Statistical-Based Trustful Access Control Framework for Smart Campuses

AHMAD B. ALKHODRE
Faculty of computer and information systems
Islamic University of Medina, KSA

***Abstract*—The vision of the Internet of Things (IoT) is based on the idea of offering connectivity to every physical object (e.g., thermometers, banknotes, smart TVs, bicycles, etc.). This connectivity ensures that immediate information about these objects and their surroundings can be obtained and therefore decisions can be taken based on real-time information. This allows increased productivity and efficiency. One of the most important implementations of the IoT is the smart (or digital) cities where the information collected from the connected devices is used in, for instance, configuring energy systems, enhancing the traffic, controlling pollution or ensuring security. However, there is no guarantee that all objects will provide information because, for example, some may be out of service or have lost connectivity bearing in mind that many objects in an IoT network are characterized by their limited resources (e.g., battery life, computing, and connection capacity). Moreover, the decision in an IoT network is mostly based on the information provided by a subset of the objects rather than all of them. In addition, the obtained information can be contradictory for many reasons, such as a defect in the object or malicious interference either in the object itself or during the communication process. Therefore, it is necessary to provide a measure that reflects to what extent the decision in an IoT network is trustful. In this paper, an approach based on statistical science is proposed to measure the trustworthiness of information collected from heat sensors. An architecture and algorithm, based on the confidence interval measurement to reduce the time taken to verify and check the trustworthiness of network sensors or any other type of IoT device.**

Keywords*—Internet of things; trust management; confidence interval; confidentiality; smart cities

I. INTRODUCTION

According to the International Telecommunication Unit (ITU) Report 2005 ([1]), the Internet of Things (IoT) has a vision of providing all objects and devices (e.g., thermometers, banknotes, surveillance cameras, control access badges, etc.) with the ability to connect to a network which is named the IoT. This connectivity ensures that immediate information about these objects and their surroundings can be obtained and decisions can, therefore, be taken based on real-time information. This allows increased productivity and efficiency. One of the important implementations of the IoT is the smart (or digital) cities [2] where information collected from the connected devices is used in, for instance, configuring energy systems, enhancing traffic control, controlling pollution or ensuring security. Hence, the needs of the city inhabitants are efficiently met [3]. However, the connected devices are vulnerable to manipulation and/or physical damage. In practice, there is no guarantee that all the connected devices will provide their information because some of them may be out of service or have lost connectivity. Moreover, the obtained information can be contrary because of a malicious interference.

The Internet of Things (IoT) is an old term. It first became popular due to industrial demand and then secondly because all the pre-requisites that were needed for IoT had never before been available as they are today. The vision of IoT is that all electronic devices will be able to communicate with each other. Although previously this capability existed among a very few devices, ultimately the IoT will generate a massive amount of information which can be used to gather further meaningful data. The IoT concept was presented two decades ago by a technologist, Kevin Ashton. He stated that any two devices can communicate with each other or can connect to the internet with the help of sensors.

The IoT is an interesting concept since it will allow the automation of objects without human intervention through the advancement of technology and other new developments in daily life. However, on the flip side, other issues arise and, of those problems, the big challenges of security and trust need to be given the utmost attention [4]. The security and development of trust among the communication of IoT-based devices as well as the sharing of privacy-preserved data for analysis are the subjects of current critical research.

The IoT devices can be divided into three layers [5] where strong bonds relating to the security and trust of the user's data are required. These are the physical layer, the network, and the application layer. If there is any malfunction in the device or the vulnerability of data, this will create an unreliable environment. In this research, the physical layer of security and data privacy are discussed. In the first place, a plenty of data is received from the physical sensors of the device which needs to be reliable. Secondly, even if the data is correct, it should remain secure and all the concerns regarding the privacy of the user's personal data should be addressed. Furthermore, the data should not be utilized without the user's permission as per the terms and conditions agreed upon.

As discussed, there are three layers in an IoT system and we can find many areas in those layers where trust management is required to promote the worldwide adoptability of the IoT system. These areas have been thoroughly discussed in the various literature. However, before moving on to the contribution of our work to ensure trust in the IoT systems in a specific area, these areas will briefly discuss them. Trust

relationships and decision making are the first objectives to be achieved by establishing a strong IoT based system. For example, trust in data perception, privacy preservation, data fusion and mining, data transmission and communication, and system security are considered.

In this work, an approach based on statistical science is proposed to measure the confidence of the collected measurements. This approach helps to reduce the time taken to verify and check the trustworthiness of network sensors or any other type of IoT devices. The structure of this paper will be as follows. Following this introduction, this paper will look at the security challenges of IoT, then the related work will be presented. Before presenting our approach, section 4 will outline the theoretical background of the proposed approach. Finally, the article will close with a discussion and conclusion.

II. BACKGROUND

A. The IoT Security Challenge

Ensuring the security, reliability, resilience, and stability of internet applications and services is critical to promoting trust and the use of the internet. As users of the internet, it needs to have a high degree of trust that the internet, its applications and the devices linked to it are secure enough to perform the kinds of activities we want to do online in relation to the risk tolerance associated with those activities. The Internet of Things is no different in this respect, and security in the IoT is fundamentally linked to the ability of users to trust their environment. If people do not believe that their connected devices and their information are reasonably secure against misuse or harm, the resulting erosion of trust causes a reluctance to use the internet. This has global consequences to electronic commerce, technical innovation, free speech and practically every other aspect of online activities. Indeed, ensuring security in IoT products and services should be considered as a top priority for the sector. As we increasingly connect devices to the internet, new opportunities to exploit potential security vulnerabilities grow. Poorly secured IoT devices could serve as entry points for cyber-attacks by allowing malicious individuals to re-program a device or cause it to malfunction. Poorly designed devices can expose user data to theft by leaving data streams inadequately protected. Failing or malfunctioning devices can also create security vulnerabilities. These problems are just as large, or even larger, for the small, cheap and ubiquitous smart devices in the Internet of Things as they have traditionally been for computers [6].

B. Confidentiality measuring

Through literary studies, mechanisms have been extensively discussed to determine trust and reputation but there is little research into trust management for the IoT nor into the study of confidence in the field of big data, taking into account the privacy of users and data [7][8].

In digital data processing, the confidence process involves verifying that the collected data is reliable and trustworthy. Through the research presented in [9], trust is calculated via social confidence and the QoS of data metrics through direct and indirect observations and recommendations to update trust metrics.

Indeed, trust has three properties. Honesty, cooperativeness and community interest are considered in the trust evaluation of IoT nodes ("things"). The honesty trust refers to the node as being honest or not, while the cooperativeness trust presents the social cooperation between trustee and trustor [10].

This paper focuses on data perception trust that works on the physical layer of an IoT based system. Data perception trust means that data should be reliably collected and recognised on the physical layer.

The services provided by the IoT vision will demand more data from the user's devices. However, that data needs to be trustworthy and secure from malicious attacks. Chend et al. [11] provided a trust and communication mechanism to securely communicate devices on the Internet of Things network. They presented the trust management model for IoT based on Fuzzy logic in a wireless sensor network environment.

Nitti et al. [12] presented the idea of trustful communication among the social Internet of Things network. In this concept, objects can create their social objects' network. They focused on how the objects were going to share information among nodes and how to evaluate the data received by another social object. The system evaluates the trust level of its peer/friend object based on its personal experience and takes the opinion of friends who are in common with all its objects.

Furthermore, Ruan et al. [13] also worked on the trust management for IoT agents and provided a framework for that. They also observed that, by using a trust-aware IoT network, the error can be reduced. They also enhanced their research findings by applying two different kinds of attacks and detected them via their trust management technique. In addition, they also provided an interface so that an end user can evaluate the whole communication process between agents.

Wand et al. [14] worked on Mobile AdHoc network trust management for a service-oriented approach. This is an ongoing research idea and they have shared the experiences they have learned whilst also providing details of their future direction. Gallahar et al. [15] studied the confidentiality measurement in a health-care environment.

It is obvious that most of the earlier work has focused on obtaining confidence in the IoT (or the connected system in general) by building a system based on reputation. In such a type of system, every time the device/node participates in an operation (e.g., communication, providing information, etc.) its credit will be increased (or respectively decreased) if this participation was correct or honest (or respectively incorrect). However, how does the reputation system decide whether the participation is correct or not? Furthermore, there is no measure that specifies to what extent the services or the operations by an IoT network are trustworthy. This research proposes a statistical-based measure of trust in order that a measure of confidence for the IoT service is provided.

C. Statistical-based Confidentiality Measure

Statistics is one of the major branches of mathematics and has wide applications. Statistics are concerned with collecting,

summarizing, representing and drawing conclusions from the available data set, trying to overcome problems such as data heterogeneity and divergence [16][17].

In statistical terminology, the population is the entire group of individuals for which statistics are made. In our case, the population is composed of sensor and thermometer measures.

In order to optimize the available resources (money, time and other types of resources), all the individuals in a large population cannot be taken into consideration. Furthermore, it is practically impossible to reach all the individuals. Thus, the decision was taken to base the study on a subset of the individuals called Sample which was selected randomly, i.e., population individuals had an equal chance of being selected. Note that it is not possible that a selected sample will represent 100% of the population and this leads to what is referred to as sample error. In order to evaluate the correctness of a sample result (i.e., to understand how far this result is from the result that could be obtained when all the individuals are used), the confidence interval can be used.

The confidence interval [18] is a concept used to measure the correctness of a sample. It reflects the percentage of error in the sample. In other words, it is seen as a measure of correctness around a sample. The confidence interval reveals the variety of values of the population within a level of correctness. The larger the confidence level, the higher the confidence in the result.

The confidence interval of the control panel decision is proposed to calculate. If this interval is heterogeneous (some values in this interval confirm the violation, while others deny it), then the control panel needs to continue collecting more information from other sensors before making a decision. If the interval is homogeny (i.e. the value of interval confirms a violation in the access control system or denies it), then the control panel reaches a trustworthy result and can make the corresponding decision. The advantages of this system include, firstly, making a decision as soon as sufficient information is gathered rather than waiting for all the information to be gathered. Secondly, this system provides a measure of confidence in the control panel decisions and, finally, it identifies the sensors and thermometers that provided the incorrect information and thus they can be checked.

The proposed solution aims to first design a smart control access system based on data collected from the sensors and the devices in our system. This system also allows making the decision, for example, to evacuate during an emergency. The second objective is to provide a confidentiality measure for the decisions taken by the smart control system.

1) Statistics and Confidence Interval

The population size could be very large therefore it is not possible to collect the data from every individual which would be costly in terms of time and resources. Statistics find a solution for such a problem by proposing to obtain the answer based on a group of individuals chosen from the population called Sample [18]. For the most part, the choice is made randomly, however, other methods of selection do exist. Since the Sample does not usually accurately reflect the whole population, an inconsistency exists, a so-called Sample Error, between the sample-based answers and the population-based answers. In practice, the sample-based answer will not be a specific value (so-called point estimate) but rather a range of values (so-called interval estimate) in which the true answer will exist. Remember that the true answer is the answer that we would get if all the individuals in the population were asked. The confidence interval is calculated based on the confidence degree. This latter is a percentage that relates to what degree we are sure that the calculated interval contains the true answer. For better understanding, suppose that a survey claims that a candidate will get between 50% and 60% of the votes and the certitude of this estimation is 95%. The 95% is the confidence degree and thus, under repeated random sampling in identical conditions, the interval [50 – 60]% will contain our sample result 95% of the time.

Our proposal is based on using the confidence interval as a reliability measure for the decision calculated, thanks to the information obtained from the sensors. For instance, if we calculate the 95% confidence interval of the decision, we will be 95% certain that the correct decision belongs to the estimated interval. Thus, if the estimated interval is homogenous (respectively, heterogeneous), we can accept (respectively, refuse) the decision.

D. Confidence Interval Calculation

In statistical science, the mean is the most used population parameter [18]. In our context, the calculation of the confidence interval is similar to the calculation of other population parameters such as median or proportion in other disciplines.

Suppose the mean of the sample is μ_s (i.e., the estimated point) and the error of the sampling is λ (standard error) which is calculated according to a specified confidence level (CL), the population mean μ is determined using the following equation

$$\mu_s - \lambda < \mu < \mu_s + \lambda \qquad (1)$$

The percentage of the confidence interval of the population mean (CL%) is given by the interval $[\mu_s - \lambda, \mu_s + \lambda]$.

The error of the sample for the mean is given by equation (2). Obviously, the key element during the estimation of the confidence interval is the error of sampling of the mean.

In order to calculate the error of sampling, the distribution of the sample should be determined. Equation (2) can be applied only when the distribution follows a normal distribution whereas other equations are used to calculate the sampling error for the distribution which does not follow the normal rule [18].

$$\lambda = z_{\alpha/2}\frac{\sigma_s}{\sqrt{n}} \qquad (2)$$

Whereas the standard deviation σ_s of a sample for the normal distribution is calculated as follows:

$$\sigma_s = \sqrt{\frac{\sum_{i=0}^{n} \mu_s - x_i}{n-1}} \qquad (3)$$

Here the factor $z_{\alpha/2}$ correlates with the confidence interval and the distribution of the sampling and x_i represents the sample of the individuals. Consider the bell distribution of data, this factor represents the zones in the tail of the bell. For example, if the confidence interval is 95% then $\alpha/2 = 0.025$. Next, according to the table, 1 z-score is z0:025= 1:96. Table (1), contains the z-scores for the most commonly used confidence levels.

TABLE I. Z-SCORES FOR THE MOST COMMONLY USED CONFIDENCE LEVELS

Confidence level	z-score
80%	1.28
90%	1.65
95%	1.96
99%	2.58
99.9%	3.29

Briefly, the following algorithm characterizes the estimation of the confidence interval of the population:

1) Select a sample which represents the population.

2) Compute the mean of the sample and its standard deviation.

3) Compute $\alpha/2$ the zone outside the confidence interval.

4) Compute the sampling error using equation 3.

5) Compute the estimation of CL as $[\mu_s - \lambda, \mu_s + \lambda]$.

III. SCAS: SMART CONTROL ACCESS SYSTEM

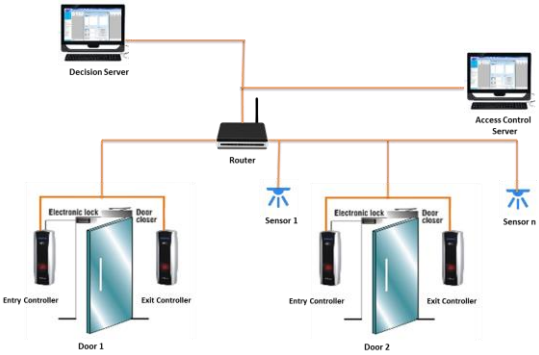

Fig. 1. Smart Control Access System

As shown in figure 1, our IoT system is composed of sensors which can sense fire, movement, pollution, heat, etc. They send their measurements to the decision server. The router (or any type of network connector device) that connects many smart heat sensors together links via the internet to a server. The access control server receives entry/exit requests from the access controllers and sends back the proper response. The decision server is a workstation used for collecting data and analyzing it in order to determine whether the data is trusted or not. Each sensor belongs to a zone that measures the temperature in its zone. The behavior of each sensor is demonstrated in figure 2. This state diagram shows six states representing the behavior of a sensor. When a sensor starts working, it will be in the idle state. When the measurement time arrives, the sensor will read/measure the temperature and store it. The state, sending data, is the state where the sensor is interrogated to give the stored data. Finally, the trust value of the sensor is updated (update trustValue) whenever it is sent by the monitoring system. If the trust value is below the required limit, the sensor receives a deny signal that causes the end state.

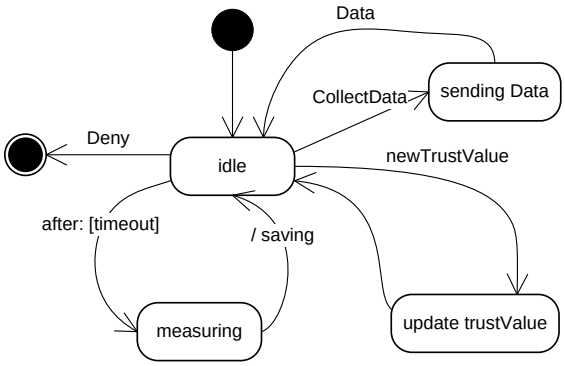

Fig. 2. the states of a smart heat sensor

The sequence diagram (figure 3) represents the diagnostic system. For the first step, a doubtful node is selected. A diagnostic procedure will take place to verify whether the node is sending correct data or not. The second step is to determine the neighbors of the node in focus to form the proof. Next, a subset (sample) is selected from the data sent by those nodes.

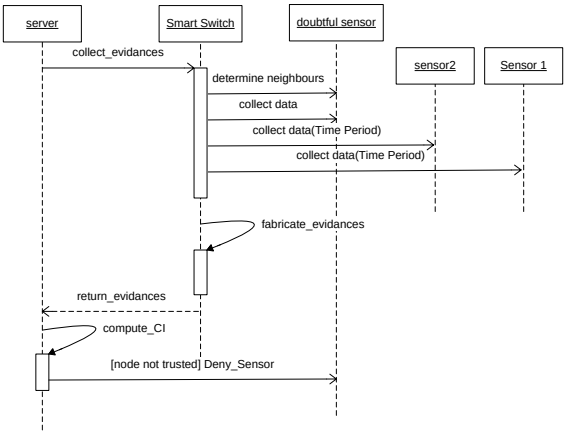

Fig. 3. the sequence diagram of evidences collection

The subset of the data is selected randomly from the neighbors of the doubtful node. In order to apply Formula 4, the weights (wi) are assigned according to the neighborhood. Next, the error of the sample and the CL confidence interval are calculated using formulas 1 to 4. The objective of calculating CL is to limit the number of proofs gathered during the doubtful node's checkup and to measure the extent of using CL in the diagnosis, especially when inconsistent proofs are gathered. For optimization of the resource and for power consumption purposes, the gathering of more proofs (possibly redundant) will not change the result of the diagnosis.

For instance, suppose a doubtful node uses the equation (4)

$$D = \sum_{i=1}^{n} w_i p_i \quad (4)$$

Where wi is a factor, this gives the trust of the neighborhood node where its value is positive or negative and pi is the proof of node i where the value is 1 (the collected data is correct), -1 means the collected data is not correct and 0 means the interrogated sensor has not responded.

After using formula 1 in calculating the sampling error, if the confidence interval is homogenous, this means that the doubtful node cannot be trusted. If the confidence interval is heterogeneous, then the true diagnostic result can either confirm or deny the doubtful node (figure 4).

For instance, suppose a doubtful node and D is calculated according to formula 4.

This is calculated based on proofs p1, p2… pn. and λ is the error of the sampling of D and CL is 95%. Then, the 95% of the confidence interval of the checkup result is [D-λ ;D+ λ]. where the result of the diagnosis is [-1,+1]

If the D+ λ <= 0 (positive values) and CL= 95% this means 95% of the proofs give a negative result and the data set confirms that the doubtful node cannot be trusted.

Similarly, if the D- λ > 0 (negative values) and CL= 95% this means 95% of the proofs give a positive result and the data set confirms that the doubtful node is trusted.

In the case where the results are negatives and positives at the same time, the latter characterizes the doubtful device as trusted but not all the time.

This can be interpreted that the system is not mature enough and more proofs must be collected to continue the diagnostic process.

In conclusion, the correct diagnostic result must be within the estimated confidence interval. Therefore, the result of a sample is accepted only if the estimated interval is homogeneous, that is, all its values are rejected. If the confidence interval is heterogeneous, then the true diagnostic result can confirm the correctness of a device or not. This means that there are still doubts about the diagnostic result obtained and, therefore, more proof must be collected before the diagnosis is complete

Algorithm 1 Procedure IoT_node_check ( )

Input a selected node
Output new trust values

```
1.  Determine node zone and neighbors
2.  Collect evidences form a subset from node's neighbor
3.  Compute confidence interval (CI)
4.  if CI is heterogonous then
5.   if CI < 0 then
6.   Change the trust value of the selected node
7.   Update trust value for all node in the zone
8.   end if
9.  else goto 2
10. end if
```

Fig. 4. Integrating the confidence interval into the diagnosis

A. Reliability of IoT Network Decisions

The collected measurements from the sensors (IoT objects in general) could be incorrect for two reasons:

- Tampered sensors that are controlled by an attacker and provide wrong measurements in order to poison the IoT network
- Damaged or biased sensors because of non-malicious events. For instance, a temperature sensor that is installed next to a light or a warming device will provide biased temperature measurements.

Regardless of the intention behind the incorrect measurements/information, they lead to contradictory information and hence prevent the decision server from making a decision or leads to a wrong decision. Thus, there is a need for a reliability indicator that helps in accepting or refusing the decision taken based on the collected measurements

B. Experiment and Proof of Concept

1) Confidence Interval as a Reliability Measure

The goal of this experiment is to prove that using the confidence interval helps in avoiding wrong decisions even in the presence of incorrect measurements because of either tampered with or damaged sensors. The measurements of 7 heat sensors are simulated and the different percentage of tampered sensors is discussed using MATLAB (figure 5). This shows the measurements of 7 sensors. The summits indicate the result of an abnormal or damaged sensor.

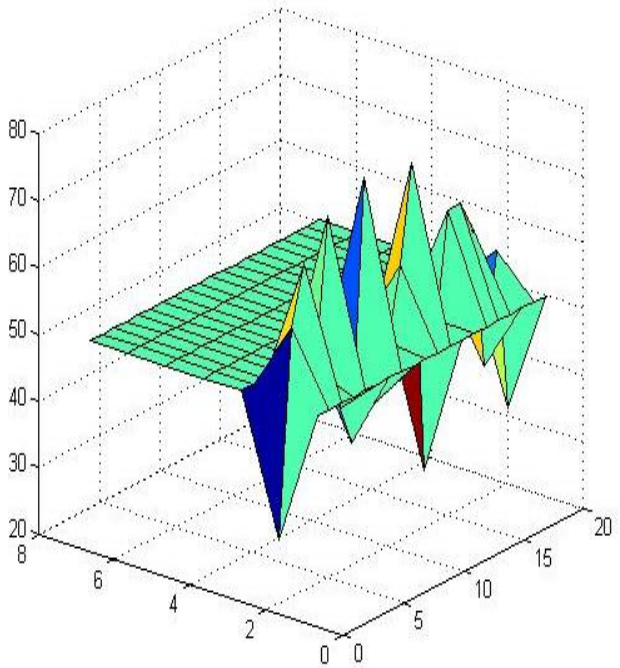

Fig. 5. the measurements of 7 smart sensors

As shown in figure 6, sensor 2 gives abnormal values compared to the other sensors, which indicates that this sensor has abnormal behavior and its measurement data must be verified (the sensor may be to blame).

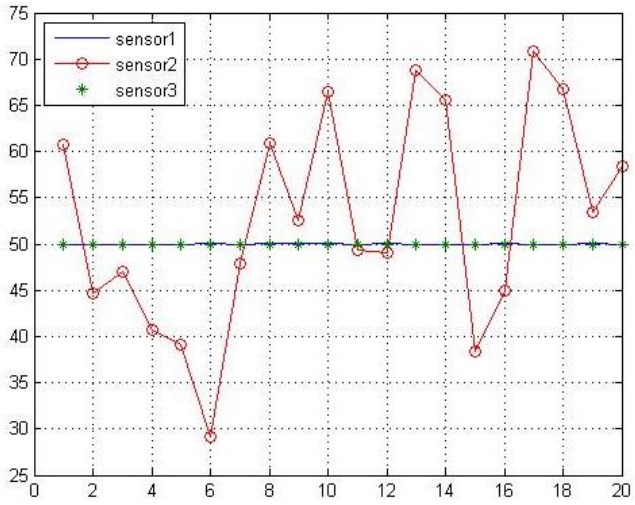

Fig. 6. the measurements of well-behaved and misbehaving sensors

In the simulation, the following Gaussian noise is used to generator erroring signal with SNR (signal-to-noise)

"awgn(V(i),10,'measured');"

Figure 7 shows the updating of trust values for the two different sensors (trusted and accused sensors).

Algorithm 2 Procedure update trust_values ( )

Input matrix of evidences (E), a matrix of trustvalue of participated node (W)

Output matrix of trustvalue of participated node (W)

1. **for** i=1 to **size_of**(W)
2. **if** e_i == -1 **then**
3. $w_i = w_i + 0.2$;
4. **else**
5. $w_i = w_i - 0.2$;
6. **end if**
7. **end for**

Fig. 7. MATLAB code for updating trust value.

The first sensor is trusted so the value of its trustvalue is increased and the second sensor's trustvalue is decreased according to the calculation in figure 8.

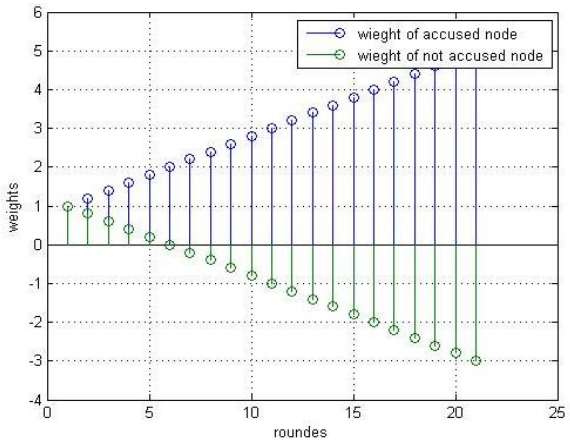

Fig. 8. the trust weights of well-behaved and misbehaving sensors

In the beginning, the 7 sensors start working and measure the temperature periodically. This task is achieved by using a timer that initiates the sensors at certain periods of time.

After the measurement is completed, the data is stored in a matrix in order to start the diagnostic process. Then, a sensor is selected to test its reliability by calculating the confidence interval. In step one, all the collected data is considered as a sample from which we will make the calculations using equation number 4. Next, the system starts to collect proofs. The proofs will be either -1, which means the measurement is not confirmed, or 1, which means the measurement is confirmed and correct. So, from these proofs, in order to prove the validity of the study, a partial data set is defined through the use of the function data-sample of MATLAB functions (figure 9). Then, the confidence interval is calculated for the chosen sample and update the trust value of all the sensors involved in the assessment process.

```
sampleError=1.96*(std2(E2)/sqrt(numel(E2)))
```

```
sample=datasample(E2,5,2);
for i=1:5
for j=1:5
 D(2,count) =D(2,count) + sample(j,i)*W1(j);
end
end
```

Fig. 9. MATLAB code for calculating the sum of the trust values of all sensors.

If the sensors gave a correct data, the trust value increases otherwise the trust values are reduced for all sensors which sent negative results. The previous operation is done for more than one round and, for each round, a different sample is taken and the previous calculations are redone. Figure 10 shows the change in the confidence area values calculated according to equation numbers 3 and 4. The upper curve shows that the values are constant positive, which gives an indication that the sensor is reliable (well-behaving) while the second curve shows that its value is increased by negative values, which means that the sensor cannot be trusted and must be removed (misbehaving).

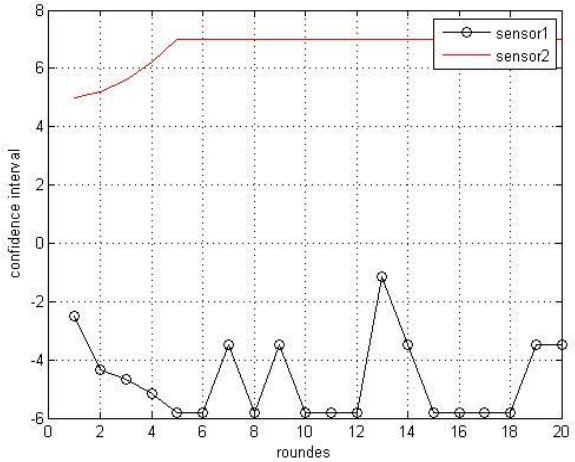

Fig. 10. the confidence interval of well-behaved and misbehaving sensors

IV. Discussion and Conclusion

This article addressed the three key challenges faced in our system. During the error diagnosis, the sensor that does not behave well may provide incorrect proof. Therefore, the diagnosis can blame a legitimate sensor. In order to make a robust diagnosis against such false proofs, an entropy-based trust model may be proposed and integrated into our approach. In fact, a proof is first weighted by the reliability of its source before being used in the diagnosis. Thus, proof from distrustful (or reliable) nodes has less (or more) impact on the outcome of the diagnosis. The reliability of a node is increased resp. decreased each time it provides correct (or incorrect) diagnostic proof. Therefore, the more the node behaves poorly and provides incorrect proof, the lower its reliability, and therefore the less detrimental impact on the diagnosis.

During the estimation of the reliability of a sensor, its recent participation in the measurement of diagnoses is privileged over older ones. This privilege helps to avoid the effects of intoxication that occur when: (i) a legitimate sensor with a high trust value is compromised and begins to provide incorrect proof, or (ii) a malicious node attempts to gain the trust of the others by providing correct proof for a while before it begins to participate maliciously in the diagnosis.

The reliability of a node is also associated with its role in sending correct data. The risk of incorrect data increases as it evolves and nears its ultimate goals and may lead to more incorrect measurements. Overall, the evaluation of the confidence-based error detection in sensors shows that the defect impact along with the evolution of the trust relationships between the nodes is reduced.

References

[1] The internet of thing overview, international Telecommunication Unit, 2005

[2] A. Cocchia, "Smart and Digital City: A Systematic Literature Review," in Smart City: How to Create Public and Economic Value with High Technology in Urban Space, Springer International Publishing, 2014, pp. 13-43.

[3] J. G. S. M. a. M. P. J. Jin, "An Information Framework for Creating a Smart City Through Internet of Things," IEEE Internet of Things Journal, vol. 1, 2014, pp. 112-121.

[4] S Sicari, A Rizzardi, LA Grieco, and A Coen-Porisini. Security, privacy, and trust in the internet of things: The road ahead. Computer Networks, vol. 76, 2015, pp.146–164.

[5] M. Wu, T.-J. Lu, F.-Y. Ling, J. Sun, and H.-Y. Du, “Research on the architecture of internet of things,” in Proceedings of the 3rd International Conference on Advanced Computer Theory and Engineering (ICACTE '10), IEEE, Chengdu, China, vol. 5, pp. V5-484–V5-487, August 2010.

[6] K. Rose, S. Eldridge, L. Chapin, "The internet of things: overview, understanding the issues and the challenges of a More connected world", The Internet Society (ISOC), 2015.

[7] Zheng Yan, Peng Zhang, Athanasios V. Vasilakos, "A survey on trust management for the Internet of Things", Journal of Network and Computer Applications, Volume 42, pp. 120-134, June 2014

[8] Zheng Yan, Jun Liu, Athanasios V. Vasilakos, Laurence T. Yang, "Trustworthy data fusion and mining in Internet of Things, Future Generation" Computer Systems, V. 49, August 2015, pp 45-46.

[9] Bao F., Chen I. "Trust management for the Internet of Things and its application to service composition", Proceedings of the IEEE International Symposium on World of Wireless, Mobile and Multimedia Networks (WoWMoM), pp. 1–6, 2012.

[10] Daly EM, Haahr M. "Social network analysis for information flow in disconnected delay-tolerant MANETs". IEEE Trans Mob Comput 2009; vol. 8, no5 pp 606–21, 2009.

[11] D. Chen, G. Chang, D. Sun, J. Li, J. Jia, X. Wang, "TRM-IoT: a trust management model based on fuzzy reputation for Internet of Things", ComSIS, vol. 8, no. 4, pp. 1207–1228, 2011.

[12] Nitti M, Girau R, Atzori L, Iera A, Morabito G. "A subjective model for trustworthiness evaluation in the social Internet of Things", Proceedings of the IEEE 23rd international symposium on Personal Indoor and Mobile Radio Communications (PIMRC), p. 18–23, 2012.

[13] Ruan, Yefeng, Arjan Durresi, and Lina Alfantoukh. "Trust Management Framework for Internet of Things." 2016 IEEE 30th International Conference on Advanced Information Networking and Applications (AINA), 2016.

[14] Wang, Yating, Ray Chen, and Jin-Hee Cho. "Trust-based Service Management of Mobile Devices in Ad Hoc Networks", The Eighth International Conference on Dependability, Venice, Italy, August 2015

[15] Shawn Michael Gallaher, "An Approach For Measuring The Confidentiality Of Data Assured By The Confidentiality Of Information Security Systems In Healthcare Organizations", Doctoral Dissertation, University of Central Florida, 2012.

[16] M. A. a. D. Kantarelis., "Essentials of Inferential Statistics", University Press of America, Fourth Edition, 2004.

[17] F. G. a. L. Wallnau, "Essentials of statistics for the behavioral sciences"., Cengage Learning; 8 edition, January 1, 2013.

[18] R. Newcombe, "Confidence Intervals for Proportions and Related Measures of Effect Size", CRC Press, 2012.