static reference point is (SA_X, SA_Y) using following procedure *GridDivide*. The reference point is set in each node before the deployment.

Procedure 1 $GridDivide(SA_X, SA_Y, x_i, y_i)$

$\lceil (x_i - SA_X)/\frac{s}{\sqrt{2}} \rceil = X_i$
$\lceil (y_i - SA_Y)/\frac{s}{\sqrt{2}} \rceil = Y_i$
$G_i = Grid_{X_i, Y_i}$
return G_i

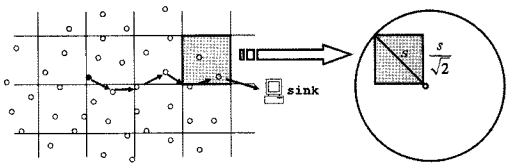


Fig. 1 Grid division

4.2 Trust Evaluation

After deployment and localization, each sensor node performs its sensing task and evaluates trust values of one-hop neighbor nodes accumulatively based on several factors.

4.2.1 Trust Evaluation Factor

Each sensor node has a trust evaluation matrix for its neighbor nodes. Note that this matrix only records trust-related information in a local sense. For node n_i, each row of the matrix I^i is reserved for each neighbor node, denoted by n_j, and columns are labeled by trust evaluation factors as follows:

(1) Identification: This factor contains a unique identification of n_j, which is determined by its deployed location and MAC address. $\|$ denotes concatenation.
- $ID_j = G_j \| (x_j, y_j) \| MACAddress_j$

(2) Distance: This factor contains distance information between n_i and n_j.
- $D_{i,j} = \sqrt{(x_i - x_j)^2 + (y_i - y_j)^2}$

(3) Straightforwardness: This factor contains straightforward communication ratio of n_j, which is utilized as a criterion for selfishness of n_j. If a node stalls the generation of reports for real events, or does not forward legitimate reports passing through it with a selfish intention (that is false negative attack), sensing failure count of this factor will increase; otherwise, sensing success count will increase.
- S_j: straightforwardness value of n_j
- ss_j: sensing success count of n_j
- sf_j: sensing failure count of n_j

(4) Sensing result: This factor represents a sensing result reported by n_j, which consists of sensing data and sensing time for an event.
- R_j: sensing result of n_j which consists of $\{st_j, sd_j\}$
- st_j: sensing time of n_j
- sd_j: sensing data of n_j

(5) Consistency: This factor represents consistency level of n_j. Based on this factor, each node identifies malicious nodes that inject false data. If a node reports unexpectedly deviated values compared with the sensing values of its neighbor nodes (that is false positive attack), inconsistent sensing count will increase; otherwise, consistent sensing count will increase. The consistency check process will be described in Section 4.2.2.
- C_j: consistency value of n_j
- cs_j: consistent sensing count of n_j
- is_j: inconsistent sensing count of n_j

(6) Trust value: This factor represents a total trustworthiness of n_j.
- T_j: trust value of n_j

4.2.2 Consistency Check

To check consistency of its neighbor nodes' reporting data, a sensor node computes *acceptable region* (AR) of an event, which is a possible region of the event, and puts boundary to the legally acceptable range of neighbor nodes' sensing data based on the AR and its own sensed value. When n_i checks sensing data of its neighbor n_j, if the data lies out of the acceptable range computed by n_i, the sensing data are estimated to be false report. The estimation result is then recorded in the consistency factor C_j in the trust evaluation matrix I^i.

To compute the legally acceptable range of sensing data of n_j, n_i should know the distances from an event to n_i and n_j respectively, and the distance from itself to n_j. Because n_i already knows the location of n_j and distance between them, it is only required to estimate AR of an event in order to compute the distance from an event to n_i and n_j, and then set bounds of the acceptable range. AR of an event is defined as a set

$$AR = (x,y) | r_{MIN} \le \sqrt{(x - x_i)^2 + (y - y_i)^2} \le r_{MAX},$$

where r_{MIN} and r_{MAX} represent the expected shortest and longest distance to an event-happened grid, respectively. The first reporting grid can be a candidate for the event-happened grid.

The expected sensing value of a neighbor node is then computed using a *reverse sense function* (*RSF*). When n_i computes the expected sensing value of n_j on an event, denoted by sd_j^*, n_i performs the *RSF* as a follow:

$$sd_j^* = RSF(sd_i, r, D_{i,j}), \quad (1)$$

where r represents a distance between n_i and an event determined by AR of the event. Particularly, the RSF in (1) is proposed for sensor applications that detect continuous values such as a temperature and sound pressure using a spatial correlation of sensing data. So, the RSF may be a little modified according to its application. For example, in a temperature-sensing application, the RSF may be modeled by Stefan-Boltzman Law (the receiving radiation energy $L \propto \frac{1}{r^2}$); and in a sound pressure sensing application, it may be modeled by the distance law for the sound pressure (sound pressure $P \propto \frac{1}{r}$).

During trust evaluation processes, sensor nodes perform the RSF to check consistency of their neighbor nodes' reported data. When n_j senses an event, it sends its identification and sensing result, $\{ID_j, R_j\}$, to its neighbor nodes. If n_i receives the sensing result from n_j, n_i checks whether the received data can be acceptable as consistent data, or unacceptable as inconsistent data using following procedure *ConsistencyCheck*.

Procedure 2 *ConsistencyCheck*(ID_j, R_j, AR)
```
if |st_i − st_j| ≤ ε then
  for all (x, y) ∈ AR do
    r = √((x − x_i)² + (y − y_i)²)
    sd*_j = RSF(sd_i, r, D_{i,j})
    compute MIN(sd*_j)
    compute MAX(sd*_j)
  end for
  if MIN(sd*_j) ≤ sd_j ≤ MAX(sd*_j) then
    cs_j = cs_j + 1
  else
    is_j = is_j + 1
  end if
end if
```

In this case, two cases can be considered. First case is that two neighboring nodes in one-hop range, n_i and n_j, succeed in sensing a same event. For the pre-defined small value ϵ, when $|st_i - st_j| \le \epsilon$, n_i and n_j are considered to sense a same event. n_i then increases sensing success count for n_j by 1, that is $ss_j = ss_j + 1$, checks consistency of the sd_j in R_j, and records the evaluated result to the corresponding trust evaluation factor for n_j.

$MIN(sd_j^*)$ and $MAX(sd_j^*)$ represent the minimum and maximum sd_j^* computed using RSF, respectively. When n_j checks consistency of sensing data of n_i in return, the legally acceptable region of sd_j^* would be $[MIN(sd_j^*), MAX(sd_j^*)]$.

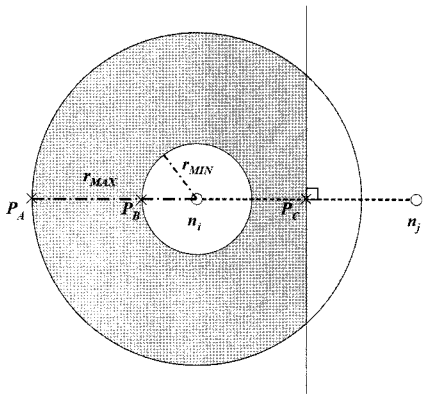


Fig. 2 Acceptable region of an event

If n_i is closer to an event than n_j, one of the possible ARs of the event can be described pictorially like Fig. 2. In Fig. 2, the gray region represents the AR of an event. Of course, the AR of an event could be shaped variously based on geographic locations of sensor nodes. For example, in a temperature sensing system, as a receiving radiation energy is proportional to $\frac{1}{r^2}$, $MIN(sd_j^*)$ would output the expected sd_j^* based on the assumption that a position of the event is P_A in Fig. 2. $MAX(sd_j^*)$ would output the expected sd_j^* based on the assumption that a position of the event is P_C. Likewise, the $MIN(sd_j^*)$ and $MAX(sd_j^*)$ would output the expected sd_j^* based on the assumption that a position of the event is P_C and P_B, respectively.

Second case is that two neighboring nodes fail to sense a same event. For example, n_i detects an event and reports the sensing result, but neighboring n_j does not report any result. In this case, n_i checks that whether n_j is located in the area in which AR of the event may not be covered by sensing range

of n_j. If n_j is estimated to be located in the area where its sensing range can cover whole AR, but it does not report any result for an obviously detected event, n_i increases a sensing failure count for n_j\$, that is $sf_j = sf_j + 1$.

4.2.3 Trust Quantification

The trust quantification process transforms individually discrete values of trust evaluation factors into continuous values from -1 to $+1$, which mean complete distrust and complete trust, respectively. As a node evaluates and revalues trustworthiness of its neighbor nodes continuously, the trust values should be quantified imperatively for impartial trust comparison among the nodes. The trust evaluation factors are quantified as follows:

(1) Consistency value

$$C_i = \frac{cs_i - is_i}{cs_i + is_i}, \text{ where } -1 \le C_i \le 1 \quad (2)$$

(2) Straightforwardness value

$$S_i = \frac{ss_i - sf_i}{ss_i + sf_i}, \text{ where } -1 \le S_i \le 1 \quad (3)$$

4.2.4 Trust Computation

The trust value of a node is computed using the quantified trust evaluation factors. The computation process involves an assignment of weights, which represent the importance of factors from 0, unimportant, to $+1$, most important, to the quantified trust factors. When W_C and W_S denote the weight of consistency and straightforwardness factor respectively, the trust value for n_i is computed by the following equation:

$$T_i = \frac{W_C C_i + W_S S_i}{W_C + W_S}, \quad (4)$$

where $0 \le W_C, W_S \le 1$ and they are not all 0. The weight may vary from application to application depending on the fact that on which security threat between a false negative attack and a false positive attack an application focuses. If the security against a false negative attack is considered more important in an application, a higher value may be assigned to W_S than that of W_C. If the security against a false positive attack is considered more important in an application, W_C may be higher than W_S. Else, W_C may be equal to W_S.

Initially, trust values of all sensor nodes are set to 0 as a neutral one. As the time elapses, they are continuously revalued. If a node temporarily malfunctions in communication or detecting events, such a temporary mistake has little influence on the trust value because it is computed accumulatively using counters by its neighbor nodes. However, if a node tries a false positive attack of data manipulation, or false negative attack for its selfish sake steadily, a trust value for that node is supposed to decrease and converge to -1. Thus, any compromised node who injects false data continuously, or shirks its responsibility of reporting sensing results for real events can be detected in this process.

4.3 Data Aggregation

Data aggregation is an essential process in wireless sensor networks to eliminate redundancy of sensing data, to minimize communication overhead, and to save energy. In addition, data aggregation can reduce effects of error in sensor readings in the network. In this process, sensor readings are aggregated in proportion to the trust values of the nodes per grid. Then, a median of the aggregated data is selected as a representative value and sent to the sink node.

4.3.1 Aggregator Selection

Prior to data aggregation, an aggregator is elected among sensor nodes per grid, which has the highest trust value in the grid using Aggregator Select procedure. At the network initialization phase before trust evaluation, aggregators are elected randomly by the sink node.

Procedure 3 *AggregatorSelect*$(Grid_{X,Y})$

```
T_temp = -1
for all n_i ∈ Grid_{X,Y} do
  if T_i > T_temp then
    temp = i
  end if
end for
return n_temp
```

An aggregator is responsible for aggregating and forwarding sensor readings from its grid to a sink node. An aggregator can be elected periodically with some application-dependent time interval by grid members, or elected by a sink node to defend against an aggregator compromise. We further dis-

cuss this problem in Section 7. After election, aggregators send their identifications to the sink and member nodes in their grids.

4.3.2 Trust Agreement

Because a trust value of a node is evaluated distributively by its neighbor nodes, trust agreement should be performed prior to data aggregation. An aggregator requests its one-hop neighbor n_j to notify the trust value of its member node n_i. If n_j has a knowledge of a trust value for n_i, n_j then replies to the aggregator with $\{ID_j, T_i\}$. The aggregator then gathers up all information for its member node n_i from the repliers and computes n_i 's representative trust value in proportion to the trust values of repliers themselves by this equation:

$$T_i = \frac{\sum_{j=1}^{l}(T_j+1)\times T_i^j}{\sum_{j=1}^{l}(T_j+1)}, \quad (5)$$

where l and T_i^j represent the number of repliers and a trust value for n_i notified from n_j, respectively.

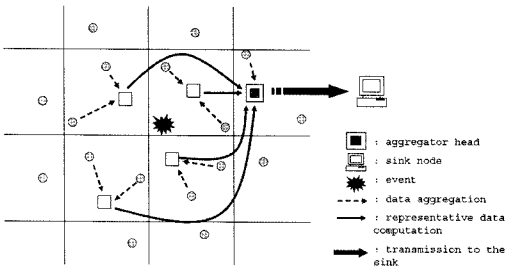


Fig. 3 Data aggregation process

4.3.3 Data Aggregation

Each aggregator n_a collects and aggregates all the received sensing data from its member nodes per grid in proportion to their trust values by this equation:

$$SR_{G_a} = \frac{\sum_{i=}^{m}(T_i+1)\times sd_i}{\sum_{i=1}^{m}(T_i+1)}, \quad (6)$$

where m represents the number of nodes in the grid. T_is are not all -1.

4.3.4 Representative Data Transmission

After aggregation, each aggregator forwards its aggregated data with its identification to aggregator head n_h, which is the nearest aggregator among them to the sink on the routing path as in Fig. 3. n_h then computes the median, Med_h, among the received data and sends it with identifications of all the participating aggregators to the sink node potentially traversing a large number of hops. The final report sent out by n_h to the sink looks like $\{Med_h, ID_{a_1}, ID_{a_2}, \ldots, ID_{a_u}\}$, where u is the number of participating grids.

5. Analysis

We analyze the proposed scheme in terms of its resilience and efficiency of excluding false data in the network under k-node attack in which k of the sensed observations can be corrupted before an estimator is applied. According to previous researches [5,12], median is very robust alternative to the other aggregation primitives such as average or min/max. So, we analyze the resilience of the proposed scheme compared with median as well as average.

Before analysis, we add some essential mathematical backgrounds on the classical estimation theory from [5].

5.1 Resilient Aggregation Theory

5.1.1 Estimation Theory

Let $x_1, \ldots, x_n$ denote a sequence of observations from a known parameterized distribution $p(X|\theta)$, where θ is a parameter whose distribution is not specified. Next, let $X_1, \ldots, X_n$ denote n random variables that are distributed according to $p(X|\theta)$ and conditionally independent given θ. Then, the goal of estimation problem is to estimate θ as accurately as possible.

An estimator is an algorithm $f: \mathbb{R}^n \rightarrow \mathbb{R}$, where $f(x_1, \ldots, x_n)$ is intended as an estimate of some real-valued function of θ. For simplicity, we assume that θ is real-valued and that we wish to estimate θ itself. Next, we define the random variable $\hat{\Theta} \overset{\text{def}}{=} f(X_1, \ldots, X_n)$. Then, the relevant metric to the proposed estimator is mean square error at

$$\theta\text{: } \mathrm{MSE}(f) \overset{\text{def}}{=} E[(\hat{\Theta}-\theta)^2|\theta]. \quad (7)$$

A minimal-variance unbiased estimator is an estimator where MSE(f) is minimal among all unbiased estimators. Thus, the mean square error can be a good measure of the inaccuracy of estimators.

5.1.2 Resilient Estimators

A k-node attack A is specified by a function $\tau_A : \mathbb{R}^n \rightarrow \mathbb{R}^n$ with the property that the sequence of observations vector x and $\tau_A(x)$ never differ at more than k positions. We can define the mean square error associated with A by

$$\mathrm{MSE}^*(f, A) \stackrel{\mathrm{def}}{=} E[(\widehat{\Theta}^* - \theta)^2 | \theta], \quad (8)$$

where $\widehat{\Theta}^* \stackrel{\mathrm{def}}{=} f(\tau_A(X_1, \ldots, X_n))$. Thus, $\widehat{\Theta}^*$ is a random variable that represents the aggregate in the presence of the k-node attack A, and $\mathrm{MSE}^*(f, A)$ is a measure of the inaccuracy of the aggregate after A's attack. If $\mathrm{MSE}^*(f, A) \gg \mathrm{MSE}(f)$, then the attack has succeeded noticeably in affecting the operation of the sensor networks. If $\mathrm{MSE}^*(f, A) \approx \mathrm{MSE}(f)$, the attack has had little effect on the network. Thus, we can think of an aggregation function f as a resilient aggregation function if $\mathrm{MSE}^*(f, A)$ grows slowly as a function of k.

5.1.3 Breakdown Point

If $S \subseteq \mathbb{R}$ is a set, the breakdown point is defined as

$$\epsilon^* \stackrel{\mathrm{def}}{=} \sup\{k/n : \mathrm{MSE}^*(f, \mathrm{k}) < \infty\},$$

where sup S is the smallest real number larger than or equal to every element of S. The breakdown point is informative when the estimator is unbounded.

In wireless sensor networks, the breakdown point indicates that fraction ϵ^* of nodes that can be captured before security breaks down. If an ϵ^* fraction of nodes are compromised, then the MSE becomes unbounded, so the adversary can drive the output of the aggregation operation to take on any value he would like. Consequently, the breakdown point is one measure of the security of an aggregation function against data spoofing attacks.

5.1.4 Data Model

The resilience of a function f depends not only on the choice of f, but also on the parameterized distribution $p(X_i|\theta)$. In practice, the exact distribution may vary from application to application. But, according to the study of Wagner [5], it seems reasonable to assume that the sensor readings X_i for continuous data come from i.i.d. random variables with the Gaussian distribution $N(\theta, \sigma^2)$ of mean θ and variance σ^2; whereas, for 0/1-valued data, X_i come from n i.i.d. r.v.'s with the Bernoulli distribution to make the analysis tractable.

5.2 Resilience Analysis

On inputs x_1, ..., x_n, let $x_{(1)}$, ..., $x_{(n)}$ denote the x_i-values placed in sorted order. When m denotes the average number of sensor nodes deployed per grid, an approximation for the variance of the proposed trust-based aggregation scheme is at most

$$\mathrm{MSE}(\textit{trust-based aggregation}) \approx \frac{m\sigma^2}{4\varphi(0)^2 n} = \frac{m\pi}{2} \times \frac{\sigma^2}{n},$$

in the worst case where local aggregation per grid just acts as the average which has breakdown point $\epsilon^* = 0$. Likewise, it can be simply induced that

$$\mathrm{MSE}(\textit{trust-based aggregation}) \approx \frac{\sigma^2}{4\varphi(0)^2 mn} = \frac{\pi}{2m} \times \frac{\sigma^2}{n},$$

in the best case where $m-1$ false data from adversaries are excluded during local aggregation per grid.

A k-node attack can increase the median and trust-based aggregation scheme to at most $x_{(r+k)}$ and $[x_{(r+k/m)}, x_{(r+mk)}]$, respectively, so

$$\mathrm{MSE}^*(\textit{median}, k) \approx (\frac{\pi}{2} + \frac{k^2}{2\pi}) \times \frac{\sigma^2}{n},$$

$$\mathrm{MSE}^*(\textit{trust-based aggregation}, k) \approx [(\frac{\pi}{2} + \frac{k^2}{2m^2\pi}) \times \frac{\sigma^2}{n}, (\frac{\pi}{2} + \frac{m^2k^2}{2\pi}) \times \frac{\sigma^2}{n}].$$

Thus, the interpretation is that, in the presence of adversaries, compromised nodes produce a gradual increase in the error term for the median and the trust-based aggregation scheme by a resilience factor of $\frac{\pi}{2} + \frac{k^2}{2\pi}$ and $[\frac{\pi}{2} + \frac{k^2}{2m^2\pi}, \frac{\pi}{2} + \frac{m^2k^2}{2\pi}]$,

respectively. In the absence of attack, the error terms for the median and the trust-based aggregation scheme are only slightly larger by a factor of $\frac{\pi}{2}$ and $[\frac{\pi}{2m}, \frac{m\pi}{2}]$, respectively, than the error term for the average. Also, the breakdown point of the median is $\epsilon^* = 1/2$ and the breakdown point of the trust-based aggregation scheme ranges from $\epsilon^* = 1/2m$ to $\epsilon^* = 1-1/2m = (2m-1)/2m$ based on the estimated trust values of adversaries in the wireless sensor networks. The analysis result is shown in Table 1.

Table 1 shows aggregation schemes, their mean square error term in the absence of attacks, resilience against k-node attack, and breakdown point. The resilience factor is the bias order coefficient which determines whether the function can be computed meaningfully and securely in the presence of up to k compromised or malicious nodes. The smaller resilience factor means the greater security. It is also important to note that the breakdown point of the proposed scheme ranges from $\epsilon^* = 1/2m$ to $\epsilon^* = (2m-1)/2m$ based on the estimated trust values of adversaries in the network. In case that the estimated trust values of adversaries are 1, that is trustworthiness of the sensor nodes are not evaluated at all, the security of the proposed scheme is worse than the median; whereas, in case that the estimated trust values of adversaries are -1, that is they are perfectly distinguished from normal nodes, the security of the proposed scheme is much better than the median as long as $m>1$. The resilience of the proposed scheme depends not only on the parameterized distribution, but also on the correctness of the trust evaluation.

5.3 Cost Analysis

Now we analyze the cost of the proposed scheme compared with a tree-based aggregation scheme which uses a same routing and aggregation path on the same network topology as the proposed scheme but the trust evaluation process and local grid-based data aggregation. Intermediate nodes and a root of the aggregation tree correspond to each aggregator and an aggregator head of the proposed scheme, respectively. In this work we focus on storage, computation, and communication overhead.

The notations A and C represent the amount of computations for an aggregator to agree the trust value for a member node and aggregate data in a grid, respectively. T represents the amount of computations for a node to evaluate a trust value of a neighbor node. m and l denote the average number of sensor nodes per grid and one-hop neighbor nodes, respectively. The proposed scheme then requires the following overhead when N sensor nodes detect an event:

- An aggregator needs to store m sensing data, and an aggregator head needs to store $u(=\frac{N}{m})$ locally aggregated data in the proposed scheme; whereas, a root of the tree needs to store N

Table 1 Resilience of the aggregation schemes

Aggregation f	MSE(f)	Resilience	Break down point ϵ^*	Trust values of adversaries
average	$\frac{\sigma^2}{n}$	∞	0	-
median	$\frac{\pi}{2} \cdot \frac{\sigma^2}{n}$	if $k < \frac{n}{2} : \frac{\pi}{2} + \frac{k^2}{2\pi}$ if $k > \frac{n}{2} : \infty$	1/2	-
proposed scheme	$\frac{m\pi}{2} \cdot \frac{\sigma^2}{n}$	if $k < \frac{n}{2m} : \frac{\pi}{2} + \frac{m^2k^2}{2\pi}$ if $k > \frac{n}{2m} : \infty$	$1/2m$	1
	$\frac{\pi}{2m} \cdot \frac{\sigma^2}{n}$	if $k < \frac{(2m-1)n}{2m} : \frac{\pi}{2} + \frac{k^2}{2m^2\pi}$ if $k > \frac{(2m-1)n}{2m} : \infty$	$(2m-1)/2m$	-1

sensing data in the tree-based aggregation scheme.

- A node needs at most $l \times T$ computations for trust evaluation and an aggregator requires $mA+C$ computations for data aggregation.

- $(2l+m+1)u$ communications are required for trust agreement, data aggregation, and aggregated data transmission; whereas, $(m+1)u$ communications are required in the tree-based aggregation scheme.

The proposed scheme requires additional communication and computation overhead for the trust evaluation over the naive tree-based aggregation scheme. However, it seems reasonable to expect that the additional cost is much cheaper than that of the cryptographic approaches such as public key cryptosystems, or various key pre-distribution schemes.

6. Simulation

6.1 Simulation Background

We simulate the proposed scheme in a temperature sensing network in C. The environments of the simulation are as follows: 300 sensor nodes are uniformly distributed at the sensing area whose size is 500×500. A grid size is 50×50. Sensing range and communication range of a node is 70. In this simulation, we mainly focus on evaluating the effect of the proposed scheme under a false positive attack. Initially, trust values of all sensor nodes are set to 0, that is all sensor nodes are taken for neutral before evaluating trustworthiness.

To make a practical simulation of temperature sensing system, Stefan-Boltzman Law is adopted, which indicates that for an ideal blackbody the radiation per unit area is proportional to fourth power of the absolute temperature. Thus, total receiving energy of an object B, whose radius is R_B and distance from A is r, from object A per unit time is

$$L_B = L_A \times \frac{\pi R_B^2}{4\pi r^2} = \sigma T_A^4 \times 4\pi R_A^2 \times \frac{\pi R_B^2}{4\pi r^2}. \quad (9)$$

Temperature data in the simulation are modeled by (9), especially the property that the receiving radiation energy is proportional to $\frac{1}{r^2}$.

6.2 Resilience of the Trust-based Aggregation

In this simulation, the resilience of each estimator is shown. 39 sensor nodes which are uniformly distributed in 13 neighboring grids near an event can sense it (n = 39 and m = 3). Attackers notify their neighbor nodes of sensing values 10 times higher like the previous simulation. k attackers are randomly chosen among the 39 participant nodes under k-node attack.

6.2.1 Aggregation with Static Trust Value

The adversaries' trust values are real-valued from -1 to 1, however, we especially choose three discrete trust values -1, 0, and 1 to make the simulation tractable. Trust values of normal sensor nodes are set to 1, that is the system is assumed to totally trust sensed data from the normal nodes.

The simulation result is shown in Fig. 4. As we analyzed, average cannot be computed meaningfully in the presence of a malicious sensor node of which the breakdown point is 0. In median, the breakdown number of k is 20; whereas, the breakdown number of k in the proposed aggregation scheme is 6 when the adversaries' trust values are 1, and 33 when their trust values are -1, respectively. Fig. 4 shows that the resilience analysis in Section 5.2 matches well with the simulation result.

Next, we measure the inaccuracy of each estimator by mean square error (MSE), and we can think of the MSE as representing a typical value of the error term $|\hat{\Theta}-\theta|$. The MSE characterizes the quality of each estimator. Fig. 5 shows the MSE of each estimator.

The MSE is estimated based on the aggregation result of each estimator under k-node attack. The

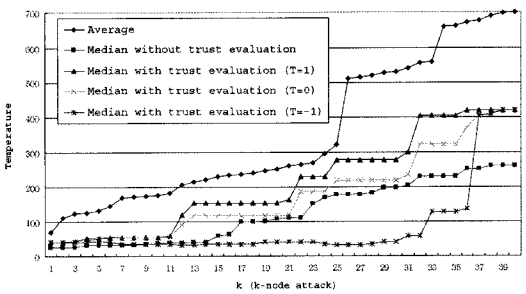


Fig. 4 Aggregation results under k-node attack with static trust values

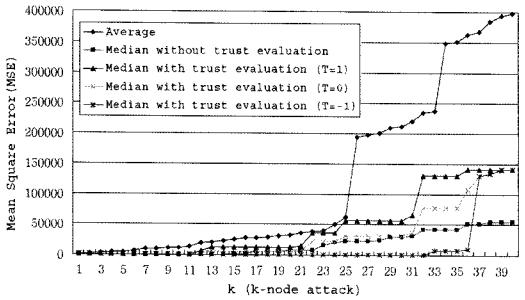


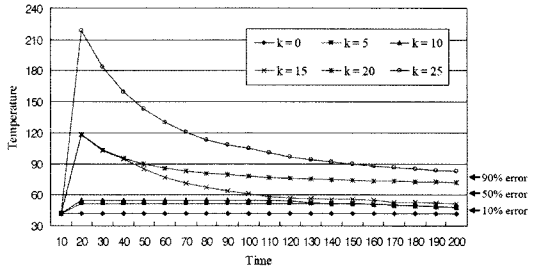
Fig. 5 Mean square error under k-node attack with static turst values

hidden parameters, θs, of the estimators are defined as the original aggregated data without any attack. Based on the pure parameters, we measure the spread of the aggregation schemes under k-node attack. In Fig. 5, the spread of a line represents the inaccuracy of an estimator. Like the aggregation results in Fig. 4, MSEs of the estimators tend to increase steeply around the breakdown point.

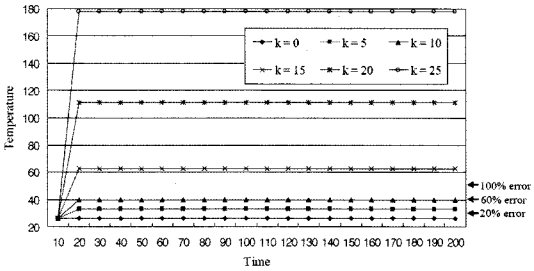
6.2.2 Aggregation with Dynamic Trust Value

Next simulation is to measure the resilience of the proposed scheme under k-node attack as the trust values of the nodes are evaluated dynamically. In this simulation, a same event occurs every 10 second. Attackers start to broadcast their sensed data ten times higher after 20 seconds.

As the time elapses, the reported temperatures are aggregated as shown in Fig. 6. The dotted lines of Fig. 6 represent the deviated error rate from original aggregated data by every increasing 20%. In case of the proposed trust-based aggregation scheme of Fig. 6(a), when k=0, the aggregated data represent 41.8°C. Under 5-node and 10-node attack, the compromised data can converge to 47.5°C whose error rate deviated from the original data is about 10% in 200 seconds. Under 15-node attack, the compromised data can converge to 51.4°C whose error rate is about 20%. Under 20-node and 25-node attack, the compromised data can converge to 74.9°C and 82.6°C whose error rates are approximately 70% and 90%, respectively. In case of the median of Fig. 6(b), when k=0, the original median value represents 26.0°C. Under 5-node attack and 10-node attack, error rates of the median are larger than 30% and 50% from the



(a) Trust-based aggregation



(b) Median

Fig. 6 Aggregation results unde k-node attack with dynamic trust values

original data, respectively. When k=15, the error rate already exceeds 140%.

Consequently, the proposed scheme shows higher robustness than median. It is important to note that security of the proposed scheme depends on the accuracy of the trust evaluation. If sensor nodes evaluate the trustworthiness of their neighbor nodes accurately, false data injected from adversaries can be filtered out more effectively than median which is known to be the robustest estimator among the conventional aggregate primitives.

7. Discussion: Stealthy Attack

Node compromise is one of the most challenging problems in sensor network security. This is also the case with our scheme. For example, if an aggregator head is compromised, the compromised aggregator head can easily report significantly biased or false readings to the sink node, instead of real aggregated results. Furthermore, if an intelligent attacker who obtained high trust value at the beginning is elected as an aggregator head, it can then also report incorrect aggregated results arbitrarily far from the true readings to the sink node,

that is a stealthy attack. Even if the proposed scheme can mitigate the cheating of a number of compromised nodes as we analyzed in Section 5.2, however, cheating from an aggregator head cannot be prevented without an additional security mechanism built-in. Therefore, an additional integrity check mechanism is necessary to avoid over-reliance on the aggregator head.

To defend against the node compromise, several methods have been proposed. A. Mahimakar and T. S. Rapparport proposed SecureDAV protocol that ensures that a sink node does not accept faulty readings for an upper bound of t compromised nodes within a cluster using threshold signatures based on elliptic curve cryptosystems [24]. Another approach is an en-route filtering framework that multiple detecting nodes jointly generate a complete report with the required number of MACs, then the intermediate nodes detect and discard bogus reports injected by compromised nodes [7,9,10]. However, these schemes not only put a cryptographically heavy processing load on resource-limited sensor nodes but also cannot identify compromised nodes trying stealthy attack.

We use an interactive proof scheme in which a sink node needs to randomly sample some raw data and check to ensure that the committed data is a good representation of the true values like the way of SIA [6] to defend against the stealthy attack under the assumption that each sensor node shares a separate secret key with a sink node. When $H_K(M)$ is represented as a keyed hash function that uses key K on input M, and k_i denotes a shared secret key between n_i and a sink node, each aggregator n_a sends its aggregated data with their hashed values, $\{ID_a,\ SR_{G_a},\ H_{k_a}(SR_{G_a})\}$, to an aggregator head to verify the committed data. The aggregator head then computes the median among SR_{G_a}s and commits to the values by Merkle hash tree construction as in Fig. 7. In Fig. 7, m_i is the sorted sequence of the SR_{G_a} with respect to their sensing values so that $m_i \le m_{i+1}$. Each $H_{k_a}(SR_{G_a})$ is placed at the leaves of the tree and each internal node is computed as the hash value of the concatenation of the two child nodes. The root of the tree is *commitment* of the collected data. The aggregator head n_h then sends $\{Med_h,\ \{ID_{a_1},\ ID_{a_2},\ ...,\ ID_{a_u}\},\ commitment\}$ to the sink node, where $\{ID_{a_1},\ ID_{a_2},\ ...,\ ID_{a_u}\}$ is sorted sequence of IDs of participating aggregators by their aggregated values, which is corresponding to the sorted sequence of m_is. The sink node can authenticate any leaf value by verifying that the leaf value is used to derive the root value. For example, to authenticate m_3 reported from aggregator n_a, the aggregator head sends M_3 along with M_4, M_{12}, M_{5678}, and the corresponding aggregator n_a sends m_3. If the following equality holds, m_3 is authentic: $M_3 = H_{k_a}(m_3)$ and $commitment = H(H(M_{12}||H(M_3||M_4))||M_{5678})$.

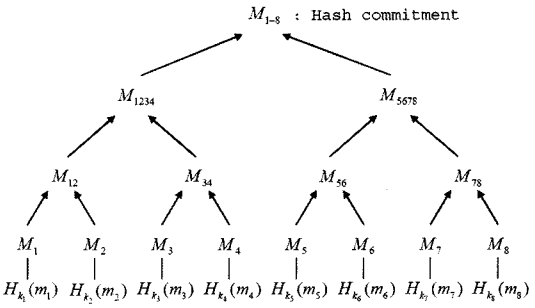


Fig. 7 Merkel hash tree construction

In the interactive proof, the sink node verifies the correctness of the alleged median *Med* by checking that the *Med* is close to the median of committed sequence. More precisely, when ε denotes the approximation error which describes the quality of a reported value, the sink node checks that the position of *Med* in the sorted sequence $m_1, \ldots, m_u$ reported from aggregator head is within $\varepsilon \cdot u$ of $u/2$, that is ε-approximation, using following median-checking procedure *MedianCheck* proposed by [6].

Procedure 4 $MedianCheck(u, Med, \varepsilon)$
request $m_{u/2}$
if $m_{u/2} \neq Med$ **then**
  return REJECT
end if
for $i = 1$ to $1/\varepsilon$ **do**
  pick $j \in_R \{1 \ldots u\} \backslash \{u/2\}$
  request m_j

if $j < u/2$ and $m_j > Med$ **then**
  return REJECT
end if
if $j > u/2$ and $m_j < Med$ **then**
  return REJECT
end if
end for
return ACCEPT

If the position ρ of the Med in the sorted sequence satisfies $|p-n/2| > \varepsilon \cdot u$, the result is "REJECT" with probability at least $(1-\varepsilon)^{1/\varepsilon} \geq 1-1/e > 1/2$. In addition, each request for m_j in the *MedianCheck* procedure needs two elements, M_j from the aggregator head and m_j from the corresponding aggregator, to verify its correctness by Merkle hash tree construction. So, by requesting $O(1/\varepsilon)$ elements, we can check that the reported value is an ε-approximation of the median with a constant probability of detecting a cheating aggregator head. Compared with the SIA method which needs $O(\log u/\varepsilon)$ elements to check ε-approximation of the median, the proposed method improves the communication complexity by eliminating a committed sequence checking procedure of the SIA, which requires $O(\log u/\varepsilon)$ samples.

8. Conclusion

To identify compromised nodes and thwart the malicious behaviors of adversaries launching various attacks is one of the challenging issues in the wireless sensor network security. Because a false negative or false positive attack from a small number of adversaries can drain out the finite amount of energy resources in battery-powered sensor networks and aggravate the functionality of the whole networks critically, some security mechanisms should be built-in to defend against such attacks in the sensor networks. However, because the compromised node knows the secret information, conventional cryptographic mechanisms cannot solve the real root of the problem of node compromise.

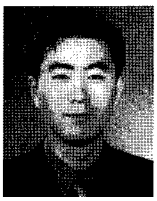
So, a novel trust-based secure aggregation scheme is proposed to make a sensor network resilient against false data injection and selfish behaviors of malicious nodes. The proposed trust evaluation scheme is best-suited to settings where there is plenty of redundancy in the data of sensor nodes, so that we can crosscheck sensor readings for consistency. Wireless sensor networks tend to consist of a large scale of cheap and crude sensors, which are exactly where our trust evaluation scheme is most appropriate. As the degree of redundancy in sensing data increases, the proposed scheme would be more applicable to a variety of applications.

The proposed trust evaluation and secure aggregation scheme does not employ cryptographic approaches or certification mechanisms, so it is light enough to fit well with wireless sensor networks without cryptographic computation overheads. In addition, as we analyzed, the proposed aggregation scheme could be a more resilient alternative to median, which is known to be the robustest conventional aggregation function. The simulation also shows that the proposed scheme achieves better security in the effectiveness of filtering false data than the median as the time elapses and trustworthiness of nodes are identified. So, the proposed scheme can offer an alternative security technique to the limited scope of the previous cryptographic approaches.

References

[1] H. Chan and A. Perrig, Security and Privacy in Sensor Networks, IEEE Computer 2003.
[2] A. Pirzada, C. McDonald, Establishing Trust In Pure Ad-hoc Networks, Proceedings of the 27th conference on Australasian computer science, 2004.
[3] C. Karlof, D. Wagner, Secure Routing in Wireless Sensor Networks: Attacks and Countermeasures, NEST 2003.
[4] A. Perrig, J. Stankovic, D. Wagner, Security in Wireless Sensor Networks, Communication of the ACM, June 2004.
[5] David Wagner, Resilient Aggregation in Sensor Networks, ACM Workshop on Security of Ad Hoc and Sensor Networks (SASN '04), October 25, 2004.
[6] B. Przydatek, D. Song, A. Perrig, SIA: Secure Information Aggregation in Sensor Networks, SenSys 2003.
[7] H. Yang, F. Ye, Y. Yuan, S. Lu, W. Arbaugh, Toward Resilient Security in Wireless Sensor Networks, Proceedings of the 6th ACM International Symposium on Mobile Ad hoc Networking and Computing, Urbana-Champaign, Illinois, USA, May 2005.

[8] L. Hu and D. Evans, Secure Aggregation for Wireless Networks, In Workshop on Security and Assurance in Ad hoc Networks. January 2003.
[9] S. Zhu, S. Setia, S. Jajodia, P. Ning, An Interleaved Hop-by-Hop Authentication Scheme for Filtering of Injected False Data in Sensor Networks, Proceedings of IEEE Symposium on Security and Privacy, Oakland, California, May 2004.
[10] F. Ye, H. Luo, L. Zhang, Statistical En-route Detection and Filtering of Injected False Data in Sensor Networks, Proceedings of IEEE INFOCOM 2004.
[11] A. Perrig, R. Szewczyk, V. Wen, D. Culler, J.D. Tygar, SPINS: Security Protocols for Sensor Networks, Wireless Networks Journal (WINE), September 2002.
[12] N. Shrivastava, C. Buragohain, D. Agrawal, S. Suri, Medians and Beyond: New Aggregation Techniques for Sensor Networks, Proceedings of the Second ACM Conference on Embedded Networked Sensor Systems (SenSys 2004), August 16 2004.
[13] H. Chan, A. Perrig, D. Song, Random key predistribution schemes for sensor networks, IEEE Symposium on Security and Privacy, Berkely, California, May 11-14 2003, pp. 197-213.
[14] W. Du, J. Deng, Y.S. Han, P.K. Varshney, A pairwise key pre-distribution scheme for wireless sensor networks, Proceedings of the 10th ACM Conference on Computer and Communications Security (CCS), Washington, DC, USA, October 27-31 2003, pp. 42-51.
[15] L. Buttyan, P. Schaffer, I. Vajda, Resilient Aggregation with Attack Detection in Sensor Networks, Proceedings of the Fourth Annual IEEE International Conference on Pervasive Computing and Communications Workshops, 2006.
[16] Z. Yan, P. Zhang, T. Virtanen, Trust Evaluation Based Security Solution in Ad Hoc Networks, NordSec 2003, Proceedings of the Seventh Nordic Workshop on Secure IT Systems, 15th-17th October 2003.
[17] R. Pickholtz, D. Schilling, L. Milstein, Theory of Spread Spectrum Communications - A Tutorial, IEEE Transactions on Communications, pp. 855-884, May 1982.
[18] S. B. Wicker, M. D. Bartz, Type-II Hybrid-ARQ Protocols Using Punctured MDS Codes, Proceedings of IEEE Transactions on Communications, April 1994.
[19] Z. Li, W. Trappe, Y. Zhang, B. Nath, Robust Statistical Methods for Securing Wireless Localization in Sensor Networks, IPSN 2005, Los Angeles, April 2005.
[20] X. Ji, H. Zha, Robust Sensor Localization Algorithm in Wireless Ad-hoc Sensor Networks, Proceedings of the 12th International Conference on Computer Communications and Networks (ICCCN03), 2003.
[21] L. Lazos, R. Poovendran, SeRLoc: Secure Range-Independent Localiztion for Wireless Sensor Networks, Proceedings of the 2004 ACM Workshop on Wireless Security, pp. 21-30, 2004.
[22] N. Sastry, U. Shankar, D. Wagner, Secure Verification of Location Claims, Proceedings of the 2003 ACM workshop on Wireless security.
[23] S.S. Doumit, D.P. Agrawal, Self-Organized Criticality and Stochastic learning based intrusion detection system for wireless sensor networks, Military Communications Conference, 2003. MILCOM '03. 2003 IEEE, pp. 609-614.
[24] A. Mahimkar, T. S. Rappaport, SecureDAV: A Secure Data Aggregation and Verification Protocol for Sensor Networks, Proceedings of IEEE Global Telecommunications Conference (Globecom) 2004, Dallas, TX, Nov 29 - Dec 3, 2004.



허 준 범

2001년 고려대학교 컴퓨터교육과 학사 2005년 한국과학기술원 전산학과 석사 2005년~현재 한국과학기술원 전산학과 박사과정. 관심분야는 네트워크 보안, 정보보안, 암호학

이 윤 호

2000년 한국과학기술원 전산학과 학사 2002년 한국과학기술원 전자전산학과 석사. 2006년 한국과학기술원 전자전산학과 박사. 2006년~2007년 한국과학기술원 정보전자연구소 박사후연구원. 2007년~현재 GTISC(GeorgiaTech Information Security Center) 방문연구원. 관심분야는 네트워크 보안, 멀티미디어 보안, 암호학

윤 현 수

1979년 서울대학교 전자공학과 학사. 1981년 한국과학기술원 전산학과 석사. 1988년 미국 오하이오 주립대학 전산학과 박사. 1989년~현재 한국과학기술원 교수 관심분야는 병렬 컴퓨터 구조, 무선 이동통신, 애드혹 및 센서 네트워크, 정보보안