CARE-CPS: Context-Aware tRust Evaluation for Wireless Networks in Cyber-Physical System Using Policies

Wenjia Li, Pramod Jagtap, Laura Zavala, Anupam Joshi and Tim Finin
Department of Computer Science and Electrical Engineering
University of Maryland, Baltimore County (UMBC)
Baltimore, MD 21250
{wenjia1, pramod1, laura.zavala, joshi, finin}@umbc.edu

***Abstract*—A Cyber-Physical System (CPS) involves a tight coupling between the physical and computational elements. Security is a key challenge for the deployment of CPS. Therefore, it is highly desirable to extract correct information from a large volume of noisy data and properly evaluate the reputation of reporting devices in CPS. In this paper, we propose a Context-Aware tRust Evaluation scheme for wireless networks in CPS (CARE-CPS), and a set of policy rules are declared to accurately describe how we determine the reputation of each reporting device based on these factors. To validate the CARE-CPS scheme, we have conducted experiments in terms of both simulation and real deployment on smart phones. Experimental results show that the CARE-CPS scheme can properly evaluate the trustworthiness of the report devices in CPS.**

***Index Terms*—Cyber-Physical System; security; trust; policy; context-awareness**

I. Introduction

A Cyber-Physical System (CPS) is a system that integrates both physical and computational elements to form a situation-aware system that responds intelligently to dynamic changes of the real-world scenarios. Since CPS is generally deployed in various critical infrastructures, security is a crucial feature that needs to be ensured in CPS, and data in CPS should be highly trustworthy. However, the data security and trustworthiness issues is a key challenge for the deployment of CPS due to the following features.

- Data are heterogeneous.
- Data come from a variety of autonomous sensors.
- Physical effects using actuators are involved.
- Control is split amongst autonomous systems.

In this paper, we propose the Context-Aware tRust Evaluation scheme for Cyber-Physical System (CARE-CPS). In CARE-CPS, multiple types of sensor data are first collected and summarized as a set of contextual conditions. Then, we declare a set of policy rules for how we should manage the trustworthiness of each sensor in different contexts.

II. Related Work

The research on Cyber-Physical System attracts increasing attention in recent years. In a latest research work, Tang et al. [1] presents a method called *Tru-Alarm*, which finds out trustworthy alarms and consequently increases the feasibility of CPS. However, this method does not take the heterogeneity of data sources into considertion, and all the sensor data are processed using the same data processing algorithm. On the contrary, our propose CARE-CPS scheme uses policies to specify trust evaluation in different contexts. In this way, different types of sensor data can be better understood and utilized in our scheme.

In our previous work [2], [3], [4], [5], [6], we tried to identify abnormal node behaviors and manage the trustworthiness of nodes in Mobile Ad-hoc Networks (MANETs). In addition, we also made some efforts to utilize policies in malicious peer detection for Mobile Ad-hoc Networks [4].

III. CARE-CPS: Context-Aware tRust Evaluation for Cyber-Physical System

In the CARE-CPS scheme, there are three major functional units, namely Data Collection, Policy Management, and Trust Management. The Data Collection unit is responsible for collecting and sending data to either the Policy Management unit or the Trust Management Unit. In the Policy Management unit, all the contextual information will be used in policies. Suppose that we are receiving readings from meters in a CPS. Various contextual information may be associated with these meter readings, such as the current weather conditions, geolocation, temperature, and signal strength. The Policy Management unit analyses the contextual information and uses policies to determine whether the meter(s) are intentionally reporting fake readings or the current environmental conditions cause those faulty meter readings.

The system can have multiple policies to consider the effects of various environmental factors. For instance, one example policy can be declared as *If the altitude is higher than 2000 feet, weather conditions are snowing and temperature is below 32F then there is a possibility of faulty reading*. This policy is represented in Jena's rules syntax specification in Table I.

In the Trust Management unit, the trustworthiness of each reporting device is evaluated based on both its reports and the contexts with which these reports are obtained. For example, if a meter is reporting incorrect data because of bad weather, then

TABLE I
POLICY TO REPORT THE POSSIBILITY OF FAULTY READINGS INCASE OF HIGHER ALTITUDE.

```
[AltitudeRule:
        (?sensorDevice a CPS:Sensor)
        (?sensorDevice CPS:has_sensed_information ?sensedData)
        (?sensedData CPS:has_weather_information ?weatherData)
        (?sensedData CPS:has_location_information ?locationData)
        (?weatherData CPS:has_weather_condition ?weatherCondition)
        (?sensedData CPS:has_altitude ?altitude)
        (?sensedData CPS:has_temperature ?temperature)
        equal(?weatherData, 4) lessThan(?temperature, 32)
        greaterThan(?altitude, 2000)
->
        (?sensorDevice CPS:faulty_device "true")
]
```

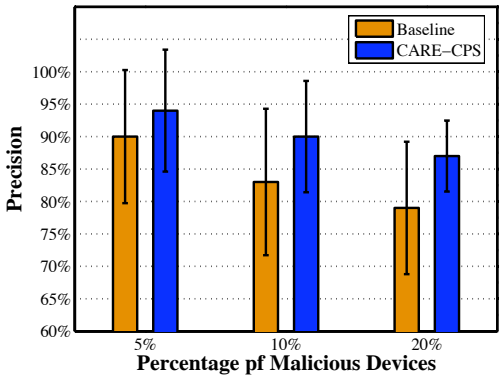

Fig. 1. Precision of CARE-CPS VS. Baseline

the trustworthiness of this meter is reduced less. In contrast, if the weather condition is normal and this meter is still reporting error readings, then its trustworthiness will be punished more.

IV. PERFORMANCE EVALUATION

We use GloMoSim 2.03 [7] as the simulation platform. Note that the simple trust evaluation method without policy management (such as trust management scheme discussed in [2], [3]) acts as the Baseline method when we evaluate the performance of CARE-CPS.

We use the following two parameters to evaluate the accuracy of our CARE-CPS scheme: Precision (P) and Recall (R). These two parameters are defined as follows.

$$P = \frac{Num\ of\ Truly\ Malicious\ Devices\ Caught}{Total\ Num\ of\ Untrustworthy\ Devices\ Caught}$$

$$R = \frac{Num\ of\ Truly\ Malicious\ Devices\ Caught}{Total\ Num\ of\ Truly\ Malicious\ Devices}$$

Each simulation scenario has 20 runs with distinct random seeds, which ensures a unique initial node placement for each run. Each experimental result is the average over the 20 runs for this simulation scenario. The simulation results are shown in Figure 1 and Figure 2.

We find from these figures that CARE-CPS always outperforms the Baseline method in terms of both precision and recall.

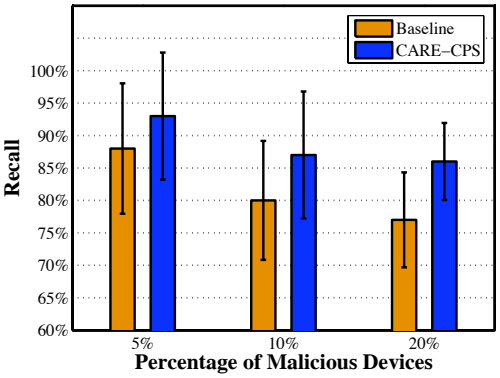

Fig. 2. Recall of CARE-CPS VS. Baseline

In addition to the simulation, we build an android application which treats smartphones as components of a Cyber Physical System. We use the device capabilities to collect sensor data and to perform reasoning over sensed data and contextual information using Jena.The experimental results show that we can properly distinguish faulty cases from normal cases based on the contextual information.

V. CONCLUSION

Security is a key challenge for the deployment of Cyber-Physical System. To address the security needs, we propose a Context-Aware tRust Evaluation scheme for Cyber-Physical System (CARE-CPS). To evaluate the performance of CARE-CPS, we conduct experiments in terms of both simulation and real deployment on Android phones. Experimental results show that the CARE-CPS scheme yields a good performance.

REFERENCES

[1] L.-A. Tan, X. Yu, S. Kim, J. Han, C.-C. Hung, and W.-C. Peng, "Trualarm: Trustworthiness analysis of sensor networks in cyber-physical systems," in *Proceeding of the 10th IEEE International Conference on Data Mining. ICDM '10.*, 2010.

[2] W. Li, J. Parker, and A. Joshi, "Security through collaboration in manets," in *Proceedings of 4th International Conference on Collaborative Computing, (CollaborateCom 2008)*, ser. LNICST, vol. 10. Springer, 2008, pp. 696-714.

[3] W. Li and A. Joshi, "Outlier detection in ad hoc networks using dempster-shafer theory," in *Proceedings of the Tenth International Conference on Mobile Data Management: Systems, Services and Middleware, 2009. MDM '09.* IEEE Computer Society, May 2009, pp. 112-121.

[4] W. Li, A. Joshi, and T. Finin, "Policy-based malicious peer detection in ad hoc networks," in *Proceedings of the International Conference on Computational Science and Engineering, 2009. CSE '09.*, vol. 3. IEEE Computer Society, Aug. 2009, pp. 76-82.

[5] W. Li, A. Joshi, and T. Finin, "Coping with node misbehaviors in ad hoc networks: A multi-dimensional trust management approach," in *Proceedings of the 11th International Conference on Mobile Data Management. MDM '10.* IEEE Computer Society, May 2010, pp. 85-94.

[6] W. Li, J. Parker, and A. Joshi, "Security through collaboration and trust in manets," *ACM/Springer Mobile Networks and Applications (MONET)*, pp. 1-11, 2010 (Online First).

[7] X. Zeng, R. Bagrodia, and M. Gerla, "Glomosim: a library for parallel simulation of large-scale wireless networks," *ACM SIGSIM Simulation Digest*, vol. 28, no. 1, pp. 154-161, 1998.