

# A Policy and Trust Driven Framework for Securing Cyber Physical Systems

Anupam Joshi, Yelena Yesha, Tim Finin, Wenjia Li, Palanivel Kodeswaran

*Department of Computer Science and Electrical Engineering  
University of Maryland, Baltimore County (UMBC)*

## 1. Introduction and Motivation

Cyber Physical Systems play a crucial role in national infrastructure and securing them is of vital importance to national security. There has been ample evidence in the recent past exposing the vulnerabilities of these systems, and this has even been reported in the popular media [1]. Further, CPS have been evolving in terms of the application domains they are being employed in ranging from patient monitoring to autonomous automobiles to nation wide power grids. Also, emerging application domains for CPS cross administrative boundaries and are not under the supervisory control of a single domain. This introduces critical issues of policy and trust that have not been traditionally addressed by the community. Cyber physical systems involve a tight coupling between the physical and computational elements and securing both the cyber and physical processes is critical to system security. Traditional methods have generally been employed to defend against physical threats to infrastructure systems. However, a cyberphysical system presents threats against the physical infrastructure that arise out of the cyber/electronic parts of it. There has been significant amount of work in securing the cyber elements of CPS such as sensors, but it has mostly focused on security of the communication links between the sensing and actuating elements [10][11][12]. We argue that in emerging application domains, we may not be able to completely guarantee physical security due to sensors being placed at inaccessible regions or due to administrative restrictions. Consequently, we propose that a more holistic approach that is policy driven and context aware is essential to secure emerging cyber physical systems. Such a framework would factor in the trust relationship among entities as well as external contextual information while processing sensor readings obtained from various sources. For example, consider Advanced Metering Infrastructure (AMI) deployments for the SmartGrid. It is possible for the power company to turn off/on power to a customer (or to a particular customer equipment such as the HVAC system), set the maximum amount of power that a customer can draw at any time etc. based on the meter readings and electronic controls (such as thermostats that accept programming signals wirelessly). There have been recent focused on provisioning the networking infrastructure

necessary to effectively support power grid communication such as GridStat [21], TCIP [22] etc. However, these works typically do not consider inter-domain security and trustworthiness as first class citizens. For example, in the home meter scenario, the physical security of the meters could be compromised and they could be hacked to report false readings. Thus the power company should weight the reported meter reading with both the established trust value of the customer as well as contextual information such as historical data of the customer, average meter readings around the vicinity etc. in its processing. This situation could even arise in inter-utility over even inter country data reporting when deciding efficient distribution mechanisms, as we discuss later in this paper.

Additionally, our policy driven approach allows the operator to specify high level goals / properties of the system rather than focusing on the low level mechanisms. This would allow operators to specify high level rules that would trigger when certain events occur such as disconnecting the system when a fault occurs, thereby preventing cascading failures.

Another example is the Cyber Physical Systems to support Intelligent Transport Systems. Such CPSs generally contains a large amount of concurrent and inter-dependent events [2]. The vehicle CPS relies on both the intra-vehicle communication and inter-vehicle communication. The intra-vehicle communication is generally utilized to control the various components of the vehicle, such as engine, steer, brake and transmission. On the other hand, the inter-vehicle communication is generally used by the vehicle CPS to implement the functionalities such as vehicle navigation, route selection, and autonomous driving. The inter-vehicle communication is normally achieved by using the Vehicular Ad-hoc Network (VANET). The communication among nearby vehicles is generally called Vehicle-to-Vehicle (V2V) communication, whereas the communication among vehicles and nearby roadside equipments is named as Vehicle-to-Infrastructure (V2I) communication. An example of VANET is shown in Figure 1 [3].

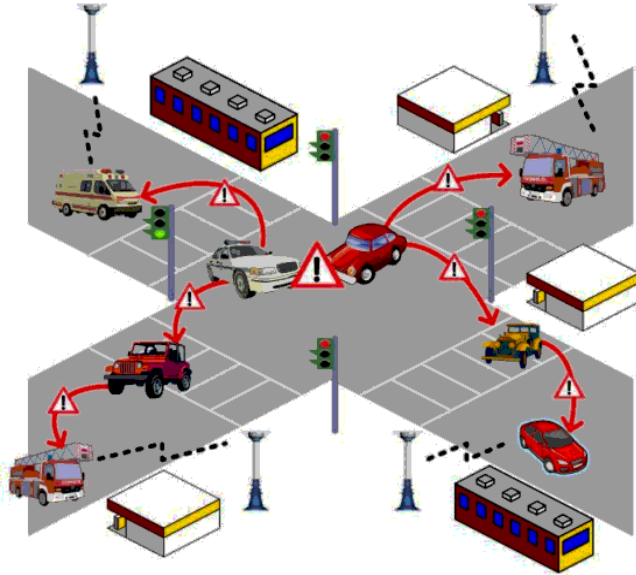


Figure 1. An Example of VANET

Traffic data is exchanged during the inter-vehicle communication. Vehicles can report their observations of abnormal road conditions, such as traffic jam, road construction, and accidents to other vehicles that they meet on the road as well as infrastructure based ITS components. This helps in individual route planning, but also overall traffic optimization, for instance using congestion pricing. However, the traffic data received from other vehicle might be imperfect due to some environmental factors. For instance, two vehicles traveling in opposite directions might have traveled out of communication range before they successfully finish traffic data exchange. In this case, the received traffic data may be incomplete and meaningless. To make things worse, vehicles controlled by malicious entities may intentionally propagate fake traffic data so as to disturb the whole transport system, and even cause crashes by feeding onboard controllers false information about the speed or movements of the vehicles ahead. As these two instances from smart electric grids and intelligent transport systems indicate, it is quite essential to work out a solution that is able to ensure the correctness and genuineness of the data exchanged between the sensing and actuating elements of a CPS to prevent attacks on the infrastructure

## 2. Related Prior Work from UMBC

Many solutions have been proposed to address the security risks in various types of infrastructure-less wireless networks, such as MANETs [4][5][6], VANETs [7][8][9], and wireless sensor networks (WSNs) [10][11][12]. In prior work, we have developed solutions to cope with various security threats especially in MANETs [13][14][15]. However, most of the current

security solutions have not taken into account the context in which the security threats exist. For example, regardless of the context in which the misbehaviors occur, most misbehavior detection and trust management systems in MANETs simply utilize the quantity of the misbehaviors witnessed by the neighbors to determine which nodes are malicious [6][14]. In other words, in the current misbehavior detection system, a node may be viewed as malicious node if it either intentionally drops packets when the communication channel is idle, or it is forced to drop packets because there is a channel collision. Therefore, it is obvious that the current security solutions may be inaccurate as well as inefficient if the context is not properly incorporated.

In some of our recent work [16][17][18], we have made efforts to incorporate the context information into various security solutions such as misbehavior detection and trust management. Given the observation that misbehaviors are deviations from the normal node behaviors, we can model the problem of misbehavior detection as a problem of how to properly identify outliers amongst all the node behaviors. We control the outlier detection process by a policy that factors in contextual conditions.

In [16], we describe a gossip-based distributed outlier detection method to detect the node misbehaviors. In this method, each node will first observe and record the local abnormal behaviors of its neighbors, and an initial view of outliers is formed based on the local observations. All the local observations will then be exchanged and the view of outliers will be updated based on the observations from other nodes. In addition, a light-weight trust management mechanism has been integrated to the outlier detection method so that observations reported by other nodes can be properly interpreted and then combined with the local observations. The trust mechanism uses some simple notions of context. For instance, packet dropping and packet modification are both viewed as node misbehaviors. However, packet dropping may be caused either by malicious intent or by environmental factors such as power failure and channel collision. On the other hand, when we observe that a node is modifying the incoming packets, we can definitely conclude that it is a malicious node. Hence, we punish more for packet modification than packet dropping.

In [17], we extend the outlier detection method and use Dempster-Shafer Theory (DST) to combine the local observations with the observations obtained from other nodes. Dempster-Shafer theory is suitable here because there is uncertainty and little "a-priori" knowledge of possible observations. We have compared the performance of the outlier detection method using DST with the outlier detection method using the Weighted Voting (WV) method and siMple aVerging (MV) method. Figure 2 illustrate Correctness Rate (CR), communication Overhead (CO), and Convergence Time (CT) of DST as

well as WV and MV with different percentage of malicious nodes.

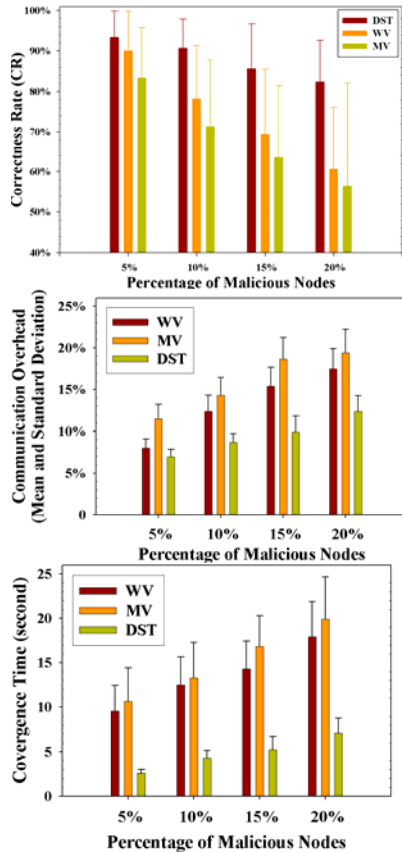


Figure 2. CR, CO, and CT with different percentage of malicious nodes (number of nodes: 100, radio range: 120m, area: 600m×600m, node motion speed: 5m/s)

From Figure 2, it is obvious that DST yields a much better performance than WV and MV with a higher percentage of malicious nodes. This is true because both WV and MV rely on enough trustworthy information to make a correct decision: MV simply follows the decision from the majority of nodes, and the weights in WV are also significantly determined by the second-hand information sent by other nodes. Hence, when there are a higher percentage of malicious nodes, the performances of both WV and MV degrade noticeably. On the other hand, DST can properly handle the outlier detection problem even in a more hostile environment because it deals with unreliable data better.

In our latest work [18], we propose and develop a policy-based malicious peer detection mechanism, in which context information, such as communication channel status, buffer status, and transmission power level, is collected and then used to determine whether the misbehavior is likely a result of malicious activity or not. In the malicious peer detection mechanism, the network/node context information is first collected and recorded, and then the corresponding security policies are enforced so that the misbehavior detection and trust

management schemes can make use of the context information to properly tell truly malicious nodes from the faulty nodes that are forced by the environmental factors to exhibit some misbehaviors.

In ongoing work, we are extending the notion of context to include factor such as initial trustworthiness, geographical location, and past experience will also be considered as part of the context, in addition to elements that are specific to a particular CPS. We believe that our policy and context driven security framework will form the basis on securing the sensing and actuating elements of a CPS, and will be able to use a variety of low level secure channel mechanisms reported in literature.

One of the important building blocks in managing infrastructure services is operator policies. Operator policies in general represent the preferences of operators towards select customers or providers which are in line with their trust relationships or business agreements. These preferences which are crucial in effectively running services can be easily modeled and implemented through policies. For example, consider the home meter example above. A utility company would tend to trust its own meter readings in the vicinity rather than its customer's reporting. Similar situations arise in inter utility scenarios as well, as envisioned in the smart grid projects where electricity would be transmitted from suppliers to customers optimally using digital technology. Demand response mechanisms are used in smartgrids to determine the amount of power flowing from suppliers to customers. In these cases, suppliers could use their preferences to determine which customers to serve and which suppliers to buy power from. Also, it is essential to ensure that power flow over existing lines does not exceed their capacity. Synchrophasor measurements which capture the health of the system in real time can be used to measure the dynamic capacity of the lines and used in determining the maximum power flow. However, most of the Phasor Measurement Units (PMU) are within the administrative control of a single domain, and therefore the trust relationship with the organization must be considered while using the Synchrophasor measurements in determining the maximum power flow. Our policy and trust driven framework will be able to capture these elements, and hence protect the CPS system from a wide class of attacks.

### 3. References

[1] <http://news.bbc.co.uk/2/hi/technology/7990997.stm>  
[2] <http://sconce.ics.uci.edu/cps-sec/cps-report.pdf>  
[3] [http://monet.postech.ac.kr/new2008/images/introduction/image\\_vanet.gif](http://monet.postech.ac.kr/new2008/images/introduction/image_vanet.gif)  
[4] S. Marti, T. J. Giuli, K. Lai, and M. Baker, "Mitigating Routing Misbehavior in Mobile Ad Hoc Networks", in Proceedings of the 6th Annual international

- Conference on Mobile Computing and Networking (MOBICOM00), Boston, MA, USA, pp. 255-265, 2000.
- [5] Y. Zhang and W. Lee, "Intrusion Detection in Wireless Ad-hoc Networks", in Proceedings of the 6th Annual international Conference on Mobile Computing and Networking (MOBICOM00), Boston, MA, USA, pp. 275-283, 2000.
- [6] S. Buchegger and J. Y. L. Boudec, "Performance Analysis of the CONFIDANT Protocol (Cooperation of Nodes - Fairness In Dynamic Ad-hoc NeTworks) ", in Proceedings of the 2nd ACM International Symposium on Mobile ad hoc Networking & Computing (MobiHoc), pp. 226-236, 2002.
- [7] M. Raya, P. Papadimitratos, and J. -P. Hubaux, "Securing Vehicular Communications", IEEE Wireless Communications, Vol. 13, Issue 5, pp. 8-15, October 2006.
- [8] G. Yan, S. Olariu, and M. C. Weigle, "Providing VANET Security through Active Position Detection", Computer Communications, Vol. 31, Issue 12, pp. 2883-2897, July 2008.
- [9] M. Raya, P. Papadimitratos, V. D. Gligor, and J.-P. Hubaux, "On Data-Centric Trust Establishment in Ephemeral Ad Hoc Networks", in Proceedings of INFOCOM 2008, April 2008.
- [10] A. Perrig, J. Stankovic, D. Wagner, "Security in Wireless Sensor Networks", Communications of the ACM, Vol. 47, Issue 6, pp. 53-57, June 2004.
- [11] C. Karlof and D. Wagner, "Secure Routing in Wireless Sensor Networks: Attacks and Countermeasures", Ad Hoc Networks, Vol. 1, Issue 2-3, pp. 293-315, September 2003.
- [12] H. Yang, F. Ye, Y. Yuan, S. Lu and W. Arbaugh, "Toward resilient security in wireless sensor networks", in Proceedings of MOBIHOC 2005, pp. 34-45, 2005.
- [13] A. Patwardhan, J. Parker, A. Joshi, M. Iorga, and T. Karygiannis, "Secure Routing and Intrusion Detection in Ad Hoc Networks", in Proceedings of PERCOM 2003, 2003.
- [14] J. Parker, A. Patwardhan, and A. Joshi, "Cross-layer Analysis for Detecting Wireless Misbehavior", in Proceedings of IEEE Consumer Communications and Networking Conference Special Sessions (CCNC 2006), 2006.
- [15] A. Patwardhan, J. Parker, M. Iorga, T. Karygiannis, and Y. Yesha, "Threshold-based Intrusion Detection in Ad Hoc Networks and Secure AODV", Ad Hoc Networks, Vol. 6, Issue 4, pp. 578-599, May 2007.
- [16] W. Li, J. Parker, and A. Joshi, "Security through Collaboration in MANETs", in Proceedings of 4th International Conference on Collaborative Computing: Networking, Applications and Worksharing (CollaborateCom 2008), Orlando, FL, USA, November 2008.
- [17] W. Li and A. Joshi, "Outlier Detection in Ad Hoc Networks Using Dempster-Shafer Theory", in Proceedings of 10th International Conference on Mobile Data Management (MDM 2009), pp. 112-121, May 2009.
- [18] W. Li, A. Joshi and T. Finin, "Policy-based Malicious Peer Detection in MANETs", submitted to 2009 IEEE International Conference on Information Privacy, Security, Risk and Trust (PASSAT 2009), August 2009.
- [19] J. Pearl, "Probabilistic Reasoning in Intelligent Systems: Networks of Plausible Inference", Morgan Kaufmann, 1988.
- [20] G. Shafer, "A Mathematical Theory of Evidence", Princeton University Press, 1976.
- [21] <http://www.gridstat.net/>
- [22] <http://www.itl.illinois.edu/content/tcip-trustworthy-cyber-infrastructure-power-grid>