CERIAS Tech Report 2015-13

Distance-based Trustworthiness Assessment for Sensors in Wireless Sensor Networks

by Jongho Won, Elisa Bertino
Center for Education and Research
Information Assurance and Security
Purdue University, West Lafayette, IN 47907-2086

Distance-based Trustworthiness Assessment for Sensors in Wireless Sensor Networks

Jongho Won and Elisa Bertino

Purdue University, Computer Science, West Lafayette, Indiana, USA
{won12,bertino}@purdue.edu
https://cs.purdue.edu

Abstract. Wireless Sensor Networks (WSNs) have been substituting for human senses to make human lives better by monitoring the environment and providing intelligence. Collected sensor data are used to make decisions as a human does. Therefore, providing trustworthy sensor data is crucial to make correct decisions. However, faulty sensors can give incorrect information. In addition, since sensors are usually deployed in unattended areas and can be compromised, cryptographic approaches are insufficient. To address this problem, we propose a distance-based trustworthiness assessment scheme. In our scheme, a centralized trust assessment module outputs an absolute trust score of each sensed value and the trust score of each sensor. The trust scores of sensed values are calculated based on the differences of sensed values provided by a sensor and its neighbors and the physical distances from the neighbors. Our simulation results show that our scheme outputs practical and accurate trust scores in a realistic environment where the sensed values of interest gradually change over the monitored areas.

Keywords: Trustworthiness assessment in wireless sensor networks, sensor trust assessment, sensor trust management

1 Introduction

Along with the advance in sensors, network technologies and embedded devices, sensor nodes in Wireless Sensor Networks (WSNs) have now become tiny and inexpensive. In the near future, WSNs will behave as a digital skin providing a virtual sense for physical environments. Collected sensed data can be utilized for many critical tasks ranging from military tasks to civilian tasks such as surveillance, fire detection, industrial facility monitoring and soil monitoring for precision agriculture. In such applications, hundreds to thousands of tiny sensor nodes are densely deployed and large amounts of sensed data are collected. The collected sensed data are then used to make critical decisions.

However, since sensors are usually made with cheap hardware and deployed in unattended hostile areas, they are exposed to the risks of being compromised by attackers. Once sensor nodes are compromised, they may endanger the system by injecting malicious false data. In addition, as pointed out in [5], in real

applications, lots of incorrect sensed data are reported by faulty sensors. Therefore, providing indications about the trustworthiness of collected data to data users is crucial in order for these users to make correct decisions.

Approaches to score sensors or sensed data based on reputation or trust management schemes have been proposed. Such approaches can be categorized into ~~two approaches:~~ *distributed* and *centralized* approaches. In the distributed approaches [9, 7, 5], each sensor has its own trust management module which evaluates the trust scores of its neighbors. On the other hand, centralized approaches [6] assess the trustworthiness of all sensors using the collected sensed data from the system perspective. Since WSNs are self-organized and cooperatively operated in a distributed manner for networking or data aggregation, many schemes have focused on how each sensor node builds trust scores about its neighbors. For example, each sensor counts selfish routing misbehavior of its neighbors or compares its sensed value with the sensed values of its neighbors. Then, each sensor node establishes the trust scores of neighbors from its own point of view. While a distributed approach is best suited for local decisions such as routing and data aggregation, a centralized approach is required in order to make decisions from the perspective of system operations. For example, by using the trust scores about sensors, system administrators can execute corrective follow-up actions such as replacing faulty or abnormal sensors, i.e. sensors with low trust scores, with new sensors. In this paper, we focus on the centralized approach.

Although previous approaches provide effective methodologies for trustworthiness assessment of sensors in WSNs, none of them have taken into account the physical distances among each pair of sensors for calculating their trust scores. In this work, we focus on the fact that the closer two sensors are, the more consistent their sensed values are. A centralized trust assessment module then compute absolute trust scores of sensors based on their sensed values and their physical distances. The simulation results show that our trustworthiness assessment scheme provides practical and accurate trust scores in realistic environments where the sensed values of interest gradually change over the monitored areas.

The rest of the paper is organized as follows. Section 2 discusses related work and Section 3 introduces some motivating examples. Section 4 presents our distance-based trustworthiness assessment scheme. Section 5 reports the simulation results and Section 6 outlines conclusions and future work.

2 Related Work

The self-organizing nature of WSNs calls for distributed trust management schemes [9, 7, 5]. Zhang et al. [9] propose a trust-based framework for secure data aggregation. The trustworthiness of each sensor in one cluster is evaluated by using an information theoretic metrics under the assumption that multiple nodes in one cluster sense the mean of the physical environment parameter of interest independently. Probst et al. [7] present a trust establishment scheme based

on computing statistical trust and a confidence interval around the trust based on direct and indirect experiences of neighbor's behavior. Ganeriwal et al. [5] propose a framework by which each sensor node maintains reputation metrics for neighbors. Using an outlier detection algorithm, the actions of neighbors are classified as either cooperative or noncooperative and then the classification results are given as input to a beta reputation system for the trust representation of neighbors. Notice that such distributed schemes require additional memory and computational resources for sensors. Furthermore, using ~~them~~ for already deployed WSNs is difficult since they require software updates all sensor nodes.

Lim et al. [6] proposed a centralized scheme which evaluates the trust score of values and nodes based on the sensed values and their provenance. The trust score of a sensed value and the trust score of a sensor node periodically evolve according to a cyclic framework by affecting each other. The scheme assumes that the set of sensed values which are affected by an event can be determined. Also, it assumes that the set of sensed values are equally affected by the event. Based on these assumptions, the scheme calculates the mean (μ) and standard deviation (σ) of all sensed values which are affected by the same event. Using μ and σ, the distribution is modeled as a normal distribution $\mathcal{N}(\mu, \sigma)$. Then, each sensed value is scored based on the distribution. That is, the closer the sensed value provided by a sensor is to the mean, the higher trust score is assigned to the sensor. However, in ordinary monitoring applications, this approach has four problems. First, defining an event may be impossible in many applications or contexts. Second, determining the set of sensed values which are affected by an event is difficult. Third, even if we can identify an event and sensors affected by the event, the event does not equally affect all these sensors. Fourth, the scheme assigns relative trust scores to sensors since the scores are calculated based on the distribution. That is, even though all sensors are working well, low trust scores may be assigned to some sensors. These problems are discussed in detail in Section 3.

Unlike [6], in this paper, we do not consider the provenance of a sensed value. In [6], when a sensed value passes through intermediate sensor nodes, the trust score of the sensed value is dominated by the worst node with the smallest trust score since a malicious intermediate node may change the sensed value passing the node. However, this assumption is too conservative since, as discussed in [5], abnormal sensed values can be generated due to other reasons such as a low voltage level, a faulty sensor module or abnormal natural phenomenon. We believe that compromised nodes can be detected by distributed schemes [5, 8][1].

None of the previous approaches take into account the correlation between sensed values and their physical distances in the computation of the trust scores. The physical distances between sensors are known by the system administrator since location information of sensors as well as their sensed values are important factors to be considered for decisions.

[1] Notice that distributed schemes ~~are compatible~~ with centralized schemes to make the system more robust.

3 Motivating Examples

The typical applications of WSNs monitor large areas with hundreds or thousands of sensors. In these applications, the sensed values reported by sensors at a specific area may be very different from the sensed values reported by sensors at a different area. For instance, consider the situation where sensors monitor temperature in a forest reserve as shown in Fig. 1. At night all sensors may

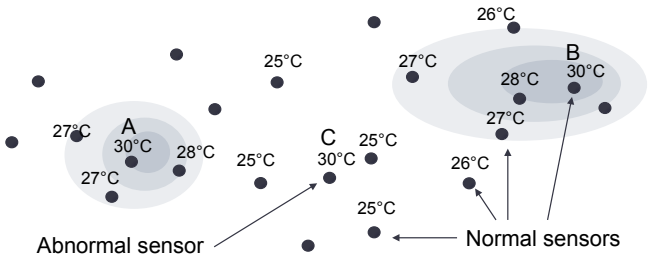


Fig. 1. An illustration of WSNs monitoring temperature

provide similar temperature values. However, in the daytime, the temperature values may differ according to the presence of direct sunlight or the angle between the sun's rays and the surface. Assume that sensor A and B are normal, but sensor C is abnormal. Sensor A and sensor B give a temperature of 30°C while most of sensors, except sensor C, give a temperature of under 30°C. In this situation, we cannot determine the set of sensors which are affected by an event. If possible, the sensors may not be equally influenced by the event. Nonetheless,

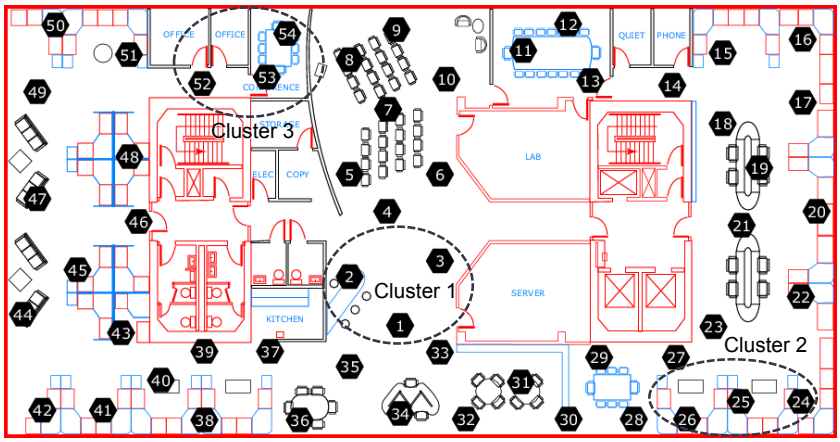
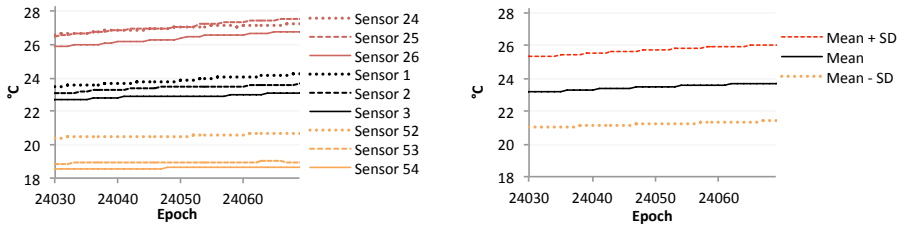


Fig. 2. The topology of sensors in the Intel lab

if we define this kind of situation (without a specific event) as an 'event' and utilize the normal distribution-based approach [6], the event will include the entire sensed values. As a result, low trust scores will be assigned to sensor A and B even if the values they provide are correct. Their trust scores may increase at night since all sensors may provide similar temperature values and trust scores are periodically re-assessed. However, the trust scores of sensor A and B will eventually become low throughout the cyclic procedure if temperature values at sensor A and B are higher than others in every daytime since such bad effects are accumulated.

This phenomenon can be verified in a real test-bed experiment. We analyzed the data collected from 54 sensors deployed in the Intel Berkeley Research lab [1]. As shown in Fig. 2, we focused on 9 sensors in three different areas. Sensor 1, 2 and 3 (cluster 1) are located in the center of the lab. Sensor 24, 25 and 26 (cluster 2) are located at the corner of the lab and sensor 52, 53 and 54 (cluster 3) are located in a conference room. Fig. 3(a) shows the temperature values of



(a) The temperature values of 9 sensors in 3 different areas

(b) The mean and standard deviation of temperature values from 54 sensors

Fig. 3. Intel lab data from 9:13 AM to 9:32 AM

the 9 sensors from 9:13 AM to 9:32 AM and Fig. 3(b) shows the mean value and standard deviation of temperature values generated by all sensors. The sensors in cluster 1 output temperature values near the mean while the sensors in cluster 2 and 3 output temperature values far from the mean value. These differences are due to various factors such as heat from PCs, the positions of air-conditioners or heat from the sun. Such experimental results confirm two facts. First, even though there is no specific event, some sensors output higher/lower temperature values than the mean plus/minus the standard deviation. Therefore, sensors in cluster 2 and 3 will get low trust scores if the normal distribution-based approach [6] is utilized. Second, sensors which are close to each other produces similar outputs due to the heat diffusion process. Although we did not include the results of humidity due to the page limit, the same phenomena were observed.

In this paper, we utilize the fact that the sensed value of a sensor is consistent with the sensed values of its neighbors. In Fig. 1, the trustworthiness of sensor A and sensor B is supported by their neighbors, while the trustworthiness of sensor C is not supported by its neighbors.

4 Distance-based Trustworthiness Assessment

In this section, we present our distance-based trustworthiness assessment for sensors based on their sensed values and their physical distances.

4.1 Overview of the Scheme

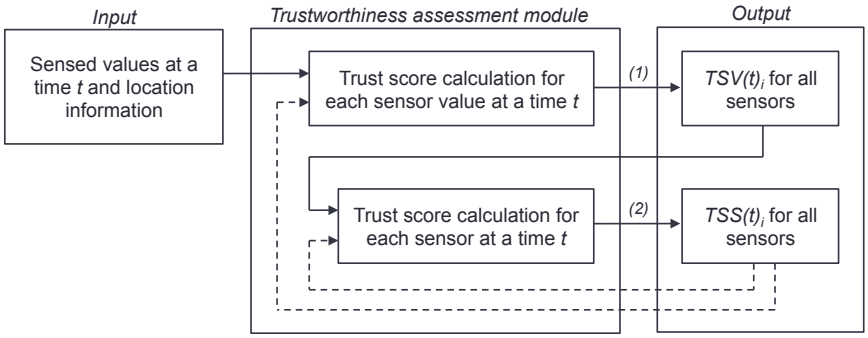


Fig. 4. Overview of the trust score calculation procedure. $TSV(t)_i$ is the trust score of the sensed value generated by sensor i at a time t. $TSS(t)_i$ is the trust score of sensor i at a time t.

Our trustworthiness assessment has two steps. In the first step, the trust score of each sensed value generated by sensor i at a time t, i.e., $TSV(t)_i$, is calculated by using as input: all sensed values at a time t, sensor location information, and the previous trust scores. In the second step, the trust score of sensor i at a time t, i.e., $TSS(t)_i$, is calculated using the previous trust score of sensor i, i.e., $TSS(t-1)_i$, and $TSV(t)_i$. The trust scores of sensors evolve through this cyclic framework as time passes. The trust scores in our scheme range in the interval [0,1].

4.2 Details of the Scheme

In the first step, the trust score of a sensed value generated by sensor i, $TSV(t)_i$, is derived by calculating the weighted mean (τ) of differences between the value of sensor i and the values of the i's neighbors as follows:

$$TSV(t)_i = \frac{1}{1+|\tau|}, \quad \tau = \frac{\sum_{j=0}^{n} \frac{(v(t)_i - v(t)_j) \times TSS(t-1)_j^{\beta}}{d_{i,j}^{\alpha}}}{\sum_{j=0}^{n} \frac{TSS(t-1)_j^{\beta}}{d_{i,j}^{\alpha}}}, \tag{1}$$

where n is the number of neighbors of sensor i, $v(t)_i$ is a sensed value provided by sensor i at a time t and $d_{i,j}$ is the distance between i and j. There are two weighting factors. One is the distance between sensor i and its neighbors and the

other is the trust score of sensor i's neighbors. α (≥ 0) is a system parameter which controls the effect of $d_{i,j}$. The bigger α is, the larger the influence of neighbors which are close to i becomes. β (≥ 0) is also a system parameter which controls the effect of the previous trust score of the neighbor, i.e., $TSS(t-1)_j$. The bigger β is, the larger the influence of neighbors with high trust scores becomes. If α and β are 0, τ is just the mean of value differences regardless of $d_{i,j}$ and $TSS(t-1)_j$, respectively. If the sensed value $v(t)_i$ is consistent with the sensed values of its neighbor, $TSV(t)_i$ becomes close to 1. Otherwise, $TSV(t)_i$ becomes close to 0.

In the second step, to obtain the trust score of sensor i at a time t, i.e., $TSS(t)_i$, the current trust score of the sensed value provided by sensor i, i.e., $TSV(t)_i$, and the previously accumulated historic score $TSS(t-1)_i$ are taken into account as follows:

$$TSS(t)_i = w \times TSV(t)_i + (1-w) \times TSS(t-1)_i, (0 \leq w \leq 1), \tag{2}$$

where constant w represents how fast the trust score of the sensor evolves as the cycle is repeated. The larger w is, the more important recent trust scores are. In other words, if w is large, the trust score of a sensor will evolve fast. In contrast, if w is small, the trust score of a sensor will evolve slowly. Fig. 5 shows

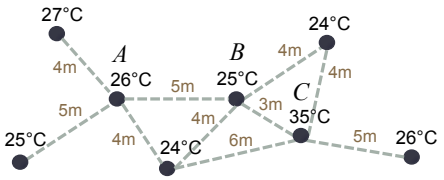


Fig. 5. Example scenario. Dashed lines represent neighbor relationships.

an example scenario at a time t when α and β are both 1 and w is 0.5. Assume that the initial $TSS(t)$s of all sensors are 0.5 at the time t and the sensed values do not change throughout this example. Also, assume that sensor A and sensor B are normal, whereas sensor C is abnormal. At the time t, $TSV(t)_A$, $TSV(t)_B$ and $TSV(t)_C$ are 0.58, 0.25 and 0.09, respectively. Sensor A provides the sensed value with the highest trust score since the sensed value is consistent with the sensed values of its neighbors, whereas sensor C provides the sensed value with the lowest trust score since the sensed value is not consistent with the sensed values of its neighbors. Notice that $TSV(t)_B$ is much lower than $TSV(t)_A$ even though $TSV(t)_B$ is also normal since one of its close neighbors, that is, sensor C provides the abnormal sensed value (35°C). However, $TSV(t+\delta)_B$ eventually becomes high as δ increases due to the following reason. $TSS(t+\delta)_C$ becomes low as δ increases and thus, when $TSV(t+\delta)_B$ is calculated, the sensed value of sensor C is taken into account to a slight extent (see Eq. 1). In this example, at the time $t+3$, $TSV(t+3)_A$, $TSV(t+3)_B$ and $TSV(t+3)_C$ evolve to 0.58, 0.55 and 0.09, respectively. The trust score of the sensed value provided by sensor B increases from 0.25 to 0.55, and thus the trust score of sensor B also increases.

4.3 Minimum Trust Score of a Normal Sensed Value

Our trustworthiness assessment scheme generates absolute trust scores for sensed values. Under the assumption that a physical phenomenon gradually changes over a physical space, we can derive the minimum trust score of a sensed value TSV_{min} produced by a normal sensor at a time specific t. To obtain TSV_{min}, we consider the case in which a normal sensor i is located at the peak of a physical phenomenon as ~~depicted at~~ Fig. 6. For instance, imagine that a sensor is located at a heat source such as a heater. We assume that the monitoring value

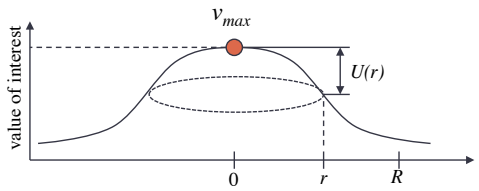


Fig. 6. An illustration which shows that a normal sensor i is at the peak of the monitoring values ($r = 0$). v_{max} is the highest value and r is the distance from the peak point. $U(r,t)$ is a monotonic increasing function of r until $r \leq R$ at a time t.

decreases from the peak value, i.e., v_{max}, according to a monotonic increasing function $U(r,t)$. For instance, if $U(r,t)$ is the heat equation, ~~it~~ is a parabolic partial differential equation describing the distribution of heat in a given region over time [4]. For this analysis, we assume that $U(r,t)$ equally increases in any direction as r ($\leq R$) increases. R is the maximum distance within which sensors are considered as neighbors of sensor i. We also assume that sensors are evenly deployed and β is 0. We only consider sensors on the inside of the deployed area since sensors at the border of the area have fewer neighbors. Then, $TSV(t)_i$ is calculated as follows:

$$TSV(t)_i = \frac{1}{1+|\tau'|}, \tag{3}$$

$$\tau' = \frac{\int_0^R \frac{U(r,t)\times\rho\times 2\pi r}{r^\alpha} dr}{\int_0^R \frac{\rho\times 2\pi r}{r^\alpha} dr} = \frac{\int_0^R \frac{U(r,t)}{r^{\alpha-1}} dr}{\int_0^R \frac{1}{r^{\alpha-1}} dr}, \tag{4}$$

where ρ is the density of sensors. If we set α to 1 and the maximum gradient of $U(r,t)$ is γ ($\gamma > 0$) at a time t, then τ' is less than or equal to $\frac{\gamma\times R}{2}$ as follows:

$$\tau' = \frac{\int_0^R U(r,t)dr}{\int_0^R dr} \leq \frac{\int_0^R \gamma \times r dr}{\int_0^R dr} = \frac{\gamma \times R}{2}. \tag{5}$$

Therefore, $TSV(t)_i$ must be greater than or equal to $\frac{2}{2+\gamma R}$.

$$TSV(t)_i \geq TSV_{min} = \frac{1}{1+\frac{\gamma R}{2}} = \frac{2}{2+\gamma R} \tag{6}$$

For instance, if R is 70 (m) and γ is 0.05 (°C/m), the minimum trust score of a normal value sensor should be greater than 0.36. Therefore, if the trust score of a sensed value is greater than 0.36, the sensed value can be considered as a trustworthy one.

5 Simulation

In this section, we present our performance evaluation through simulations. We first describe the simulation settings, and then present the simulation results.

5.1 Simulation Setting

We developed a simulator specialized for sensor trust assessment and focused the performance of our algorithm ~~itself~~. Since the considered algorithms are purely based on sensor readings and their locations, we did not use general network simulators such as TOSSIM [3] and NS-2 [2].

For the simulations, 250 sensors are randomly deployed in a 400m×400m area. n IDs are assigned to the sensors from 0 to 249 as shown in Fig. 7. Sensors from 0 to 229 are normal, while sensors from 230 to 249 are abnormal. Each sensor reports 100 temperature values at a time t ($0 \leq t \leq 99$). Both α and β are set to 1 and w is set to 0.2. A temperature value of a normal sensor is sampled from the normal distribution with the mean of 25 and the standard deviation of 2, i.e., $\mathcal{N}(25, 2)$.

The maximum neighbor range R is set to 70m, which means that the neighbors of sensor i are the sensors within 70m of sensor i. Sensors at the center of the area have approximately 24 neighbors, while sensors at the corners have approximately 6 neighbors. If R is too small, the accuracy of trust scores becomes low since only a few neighbors might be taken into account to compute the trust score of a sensor. As R increases, the accuracy increases with the increased computational cost. However, if R becomes larger than a certain level, the accuracy improvement becomes limited since distant neighbors scarcely affect the trust score of a sensor.

A heat source is located at (300, 300) and the mean temperature of the peak point is set to 45°C. From the peak point, the temperature linearly decreases with the gradient of 0.05 (°C/m). If the distance from the peak point is greater than 400m, the temperature does not decrease. Thus, in our simulation, TSV_{min} is 0.36. We varied two parameters Δ_{mean} and Δ_{sd} for abnormal sensors. Δ_{mean} and Δ_{sd} are added to the mean and the standard deviation of the normal distribution of a normal sensor, respectively. That is, temperature values of an abnormal sensor are sampled from $\mathcal{N}(25 + \Delta_{mean}, 2 + \Delta_{sd})$.

Throughout the simulations, we compare two schemes: our scheme and the normal distribution-based scheme. The normal distribution-based scheme calculates the trust score of a sensed value based on the normal distribution which is modeled by using all sensed values at each time as in [6, 9].

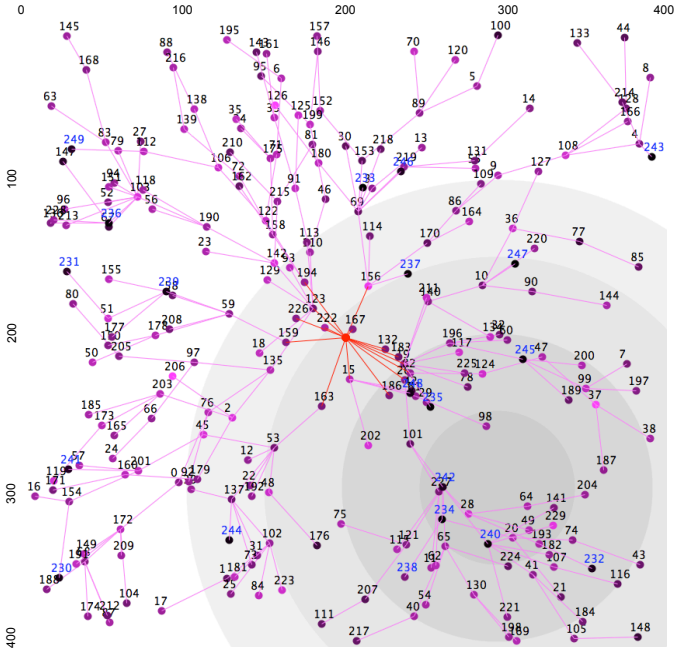


Fig. 7. Simulation topology

5.2 Simulation Result

First, we obtained the trust scores of sensors when all sensors are correctly working, i.e, $\delta_{mean} = 0$ and $\delta_{sd} = 0$.

Fig. 8 shows the sorted trust scores of all sensors when the normal distribution-based scheme is used. Even if there is no abnormal sensor, some sensors get low trust scores since the trust scores are relative. As a result, the administrator of the WSNs cannot distinguish whether there are abnormal sensors in the network or not.

However, since our scheme outputs absolute trust scores (see Fig. 9). the administrator of the WSNs can distinguish whether there are abnormal sensors in the network or not under the assumption he/she knows the minimum trust score. Notice that, in this scenario, 26 sensors have lower trust scores than TSV_{min} (=0.36) even though all sensors are normal due to the following reasons. First, the sensors are not perfectly evenly-deployed and some sensors do not have enough neighbors. Second, the sensed values are generated with the standard deviation of 2. Thus, the overall trust scores are lowered. In real applications, TSV_{min} may be estimated at the time of the initial deployment when all sensors are working correctly. If the administrator successfully obtains TSV_{min} for his/her application, he/she can distinguish normal sensors from abnormal sensors and execute follow-up actions such as replacing sensors with trust scores under TSV_{min} with new sensors.

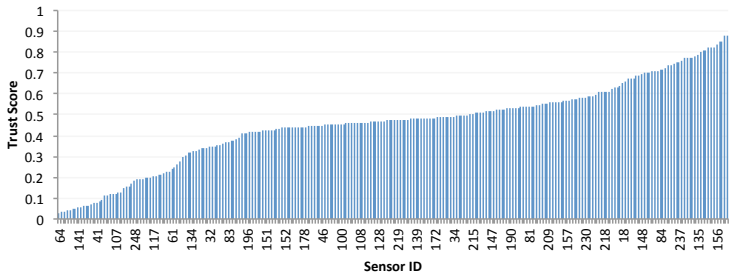


Fig. 8. Trust scores of sensors when the trust scores are calculated by the normal distribution-based scheme. Sorted by the trust score ($\delta_{mean} = 0$ and $\delta_{sd} = 0$)

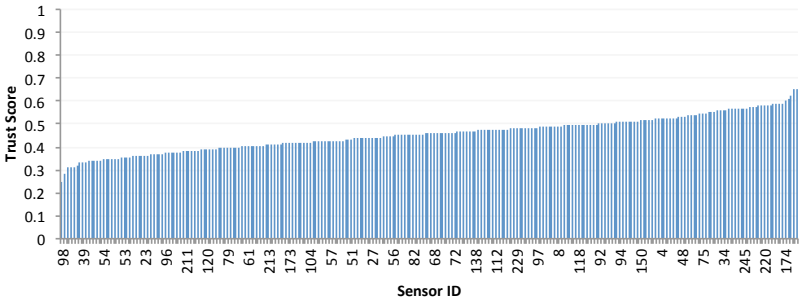


Fig. 9. Trust scores of sensors when the trust scores are calculated by our scheme. Sorted by the trust score ($\delta_{mean} = 0$ and $\delta_{sd} = 0$)

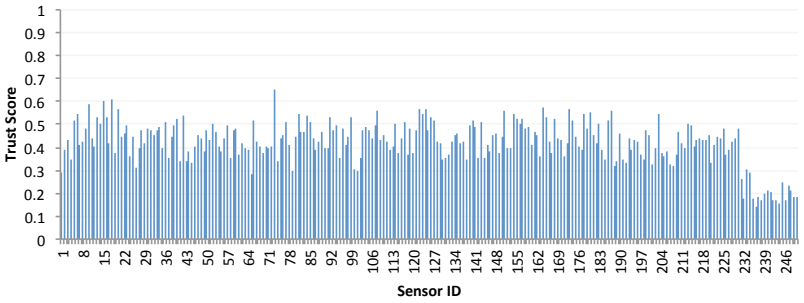


Fig. 10. Trust scores of sensors when the trust scores are calculated by our scheme. Sorted by the ID ($\delta_{mean} = 5$ and $\delta_{sd} = 0$)

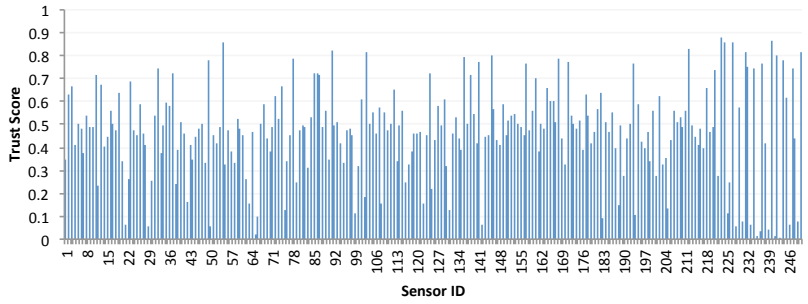


Fig. 11. Trust scores of sensors when the trust scores are calculated by the normal distribution-based scheme, Sorted by the ID ($\delta_{mean} = 5$ and $\delta_{sd} = 0$)

Fig. 10 and Fig. 11 show the trust scores of the all sensors when our scheme and the normal distribution-based scheme are used, respectively; δ_{mean} is set to 5 and δ_{sd} is set to 0. As shown in Fig. 10, when our scheme is utilized, the trust scores of the sensors from 230 to 249 are distinctly lower than the trust scores of the normal sensors. However, when the normal distribution-based scheme is used, sensors near the peak location get low trust scores since the sensed values provided by them are far from the mean, while sensors at the middle of the slope get higher trust scores than others since they are close to the mean.

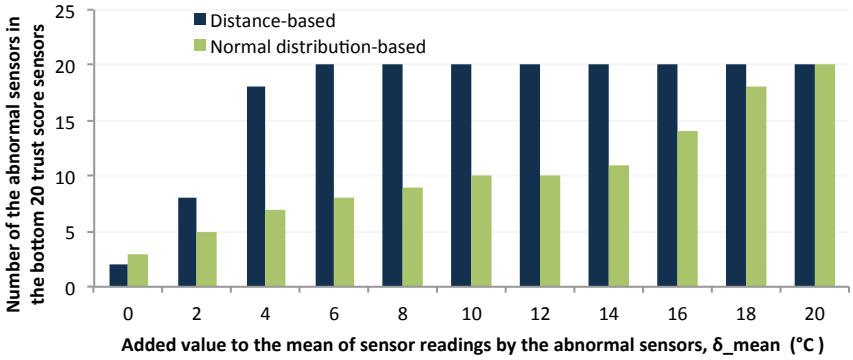


Fig. 12. Comparison between our scheme and the normal distribution-based scheme when δ_{mean} varies from 0 to 20

Fig. 12 shows the number of the abnormal sensors (sensors from 230 to 249) on the bottom 20 trust score sensor list when δ_{mean} varies from 0 to 20. When all sensors are correctly working, in our scheme, 2 abnormal sensors are included on the bottom 20 list. However, when δ_{mean} is only 4, our scheme includes 18

abnormal sensors on the list and when δ_{mean} is 6, all the 20 abnormal sensors are included on the list by our scheme. On the other hand, the normal distribution-based scheme cannot include as many abnormal sensors on the bottom 20 list as our scheme does. When δ_{mean} reaches 20, the normal distribution-based scheme can include all the 20 abnormal sensors on the list.

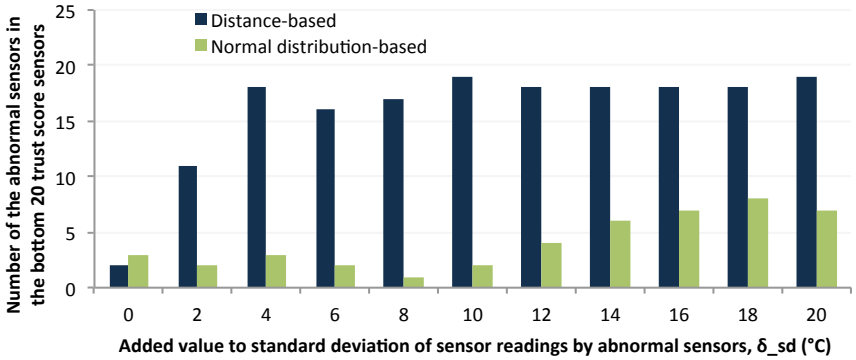


Fig. 13. Comparison between our scheme and the normal distribution-based scheme when δ_{sd} varies from 0 to 20

Fig. 13 shows the number of the abnormal sensors on the bottom 20 trust score sensor list when δ_{sd} varies from 0 to 20. Similarly to the prior result, our scheme includes more than 16 abnormal sensors on the list when δ_{sd} is larger than or equal to 4. However, the normal distribution-based scheme includes less than half of the abnormal sensors on the list. These results confirm that our distance-based trust assessment scheme outperforms the normal distribution-based scheme in realistic scenarios where the sensed value of interest gradually changes according to the locations.

6 Conclusion and Future Work

In this paper, we propose a novel sensor trustworthiness assessment scheme using the distances between sensors. In the cyclic framework, the trust score of a sensed value is evaluated based on the fact the sensed values are correlated with their positions. In the first step, the trust score of a sensed value is calculated using the sensed values of its neighbors, their trust scores and the distances from the neighbors. Then, the trust score of a sensor evolves at each time by taking the new trust score of its sensed value into account. Our simulation results confirm that our trustworthiness assessment scheme provides practical and accurate trust scores of sensors in a realistic scenario. As future work, we plan to investigate extensions of our approach to reliably assess sensor trustworthiness in presence

of collusion attacks. We also plan to investigate how our approach needs to be extended/modified with dealing with different physical phenomena.

Acknowledgments

The work reported in this paper has been partially supported by the Purdue Cyber Center and by the National Science Foundation under grant CNS-1111512.

References

1. Intel lab data, http://db.csail.mit.edu/labdata/labdata.html.
2. ns2, http://www.isi.edu/nsnam/ns/.
3. Tossim, http://tinyos.stanford.edu/tinyos-wiki/index.php/tossim.
4. J. R. Cannon. The one-dimensional heat equation. 1984.
5. S. Ganeriwal, L. K. Balzano, and M. B. Srivastava. Reputation-based framework for high integrity sensor networks. *ACM Trans. Sen. Netw.*, 4(3):15:1–15:37, June 2008.
6. H.-S. Lim, Y.-S. Moon, and E. Bertino. Provenance-based trustworthiness assessment in sensor networks. In *Proceedings of the Seventh International Workshop on Data Management for Sensor Networks*, DMSN '10, pages 2–7, New York, NY, USA, 2010. ACM.
7. M. Probst and S. Kasera. Statistical trust establishment in wireless sensor networks. In *Parallel and Distributed Systems, 2007 International Conference on*, volume 2, pages 1–8, Dec 2007.
8. Q. Zhang, T. Yu, and P. Ning. A framework for identifying compromised nodes in wireless sensor networks. *ACM Trans. Inf. Syst. Secur.*, 11(3):12:1–12:37, Mar. 2008.
9. W. Zhang, S. Das, and Y. Liu. A trust based framework for secure data aggregation in wireless sensor networks. In *Sensor and Ad Hoc Communications and Networks, 2006. SECON '06. 2006 3rd Annual IEEE Communications Society on*, volume 1, pages 60–69, Sept 2006.