Enhancing Security in Cyber Physical Systems through Policy based Trust Management against Deception Attack

Kanchana Devi V
Assistant Professor
VIT University
Chennai Campus

Ganesan R, PhD.
Associate Professor
VIT University
Chennai Campus

ABSTRACT
The World is moving towards invisible computers, Ubiquitous Computing (any information everywhere), Pervasive Computing (which combines current network technology with wireless computing), Ambient Intelligence (which refers to electronic environments that are sensitive and responsive to the presence of people), and Traditional Embedded System (which is a closed system, not only in the sense of closed physical locations or dedicated hardware, but also closed with respect to the boundaries, where **CPS (Cyber Physical Systems)** is an open system which integrate computing and communication with monitoring and/or control of entities in physical world. CPS is the integration of several Wireless Sensor Networks.CPS is used in several applications like Automotive electronics, Avionics, Medical systems, Forestry machines, Logistics, Autonomous Vehicles, and Smart Structures. These are all "Critical Systems", the failure of the system will harm the people who depend on it. Some challenges in CPS are low power, no standard interface of sensors, low cost and high accuracy terminal devices and security. A system without security is like bank without locks. "Trust Management" plays an important role in security of CPS, since it is an open system. Trust Management is a dynamic concept which changes depending on the application. Trust is related to the authentication, authorization which comes under the hard side of trust. And also competence, reliability, integrity, timeliness, accuracy which comes under soft side of trust. Secured data or information can be trusted. This paper mainly focuses on the trustworthiness of a sensor and controller, where the trust depends on the reliability of the data sent by them. The Policy Based Trust Management is used to identify the false information sent from sensors/controllers by calculating the weight-age of the data integrity. This ensures the truthfulness of the sensor/controller in the CPS.

General Terms
A novel security algorithm has been developed to bring a secure shield for CPS, where the future is going to be CPS everywhere. Since the data collected by sensor nodes plays an important role, if it goes wrong the reflection will be very severe.

Keywords
Cyber Physical Systems, Security, Trust Management, Data Integrity

1. INTRODUCTION
Cyber Physical Systems (CPS) is a new system which has cyber capabilities in the physical world. The data from the environment will be gathered by the sensor nodes and will be sent to the sink where the data processing will take place, later the data will be directed to the controller then corresponding decision will be taken to activate the actuator. The difference between a regular control system or an embedded system and CPS is re-configurability, scalability, complexity. And also CPS has intelligence in sensors and actuators. Cyber capabilities are embedded in every physical component, and each networked. CPS is called as system-of-systems because it changes the physical system to include human, infrastructure, and platform. The resulting systems-of-systems are networked and dynamic, with highly complexity, the one who makes policies should be educated in safety, reliability, and security challenges of cyber–physical interactions [4].

In some smart environment, people with physical disabilities receive healthcare services any time for any event, in a more secure way while their dear ones are not nearby. When abnormality is reported by BAN, Smart Home Systems send information and other relevant data through the network (local controller) to nearby healthcare which can offer required response, and service.

Usually CPS gathers data from the physical environment using sensors and feed the sensor data into controller, which make decisions. The main difficulty of such systems is highly dynamic in nature. The middleware which is currently present cannot handle the dynamic nature of CPS. Thus, the CPS is leading to a 3rd generation of control systems. There will be evolution in the technology of control system to implement such kind of distributed systems. The CPS is the future and future is the CPS like Embedded is the future and the future is embedded.

2. RELATED WORK
Cyber-physical systems (CPS) are physical and engineered systems whose operations are monitored, coordinated, controlled and integrated by a computing and communication core. There is a bond between software and physical world will be manifested from the small to large and wide-area systems [2]. CPS has proof for the correctness of the overall system design. System will be more complicated, involves differential equation, and also discrete models, real-time computation and communication [18]. Several new challenges and a research roadmap are presented. CPS follows feedback process for this it requires a separate line which should be a

secure one. There are certain systems which work in real time, so far can be geographically distributed. There are several multiple time-scale systems available in overall it is called as system-of-systems [1]. The exposure of CPS is improved for the reason that controllers are prone to errors and attacks, the networks are open and large, increasing use of product so that systems are liable to the flaws of components, rules for control are suitable open and accessible, and growing functionality of CPS makes new problems [11].

Central implementations schemes are generally more accurate than local schemes. Nevertheless, it leads to non-negligible intelligibility, and have poor mistake acceptance and scalability properties. That is why distributed algorithms seem to be gaining thrust nowadays. In sensor network applications, an incident is significant and triggers a response only when it its location is known. Localization is one of the important concept which deals with how a sensor resolve its spatial coordinates. A solution to such problem is to add GPS capability in every sensor node for exact location. In general there will be large amount of sensors used then the cost of each sensor will be more which will not be suitable one. Furthermore, GPS mainly works with satellite signal which is from outside source. This restricts its usage in local environments which triggers finding new substitute for localization methods [12].

Trust is required in open system which is categorized by uncertainty and where the participants need to depend on each other to achieve their goals. Prior to engaging in interactions with other sensor nodes, a sensor node should ideally be able to estimate the likelihood of a successful interaction. There are a number of ways of achieving this goal. One way is for it to interact with all other sensor nodes in its network community and gather firsthand experience data about them. In a long enough period of time, if the behaviors of all the sensor nodes are relatively stable, the trustworthiness of each sensor node could be measured. However, this method requires each sensor node to engage in a large number of interactions before accurate assessments become available. To speed up the assessment process, a sensor node might find it beneficial to use information gathered by other sensor nodes provided the information is reasonably accurate. Since in both MANETs and WSNs, the underlying system architecture is usually distributed, TRM systems cannot assume the existence of a central trusted entity to provide reputation information about nodes. Moreover, in an open system, the accuracy of any information shared by a sensor node is questionable. A mechanism is then required to allow sensor nodes to filter out inaccurate information about a node disseminated by other sensor nodes. In the case of a CRN in which the collective decision making process occurs in a central entity which can direct communicate with all nodes e.g., a base station or a fusion center, there is no need to share second-hand information as there is only one agent.

3. PROPOSED SYSTEM

In case of emergency, people usually approach the higher authority in order to get proper solution or suggestion to their problem. Likewise if there is any abnormality (emergency) happen in the environment, the sensor nodes will report to the local sink and controller which makes time-being decisions in order to handle the situation/problem, by activating the actuators and suppose if it is Cyber Physical System a centralized and integrated controller will integrate the appropriate local controller to help in emergency situation (Figure 2). Before integrating, a cross checks should be done whether the sensed data by the sensor node are actual data or not called data integrity check in order to avoid big disasters.

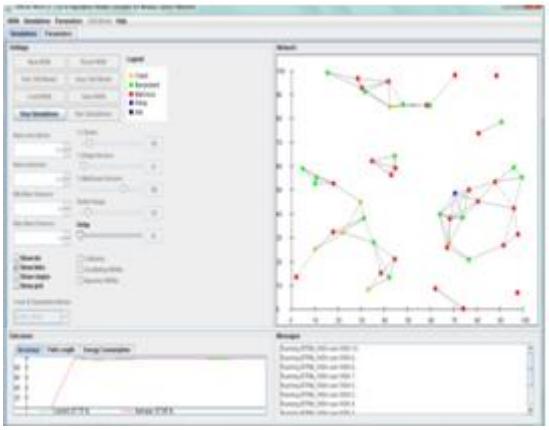

Fig 1: Simulator

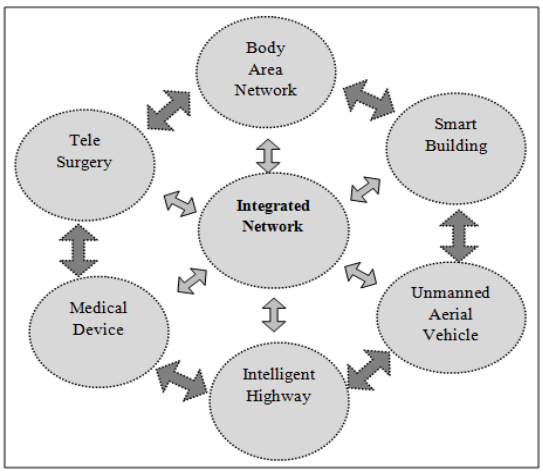

Fig 2: Structure of CPS

For checking such data integrity a policy based trust management is proposed which will check for the integrity against deception attack via policies (do's & don'ts). The do's and don'ts are the famous different technique which verifies the integrity of data in order to avoid falsification (deception attack) of information. i.e. Rules to be followed by the sensor node to prove the integrity of information by which it is weighed say $W_1=V_1+V_2+V_3+\ldots+V_n$ and $W_2=U_1+U_2+U_3+\ldots+U_n$ Where V is the value given to each do's(Correct time, Message Integrity Code, etc.) and U is the value given for each don'ts, The weight-age is calculated for trustworthiness of integrity $W=W_1+W_2$. Now the weight-age W is compared with the Threshold value (TH), If the W value is greater than the TH (W>TH) the data from the node is considered as a trusted one and if the W value is less than the TH (W<TH) then the sensor node data cannot be trusted. The trust plays a very important role because if a false node is trusted, then it will cause the whole system to be a failure one it affects the human life too, who depends on such system.

3.1 Algorithm

To check whether the sensor node can be trusted or not by testing the data

Input: Data from Sensor Node

1. Start
2. W_1,W_2 are the observed Weight-age
   Where $W_{1=}V_{1+}V_{2+}V_{3+\ldots+}V_n$ and $W_2=U_{1+}U_{2+}U_{3+}\ldots\ldots+U_n$
3. Calculate $|W|= W_1+W_2$, Fix the |TH| value
4. If |W|>|TH|
5. Then "Sensor Node can be Trusted"
6. Else "The Sensor Node cannot be Trusted"
7. End

Output: Sensor Node can be Trusted or not

The above proposed algorithm helps in identifying the malicious sensor node from sending false information called "deception attack". In order to reduce the cost not all the data will go for all policy check in our trust model. Only data which has the variation will undergo with additional support for checking the policy. In such case the computation can be reduced, energy can also be saved. Undoubtedly the cost will be automatically reduced compared to previously available trust models which are highlighted in the Table 1. Also for the future enhancement the trust model can be built for preventing the malicious sensor nodes from falsifying along with redirecting with some other sensor node to get the data and we have a plan to recover it.

The trust model should be written in the data link layer of the sink. The implementation of such policy based trust management will help the whole Cyber Physical System along with the users from bigger damages. Since, CPS is a life critical system any small error in CPS will affect the human beings life. This paper main focus on policy based trust model in the Cyber Physical Systems. Sensor nodes data is that much important, if something goes wrong it will even kill the human being. Cyber Physical System is a double edged sword for both the developers and the people who depend on it.

4. ANALYSIS

The following table reveals some of the already existing trust model and also provides a clear view of our new model in the aspects of accuracy and energy consumption.

Table 1. Analysis of existing and proposed trust models

Trust Models	Description	Accuracy	Energy Consumption
Bio-inspired Trust Management	Ant Colony Algorithm	Good	More
Eigen Trust	The system will compute a global trust value for a peer by manipulating the left principal eigenvector of a matrix of normalized local trust values	Average	Average
Peer Trust	Trust is evaluated by feedback submitted - Community based reputation and transaction based feedback	Average	Average
Policy Based Trust Management in CPS	Policy based algorithm, provides accuracy and less energy consumption	Good (Policy/Rules)	Very Less (Not all data will undergo policy check only data which has variation will undergo policy check)

5. CONCLUSION

A new model for trust management is proposed and we consider the parameters like accuracy and energy consumption status of our model. The model will be implemented through the simulator TRMSim - WSN simulator [22], which is a simulator for trust management in wireless sensor networks (Figure 1). From the Table 1, it is understood that our proposed model would be better than the other trust models in terms of its accuracy and energy consumption. In this proposed model, parameter like satisfaction factor will also be included to improve the trust worthiness of the CPS. The sensor node which sends the data will be marked as "black node" when it produces trustless data. The sensor node can loose its trust value because of this 'black' mark.

6. REFERENCES

[1] C. Neuman, 2009, Challenges in Security for Cyber-Physical Systems, in Proc. S&T Workshop Future Directions Cyber-Physical Syst. Security.

[2] Insup Lee, 2010, Cyber-Physical Systems: The Next Computing Revolution Design Automation Conference 2010, Anaheim, California, USA.

[3] Gunnar Peterson, September/October 2010, Don't Trust. And Verify, Co-published by the IEEE Computer and Reliability Societies.

[4] Radha Poovendran, August 2010, Cyber–Physical Systems: Close Encounters between Two Parallel Worlds, Proceedings of the IEEE Vol. 98, No. 8.

[5] Jatit & Lls, 2010, A Study of Security Challenges in Wireless Sensor Networks, Journal of Theoretical and Applied Information Technology.

[6] Lichen Zhang, Jifeng He et al. March, 2013. Challenges, Promising Solutions and Open Problems of Cyber-Physical Systems, International Journal of Hybrid Information Technology Vol. 6, No. 2.

[7] Parolini L., Sinopoli, B., Krogh, B. H., 2012, A Cyber–Physical Systems Approach to Data Center Modeling and Control for Energy Efficiency, proceedings of IEEE Vol. 100, Issue: 1.

[8] January 2012, Toward Continuous State–Space Regulation of Coupled Cyber–Physical Systems, Proceedings of the IEEE, Vol. 100, No. 1,

[9] June 2012, Hierarchical Trust Management for Wireless Sensor Networks and its Applications to Trust-Based Routing and Intrusion Detection, IEEE Transactions on Network and Service Management, Vol. 9, No. 2.

[10] Second Quarter 2012, Trust Computations and Trust Dynamics in Mobile Adhoc Networks: A Survey, IEEE Communications Surveys & Tutorials, Vol. 14, No. 2.

[11] A. A. Ca´rdenas, S. Aminy, Jun. 2008, Secure control: Towards survivable cyber physical Systems, in Proc. 28th Int. Conf. Distrib. Comput. Syst. Workshops, pp. 495–500.

[12] Xu Li, Inria Lille & et.al**,** July 2012, Servicing Wireless Sensor Networks by Mobile Robots, IEEE Communications Magazine.

[13] Xu Li, Rongxing Lu, Xiaohui Liang, and Xuemin (Sherman) Shen Jiming Chen Xiaodong Lin, November 2011, Smart Community: An Internet of Things Application, IEEE Communications Magazine.

[14] Xu Wu, October 2011, A Lightweight Trust Establishment Method for Wireless Sensor Networks, Advances in information Sciences and Service Sciences (AISS).Vol. 3, No. 9.

[15] Ragunathan (Raj) Rajkumar, May 2012, A Cyber–Physical Future, Proceedings of the IEEE, Vol. 100.

[16] Weiqi Dai, T., Paul Parker, Hai Jin, and Shouhuai Xu, November/December 2012, Enhancing Data Trustworthiness Via assured Digital Signing, IEEE Transactions on Dependable and Secure Computing, Vol. 9, No. 6.

[17] Insup Lee, Oleg Sokolsky, Sanjian Chen, et.al, January 2012, Challenges and Research Directions in Medical Cyber–Physical Systems, Proceedings of the IEEE, Vol. 100, No. 1.

[18] Kyoung-Dae Kim and P. R. Kumar, May 2012, Cyber–Physical Systems: A Perspective at the Centennial, Proceedings of the IEEE.

[19] Xu Li, Chunming Qiao, & et al., Sep 2012, Toward Effective Service Scheduling For Human Drivers in Vehicular Cyber-Physical Systems, IEEE Transactions on Parallel and Distributed Systems, Vol. 23, No. 9.

[20] Wattana Viriyasitavat, Andrew Martin, Third Quarter 2012, A Survey of Trust in Workflows and Relevant Contexts, IEEE Communications Surveys & Tutorials, Vol. 14, No. 3.

[21] Zhengqiang Liang and Weisong Shi, January 2010, TRECON: A Trust-Based Economic Framework For Efficient Internet Routing, IEEE Transactions on Systems, Man, and Cybernetics—Part A: Systems And Humans, Vol. 40, No. 1.

[22] Felix Gomez Marmol, TRMSim-WSN, A Trust & Reputation Models Simulator for Wireless Sensor Networks, http://ants.dif.um.es/felixgm/research/trmsim-w

[23] S. Karthik, K.Vanitha, Dr .G. Radhamani, 2011, Trust Management Techniques in Wireless Sensor Networks: An Evaluation, International Conference Communications and Signal Processing (ICCSP).