Cyber-Physical Systems: Survey

Yenumula B Reddy
Department of Computer Science
Grambling State University, Grambling, LA 71245, USA
(ybreddy@gram.edu)

ABSTRACT

The cyber-physical systems are the combination of computational elements and physical entities that can interact with humans through many modalities. The security includes the malicious attempts by adversary that disrupts or destructs the functions of physical systems that affects infrastructure, businesses, and routine human life. The research in cyber-physical systems is in its infantry. The work requires the development of security models at cloud interacting with physical systems. The current research discusses four parts. The security requirements in the future engineering systems includes the state of security in cloud cyber-physical systems, security requirements in Hadoop distributed file systems and trust-based security model in sensor networks. Further, the proposed research develops the agent-based approach as an example of trust-based packet transfer. The approach keeps the each node's current status. The results show that maintaining the ratings of each node, the trust can be calculated and eliminate the malicious node.

KEYWORDS

Cyber-physical system, sensors, actuators, trust-based systems, environment, neighbor node.

1 INTRODUCTION

The United States presidential advisory committee has placed Cyber-physical system (CPS) on the priority list for federal research investment during their presentation at St. Louis in April 2008 on Science and Technology [1]. The main objectives of the report include:

- promoting the open education to help researchers, educators and students around the world
- strengthening safety and security in life sciences, USA
- paying for success to transform technology into instruction
- economic growth in industry and manufacturing
- identifying breakthrough in all fields including life sciences

Development of embedded systems with real-time performance helps to achieve the above objectives. GPU technology helps in achieving the real-time response. The SRIS interview is one of the examples of achieving the performance goals beyond the general purpose computing facilities [3].

CPSs are control systems. They are distributed, intelligent, real-time, adaptive, networked (wired/wireless) and possibly connected in the loop. CPS integrates computational and physical capabilities that can interact with humans through distinct technologies. CPS requires cyber security (privacy, resilience, malicious attacks, and intrusion detection) with improved design tools and methodology. Typical design of CPS has network of interacting elements with physical input and output. CPS links between computational and physical elements to improve usability, efficiency, safety, reliability, adaptability, and functionality. CPS has applications in robotics, military, communications, healthcare, transportation, manufacturing, energy, and infrastructure.

ISBN: 978-1-941968-03-1

Cyber world includes communications, networking, sensing, storage, processing, and controlling. The physical world includes hardware, materials, and sensors. The coordination of cyber world and physical world connects with human and changes the future computational facilities in all fields including business, scientific, defense, and healthcare with unprecedented capabilities. The CPS consists of intelligence (using sensors and actuators) with visualization that helps human in most of their daily life activities. The functionalities include flight control, electronic cabin windows in airplanes, adaptive cruise control, anti-theft devices in cars, remote visualization of house security, location services in cell phones, pacemakers in humans, robotic vacuum devices, location sensing, robot controlled operations in the medical field, and in the field of e-commerce. The future CPS capabilities include controlling of motors (breaks and engines) on road (transportation), medical, energy, defense, environment, law enforcement, and construction.

The CPS uses communications, intelligence, connects the human in real-time and has additional intelligence in sensors and actuators with strict constraints. Traditional cyber systems have procedures, policies, and methodologies. Current technology is trying to integrate cyber capabilities into every physical process including e-commerce, automation, defense, flight control, and facilities in daily life. CPS infrastructure incorporates the human and physical systems that increase the dependability of its (CPS) interface and interactions. The CPS design can improve the quality of life through the applications including rescue operations, disaster recovery, ubiquitous healthcare, and fingerprints.

The impact is far-reaching, and the goals of CPS are unlimited. Multidisciplinary approach for understanding models, methods, approaches, abstractions, analysis and design creates environment and solutions for a better life. New tools for validation, time-efficient verification, and post-facto certification are required to improve the quality of life. The current educational framework needs to be changed to meet the CPS environment. To meet the future CPS applications, it ties with multiple academic disciplines and requires course offering computer science with engineering and computational physics, anthropology and sociology, and control theory. CPS with wireless networking demonstrates safety, reliability, and security environments.

The CPS design, configuration, and automatic testing exceed today's levels of freedom, functionality, reliability, usability, and cyber security. The CPSs are expected to play a significant role in future engineering systems with new capabilities. The future research depends on standardization of (a) architectures that permit modular design and development, (b) new frameworks, algorithms, and tools, (c) dependable, highly reconfigurable and trustworthy hardware, and software components. Further, the cost effective theory and tools are required for analysis, design, and verification.

The potential of CPS improves in many areas including collision avoidance, air traffic control, robotic surgery, rescue operations, deep sea exploration, healthcare monitoring, and defense operations. The fully implemented CPS technology as a network of physical and cyber security elements that interacts with human input and output increases dramatically the adaptability, autonomy, efficiency, safety, functionality, and reliability. Currently, CPS is one of the key areas of research in defense and civil operations. Recent use of smartphones increased the importance of CPS due to the network connectivity and cloud environment. The cloud environment provides the complex computational resources and processing facilities that are impossible under local resource constraints.

Currently, research areas are partitioned into isolated sub-disciplines such as

ISBN: 978-1-941968-03-1 ©2014 SDIWC

mathematics, neural networks, genetic algorithms, networking, sensors, communications, and software engineering. CPS is an embedded system where the development involves the multiple disciplines. CPS needs diversity models and formalisms that support component-based 'divide and conquer' approach. The new divide and conquer approach may lead to a serious problem to verify overall correctness and safety of the design. Special care must be taken to use mixed model approach to CPS design for diversity of models.

2 DESIGN CHALLENGES

The grand challenges of CPS include blackout-free electricity generation and distribution; energy-aware buildings and cities; extreme yield agriculture; everlasting life assistance for senior and disabled people; safe automotive from the hazardous situation; and continuous monitoring and controlling the patient's conditions. CPS requires computer scientists and network professionals to work with experts in various science and technology disciplines to achieve scientific breakthroughs for major societal and economic gains.

The design of CPS systems requires advanced technology and incremental improvement in formal verification, software engineering processes, design patterns, artificial intelligence techniques, emulation and simulation techniques, and component design technologies. The CPS bridges the gap between cyber world (transferring information) and physical world. The CPS design must consider performance and real-time response. CPS examples are smart cities, smart grids, automotive controls, robotics, and medical devices. The question is the possibility of achieving time and performance. Time and performance can be achieved only through graphics processing units (GPU) technology using NVIDIA tools. CPS is heterogeneous design involves computation, communication devices, together with sensors and actuators.

The integration of computational power and sensor networks into automotive systems needs design safe automotive systems. They protect passengers from the hazardous situation. The design includes fault-tolerant environment of sensor network. The sensor network in the vehicle and interaction of vehicles on a higher system level involves the communication exchange between vehicles, vehicle position and speed of the vehicle. The vehicle moment on a particular road depends on accidents, traffic jam, and driving conditions on a particular road. The planning strategies during the design require fast error detection and fault tolerance.

High-tech medical system helps with networking and communication capabilities to monitor and control the patient's conditions. Designing of medical CPS with reliable embedded system are imperative. Research must focus on modeling and analysis techniques of such devices. Similar functionality is the cardiac dynamics to predict the onset of arterial and ventricular fibrillation. The GPU technology helps to achieve the simulation speeds in near real-time response [2-3]. Researchers at Urbana-Champaign (University of Illinois) achieved the HIV chemical structure "capsid," that protects the virus's genetic material using NVIDIA® Tesla® GPU accelerators [4].

Basic models of CPS deal with cyber-based physical energy system. For example, energy generation and distribution helps blackout-free electricity and creates energy aware buildings and cities. Recent studies provide the energy-based systems for maximum battery life [5, 6], minimum energy expenditure without violating time constraints [7], and cluster architecture to achieve energy efficiency [8]. More study is required to design long lasting battery and achieve energy efficient devices (consumes less energy).

ISBN: 978-1-941968-03-1 ©2014 SDIWC

Modern research on security contributed mainly to identify the authentication, key management, and honeypots databases. CPS integrates communication with the physical process. CPS-based systems do not operate under controlled environment. CPS systems must be designed and assembled with predictable and reliable components. Since no component is 100% reliable and predictable to unexpected conditions, systems must be designed to be robust for unexpected failures (similar to wireless links that coding is robust and adaptable). More details on design challenges are discussed in [9].

Nation's economy and security depend upon these essential services. Power, oil, water, transportation, communication, and networks are nation's critical assets. Protecting these assets is required as they are essential to nation's economy. The challenge in the case of a power grid is to develop a stable, fully integrated, robust, failure-free intelligent and real-time control system with cyber and physical resources. The design requires systematic analysis of the interactions between information processing, engineering design, and human interaction. Clear intellectual and scientific foundations must be incorporated to ensure overall system robustness, security, and reliability.

From system engineering point of view, CPS requires scientific methodology to build system structure and behavior. The engineering modeling ensures the data flow. The new model must include time-triggered and event-driven system applicable different time scales. As the complexity increases, CPS systems bring more privacy and security concerns. For example, medical and defense data must be protected at different levels of information disclosures. CPS systems are hybrid, distributed, and real-time with many critical applications. The components must provide comprehensive system integration and relevant quality of service properties and constraints.

Huge challenge of CPS is the design and ahead that include modeling, real-time responsiveness, data freshness, security, and energy. Added security drains energy, slows transactions and response. Real-time updates to database conflicts with other transactions and slows the transactions. Further, multi-layer model increased level of security related to increased energy consumption [10].

3 RECENT DEVELOPMENTS

Molina et al. [11] proposed a Model-based design methodology to verify different domains to work together for energy management in buildings and environments. The models include network, radio propagation, electronic system level, and quantities to be captured by the sensor systems. Derler et al. [12] uses fuel management system to discuss technologies and challenges arrive to design CPS. Mitchell and Chen [13] discussed role of intrusion detection techniques for CPS and proposed research directions in CPS intrusion detection systems (detection and Audit material).

Shi et al. [14] provided in their survey paper a better understanding of CPS methodology through three steps. First, features of CPS and its research progress are summarized through system resource allocation, model-based software design, energy control, control techniques, transmission, and management. Second, explained through classic applications health care and medicine, electric power grid, and integrate intelligent road with unmanned vehicle. Finally, the authors suggested the future research challenges. Lee [9] discussed the design challenges, need to improve the design processes, raise the level of abstraction, computing, and networking abstractions. The author concluded that the effective orchestration of software and physical resources require semantic models that reflect their properties.

Guturu and Bhargava [15] addressed the nuts and bolts of the CPS and opportunities and

ISBN: 978-1-941968-03-1 ©2014 SDIWC

technological challenges in multidisciplinary areas. Bartocci et al. [16] presented theoretical and practical challenges using automotive scenario and medical CPS. Raj et al. [17] suggested that the design, construction and verification of CPS should be addressed through cross-disciplinary community of researchers. Their presentation includes the grand challenges in advanced power grid, symbolic cyber-physical networks, disaster response, assistive devices, scientific foundations and social impact. Sha et al. [18] review the .challenges and promises and then discussed the specific research challenges in sensor networks, ubiquitous and trustworthy computing. Cardenas et al. [19] discussed the trust analysis, design, and new proactive algorithms and architectures. The explained the design reactive algorithms and architectures for real-time detection and response for a given adversary model, new algorithms on attacks that affect the performance of computing resources.

Pasqualetti et al. [20] discussed the attack detection and identification in CPS. They proposed mathematical framework for CPS, characterize fundamental monitoring limitations from graph point of view, designed the distributed attack detection model and validated through examples. Karim and Phoha [21] presented the relation between physical component and cyber component. They discussed the integration of cyber and physical systems, attack issues involved, resisting the attacks, and recovering from attacks. Fawzi et al. [22] discussed the malicious activity of the attacker on sensors or actuators. The discussion outlines the control of linear systems and estimation of attack level in the sensor network. They proposed an algorithm to estimate the state of sensors and characterize the performance.

Integration of cloud and physical systems opens the door to the adversary for launching cyber-attacks. Possible attacks may include socially engineered Trojans, unpatched software, phishing attacks, and network-traveling worms [23]. The statistics show that most of the cyber-crimes listed are unauthorized access and viruses. Recent cyber-attacks include the following [24].

- ransomware - lock the computer files and demands payments to unlock the victim's files
- fake flappy bird - fake Apps on mobile phone and take control of mobile device
- codec - tempting to watch free movie and fills with potential cyber-attacks

Colombo and Karnouskos [25] presented cloud-based industrial CPS in ERCIM news on April 2014. Computing in cloud and connectivity creates new security threats. The nature of the functionalities, degree of dependence on external resources, computational power, operations and network connectivity will be a key factor to threats on device or in-cloud. The cyber part must be independent of cloud and physical devices with appropriate interaction in cloud-based design, development, and operation.

Abid et al. [26] proposed a V-Cloud architecture keeping in view of the safety and comfort to the driver in a car (vehicle). The authors suggested a three layer architecture that includes vehicle-to-vehicle, vehicle-to-infrastructure, and CPS. The proposed architecture helps the location awareness all times (normal and emergency) and in case of vehicle theft. Further, the proposal explains the context awareness (vehicle is at accident spot or close to jamming spot or shopping mall area).

In emergencies CPS involves mobile rescue team, interaction with civilian team, diverse environment, control equipment, and the environment. Gelenbe and Wu [27] discussed the sensor assisted evacuation, rescue systems, and research issues involved. The study further discusses the integrated asynchronous control of large-scale emergency response systems, prototype platforms, and knowledge discovery for rescue.

ISBN: 978-1-941968-03-1 ©2014 SDIWC

Wireless network plays a significant role in CPS. Heterogeneous wireless testbeds for CPS applications with low hardware costs is an impressive research. Szczodrak et al. [28] presented the experimental setup with heterogeneous wireless testbeds for CPS applications and studied outdoor lighting installation in commercial parking lot as well as indoor (university building). The experiments include maximum sensor sampling frequency, collecting data through low-power wireless network, and sensing for event detection.

4 CPS AND CLOUD

The advances in technology have potential benefits with the combination of functionalities of cloud (cyber), on-devices and physical systems. High tech industries including Microsoft, Schneider Electric, and Honeywell are investigating the cloud-based CPS (CCPS) due its benefits of resource flexibility and scalability. CCPS exposes business functionalities as services. CCPS can be used for the functionalities as the traffic control, vehicle location detection, robot surgery, and healthcare. CCPS helps the isolated soldier or group of soldiers the current position in the war field and identification of enemy in the war field (modernizing the defense functionalities). The future customers take advantage of cloud (modern hardware and software) as their facility (pay per service). Figure 1 demonstrates that cloud CPS is the future architecture.

Processing of Big Data in real-time for decision making is a major problem in the current research. Big data is larger in size compared to traditional data. It has bigger storage capacity, and less adaptable. It is unstructured and to process it requires a new technology called Apache Hadoop.

Big Data can be gathered through different sensors which include medical, traffic, and social data. Healthcare system database is one of the examples of Big Data. To achieve the real-time decisions on healthcare (medical databases) systems a new platform called medical cloud cyber-physical systems (MCCPS), a fully elastic Apache-based system is required.

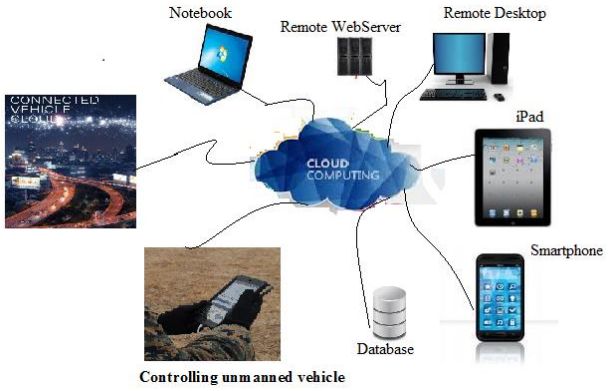

Figure 1: Cloud Architecture

Due to the nature of CCPS with added sophisticated capabilities, it demands a new design, development, and operation. The cloud (cyber) and physical part are expected closely to meet the customer demands. The degree of dependence on computational power, the nature of the functionalities, network connectivity, and operational scenarios will play a key role for hosting them on-device and or in-cloud.

5 CPS AND CLOUD SECURITY

The advantage of public cloud has reduced cost, self-service, no capital investment, scalability, and location independence. Private, public and hybrid clouds require dynamic and highly integrated mechanisms to keep the data (information) safe. Trust of the customers is their investment. Providers can instill that confidence by putting proper service level agreement (SLA). The customers and providers must mutually agree on the security standards and practices. Juniper Networks claims that they provide most efficient, scalable, secure, and cost-effective cloud environment in the industry [29].

Hadoop distributed file systems (HDFS) provides cloud-based distributed file system

and MapReduce batch job processing on large clusters using commodity servers. HDFS provides shared multi-tenant service and stores public or private sensitive data is a major problem in the security. The HDFS systems are designed with authentication and authorization. Examples include Amazon Elastic MapReduce, IBM Hadoop & Enterprise, Horton works, Yahoo, Facebook, and Twitter. Das et al. [30] discussed the notion of trust for secondary services to Kerberos authentication mechanisms in Horton work HDFS. Horton works considered in the Hadoop design by incorporating Kerberos service token mechanism as a wider adoption. The design has pluggable security mechanism in the remote procedure call (RPC) layer which is alternative to Kerberos mechanism.

Reddy [31] discussed the access control for sensitive data in HDFS. The contribution discusses the controlling the user access to databases in Hadoop cluster. The access control extends the Kerberos token mechanism using game model by adding 'accessLimit.' The mechanism recommends the MapR module that verifies the access rights of the user before filtering (reduce) and deliver the filtered response to a user query. The model recommends allocating the access rights at the time of access to data (mapping). The extended access level (right to access and retrieve data) to the doctor or nurse help the patient to limit the access to his/her personal data.

Survey of security issues in cognitive networks and data transfer in cloud cognitive networks were discussed in [32][33]. The survey discusses the security issues in cognitive radio networks, signal sensing and management issues, attacks on cognitive networks, attacks on network layers (physical, data link, network layer, transport, and application layers), the current security solutions, and privacy acts implemented in the communications. The survey suggests the requirement of careful engineering and design in cognitive radio networks with appropriate security checks.

6 ATTACK DETECTION MODELS

In CPS network, the systems are vulnerable to physical attacks as well as cyber-attacks. Figure 1 shows the networking of physical devices and cyberspace. The attack at physical components through vandalism has possible security issues at cyberspace and vice versa. The research on attack detection in most of the research papers [20][21][27] are done using sensor data. The problems are related intrusion detection [21], emergency management [27], and mathematical models [20]. The routing tree based on the integration of sensors or any physical components through network to cyberspace. Trust-based packet transfer, agent-based trust calculation, and cooperative, collaborative approach for secure packet transfer are some of the examples of secure information transfer in sensor networks [40][41][42][43][44].

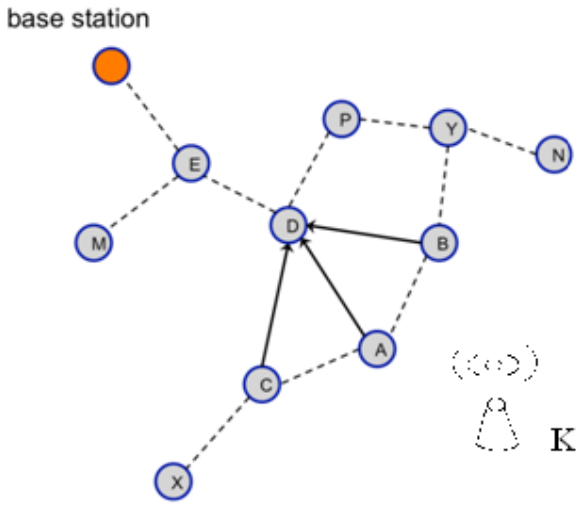

Figure 2: Wireless sensor network communication topology

Figure 2 shows that a collaborative approach to trust a node in the path. Simulations were conducted to trust the node D to transfer the packets using a collaborative approach. If the node D is updated with

malicious code, the collaborative approach detects the corrupted node.

Figure 3 shows the reputation of a node D at node A with respect to node B and C. The reputation of node D at A is given by {45][46][47]

$$R_{A,D} = \alpha.R_{A,D} + \beta.R_{C,D} + \gamma.R_{B,D} \quad (1)$$

and

$$\alpha + \beta + \gamma = 1 \quad (2)$$

where

$R_{A,D}$ reputation of node D at node A

$R_{C,D}$ reputation of node D at node C

$R_{B,D}$ reputation of node D at node B

The nodes C (node 4 in Figure 3) and B (node 3 in Figure 3) are neighbors of node A (node 2 in Figure 3). The direct reputations are at decision node, and indirect reputations are from its neighboring nodes. The values of β and γ are based on the trust of node A with respect to nodes C and B. Similarly the trust of node B and C can be calculated with respect to its neighbors. Calculate the trust of node B and node C on node D.

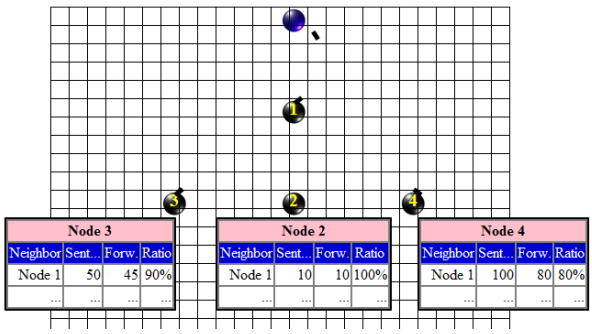

Figure 3: Simulation Of Wireless Sensor Networks using DSR Protocol

Compare the trust factor of node A with node B and node C on D. If node B and node C trusts node D then assume that there is some problem with communication and alter the route of packets. If the node A and its neighbors do not trust node D, the base station must be signaled to eliminate node D from the communication path. Trust-based approaches detect the malicious node. The trust-based approach is simple, and low-cost model compared to cryptography and various authentication methods.

The trust of node D with respect to node A is calculated using its neighbors' (node B and node C) trust on node D.

(a)Trust of node D at node B with respect to node A ($R_{B_A,D}$) is the sum of the trust of node B on node D and trust of node B on node A (R_{BA})

$$R_{B_A,D} = R_{A,D}.R_{BA} + (1 - R_{BA})R_{B,D} \quad (3)$$

(b) Trust of node D at node C with respect to node A ($R_{C_A,D}$) is the sum of the trust of node C on node D and trust of node B on node A (R_{CA}).

$$R_{C_A,D} = R_{A,D}.R_{CA} + (1 - R_{CA})R_{C,D} \quad (4)$$

Find the average of trust of node A on D, trust of node B on node D with respect A and trust of node C on node D with respect A.

$$R_{A,D} = (R_{A,D} + R_{B_A,D} + R_{C_A,D})/3 \quad (5)$$

Figure 4a shows the slow decrease of trust calculated through equations (3), (4) and (5). The confidence factor helps to confirm the successive node status. Figure 4a is drawn with higher reputation of neighbor nodes and trust of node A on node D is decreasing. Figure 4b is

drawn for higher reputation of node D at node A (above the threshold value) and lower reputation of nodes B and C on D. The results show that the lower reputation of node D at neighboring nodes effects the decision at node A.

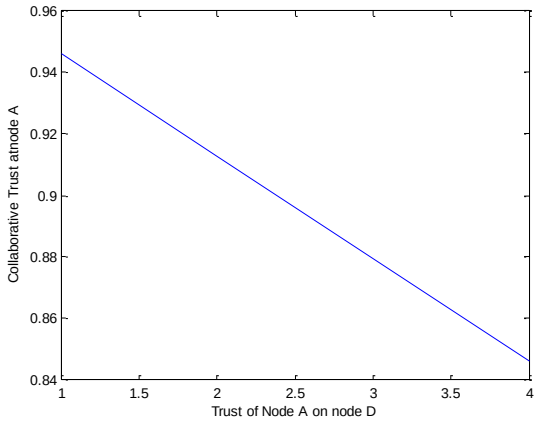

Figure 4a: Trust of node D at A with a collaborative effort

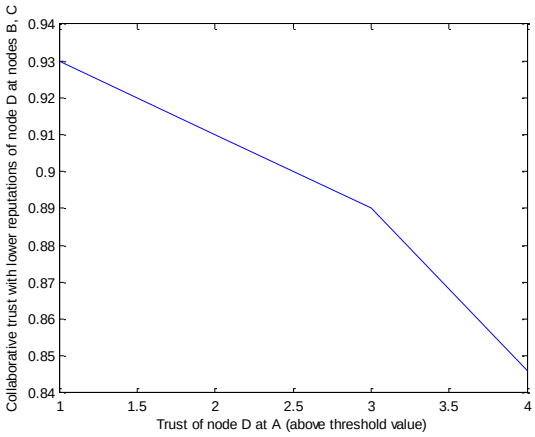

Figure 4b: Trust of node D at A with a collaborative effort with lower confidence at nodes B and C

The equations (1) and (2) approximately produce the same result. The results show that if the node D is malicious and temporarily produces better reputation at A, the collaborative effort will give warning to drop a node from the communication path.

7 ROOTKIT VIRUS AND THREAT

UNIX systems have a different type of threat. Rootkit poses serious security threat in UNIX or Linux-based operating systems. Attackers can access target computer without the owner's notice. Rootkits are difficult to remove due to the way they are used and installed. Currently, they are used to mask malware payloads more effectively. Existing anti-virus have limitations when applied to the cloud environment.

Baliga et al. [34] studied rootkits using kernel-level data structures (violation of invariants indicates an infection). They claimed that their procedure detected the rootkits using data structure invariants. Biachi et al. [35] analyzed the presence of rootkits among groups of similar machines. Zhang et al. [36] developed RootkitDet algorithm in a cloud environment. Gadaleta et al. [37] used an invariance enforce framework that takes advantage of current virtualization technology. Elimination of rootkit is in the initial stage. There are very few publications in this area of research. McAfee [38][39] claims that it invented more sophisticated solution for endpoint detection compared to malware signatures and operating-system level heuristics. Once McAfee deep defender removes the kernel-mode activities of stealthy rootkits, then rootkits were cleaned by traditional file-based scanning of McAfee VirusScan.

Elimination of rootkits is part of the operating systems and hardware dependent. Once the operating system is loaded, the rootkits will be eliminated through special virus scan process. Figure 4 shows the service providers eliminates the viruses using known security parameters and mechanisms. It is suggested to incorporate security service as part of the operating system. The recommendation is that security parameters and mechanisms required to be updated for every new release of operating system.

ISBN: 978-1-941968-03-1 ©2014 SDIWC

Figure 4: Security service providers

8 SECURITY ARCHITECTURE FOR CLOUD

Cloud CPS requires dynamic and integrated security to keep the information safe. Performance degrades as security level increase and production may go down. Scale the resources up and down as needed to control the cost and keep the customer satisfaction. Security technology must provide fault tolerance, management, and enforcement level. Organization should have total visibility of users, resources, services, and control of network traffic. Figure 5 depicts the proposed cloud integrated security.

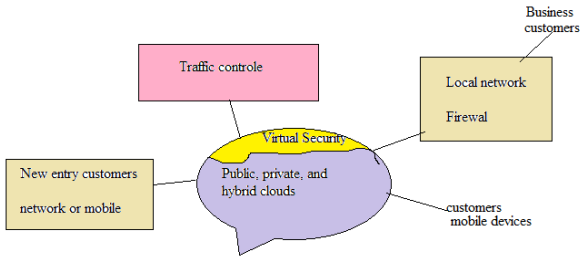

Figure 5: Cloud Integrity security

Various clients include Government, Industry, Defense, Public, and private partners access the cloud. The virtual environment creates a window for each customer interacting with the system and allocates needed space for the customer. The system reutilizes the space as soon as the client ends the job. The virtual environment helps the customers to allocate required space and reutilizes to cy other customers as soon as the job completed.

Cloud integrity is designed to guide policies for information security within organization and network. It involves the maintaining consistency, accuracy, and trustworthiness of data over its entire lifecycle. Security parameters depend upon the sensitivity of information and users connected to the information. If the environment is a hospital, access to patient's information depends on the user is a nurse, an administrator or a doctor. The doctor can access all medical records of a patient to diagnose a health problem. Nurse has a limited access to total information. Similarly, other people interacting with a patient have limitations to patient's personal information.

In business, information access changes depending upon the type of employee. Retrieval of information, modification of information depends upon the access rights. The virtual security evaluates the users interacting with resources to access or process the information.

9 RESEARCH CHALLENGES

Research challenges for cloud CPS involve multiple directions. Business, healthcare, surgery, traffic control, criminal, defense, environment, mobile devices, and scientific data are some of the problems. Infrastructure protection and information security takes a significant role of CCPS. Problem like rootkit virus takes a long time to solve solutions. McAfee published the solution for rootkit and application is not in the market.

Medical CPS for monitoring and controlling of patient's bodies requires sophisticated embedded systems with network communication capabilities. Reliability and safety take primary importance. Malfunction of these devices can have an adverse reaction on patient's body. Current GPU (graphics processing unit) technology can replace supercomputing facility for real-time simulation of organs.

The sensor networks and computational power enabled the development of various systems to assist the driver during motion.

ISBN: 978-1-941968-03-1 ©2014 SDIWC

Vehicle to vehicle and vehicle to infrastructure communication helps to minimize the jamming and accidents. Research needed for a new design (for intelligent vehicles) to prevent accidents, multiple collisions, and sending automated emergency calls.

Conducting biological experiments using robot controlled design is required that can be formulated through mathematical analysis and pattern analysis algorithms. Closely related problem is providing elderly care at home without sending them to expensive nursing homes. Research is required to create CPS infrastructure that supports the telepresence to elderly care at their home. Major financial benefits results, when elderly can live independently without loss of privacy. It is possible only with new technology through cloud CPS.

The scientific challenges of integration of cyber-physical systems are as follows.

- The future design includes a new paradigm for real-time resource management that goes beyond traditional methods. The interconnection of mobile devices requires dynamically reconfigured and system infrastructure meets these demands.
- Reliability, safety, and security of CPS against environment attacks and natural disasters. Fully tested perfect physical devices are not available. Need such devices for high reliability.
- Quality of service is one of the requirements in heterogeneous hybrid environment.
- Users of CPS need high level of trust. Customers' (users) trust can come with reliability, safety, security, privacy, and usability.

.

The challenges are more and research is in its infantry in the cloud CPS and security.

8 CONCLUSIONS

In this paper, we discussed several key research challenges in the design and developed cloud-based cyber-physical systems and their security. The paper provides the state-of-the-art in cloud CPS and new design and research challenges. Research issues in medical, business, automotive industry, elderly needs, traffic control and security in cloud and infrastructure.

The security requirements in Hadoop distributed file systems and Kerberos service token mechanism and need for modification of access rights in HDFS were discussed. We highlight the pluggable security mechanism in the remote procedure call (RPC) layer which is alternative to Kerberos mechanism.

The research describes various attack detection models in cloud, infrastructure, and system kernel. The paper further discusses the current state of detection of rootkit virus and McAfee solution.

10 ACKNOWLEDGEMENTS

The research work was supported by the AFRL Collaboration Program – Sensors Directorate, Air Force Contract FA8650-13-C-5800, through subcontract number GRAM 13-S7700-02-C2.

REFERENCES

[1] Presidential Advisory Committee Report: Cyber-Physical Systems Summit, April 25, 2008, Missouri, http://ostp.gov/pdf/nitrd_review.pdf

[2] E. Bartocci et al., "Towardreal-time simulation of cardiac dynamics", in proc. Of CMSB 2011, New York, pp. 103-112.

[3] NVIDIA., "GEO Intelligence Case Study", http://www.nvidia.com/content/tesla/pdf/sris-case-study-final.pdf, 2013

[4] http://nvidianews.nvidia.com/News/Breakthrough-in-HIV-Research-Enabled-by-NVIDIA-GPU-Accelerators-9a2.aspx, 2013.

[5] W. Jiang, G. Z. Xiong and X. Y. Ding., "Energy-saving Service Scheduling for Low-end Cyber-Physical Systems", Proc. Of 9th Int. Conf. for Young Computer Scientists, 2008.

[6] C. J. Xue, G. L. Xing, Z. H. Yuan, et al., "Joint Sleep Scheduling and node Assignment in Wireless

Cyber-physical Systems", proc. 29th Int. Conf. on Distributed Computing Systems Workshop, 2009.

[7] Q. H. Tang, S. K. S. Gupta, and Varsamopoulos, "Energy-efficient Thermal-aware Task Scheduling for Homogenous High-performance Computing Data Centers: A cyber physical approach, IEEE Transactions on Parallel and Distributed Systems, vol. 19. 2008, pp. 1458-72.

[8] J. R. Cao and H. A. Li., "Energy-efficient Structuralized Custering for Sensor-based Cyber Physical Systems", Proc. Symposia and Workshops on Ubiquitous, Automatic and Trusted Computing, 2009.

[9] E. A. Lee., "Cyber Physical Systems: Design Challenges", Invited paper, International Symposium on Object/Component/Service-Oriented Real-Time Distributed Computing (ISORC), Orlando, FL, 2008, pp. 363-369.

[10] Nikolaos E Petroulakis, Ioannis G Askoxylakis, Apostolos Traganitis, and George Spanoudakis. A privacylevel model of usercentric cyberphysical systems. In Human Aspects of Information Security, Privacy, and Trust, pages 338–347. Springer, 2013.

[11] J. M. Molina, M. Damm, J. Haase, E. Holleis, and C. Grimm., "Model Based Design of Distributed Embedded Cyber Physical Systems", Models, Methods, and Tools for Complex Chip Design Lecture Notes in Electrical Engineering, Vol. 265, 2014, pp 127-143.

[12] P. Derler, E. A. Lee, and A. S. Vincentelli., "Modeling cyber–physical systems", Proc. of the IEEE magazines, 100(1):13–28, 2012.

[13] R. Mitchell and I. Chen., "survey of intrusion detection techniques for cyber-physical systems", J. ACM Computing Surveys, vol. 46, issue 4, pp. A1 – 27, 2014.

[14] J. Shi, J. Wan, H. Yan, and H. Suo., "A survey of Cyber-Physical Systems", Proc. Int. conf. on Wireless Communications and Signal Processing, Nov 2011, pp. 1-6.

[15] P. Guturu and B. Bhargava., "Cyber-Physical Systems: A confluence of Cutting Edge Technology Streams," International Conference on Advances in Computing and Communication ICACC-11, 2011, India.

[16] E. Bartocci, O. Hoeftberger and R. Grosu., http://ercim-news.ercim.eu/en97/special/cyber-physical-systems-theoretical-and-practical-challenges, April 2014.

[17] R. Rajkumar, I. Lee, L. Sha and J. Stankovic., "Cyber-physical systems: The next Computing Revolution", 47th ACM/IEEE Design Automation Conference (DAC), 2010, pp. 731-736.

[18] L. Sha, S. Gopalakrishnan, X. Liu, and Q. Wang., "Cyber-Physical Systems: A New Frontier", IEEE International Sensor Networks, Ubiquitous and Trustworthy Computing (SUTC 2008), 2008, pp. 1-9.

[19] A. Cardenas, S. Amin, and S. Sastry., "Secure Control: Towards Survivable Cyber-Physical Systems", 28th International conference on Distributed Computing Systems Workshops (ICDCS 2008), 2008, pp. 495-500.

[20] F. Pasqualetti, F. Dorfler, and F. Bullo., "Attack Detection and Identification in Cyber-Physical Systems", IEEE Transactions on Automatic Control, vol. 58, issue 11, 2013, pp. 2715-2729.

[21] M. Karim and V. Phoha., "Cyber-physical Systems Security", Applied Cyber Physical Systems, edited by C. Sang, U. Suh, John Tanik, John N. Carbone, and Abdullah Eroglu., Springer 2014, ISBN: 978-1-4614-7335-0, pp. 75-84.

[22] H. Fawzi, P. Tabuada, S. Diggavi., "Secure Estimation and Control for Cyber Physical Systems Under Adversarial Attacks", IEEETransaction on Automatic Control, Vol. 9, issue 6, 2014, pp. 1454-1467.

[23] http://www.infoworld.com/article/2616316/security/the-5-cyber-attacks-you-re-most-likely-to-face.html

[24] http://www.nbcnews.com/tech/security/beware-these-4-common-dangerous-cyberattacks-n162106

[25] A. W. Colombo and S. Karnouskos., "Cloud-Based Industrial Cyber-Physical Systems", http://ercim-news.ercim.eu/en97/special/cloud-based-industrial-cyber-physical-systems, April, 2014.

[26] H. Abid, L. Phuong, J. Wang, S. Lee, and S. Qaisar., "V-Cloud: Vehicular Cyber-Physical Systems and Cloud Computing", Proc. 4th Int. Symp. On Applied Sciences in Biomedical and Communication Technologies (ISABEL '11), Article No. 165, ACM New York, NY, USA ©2011, ISBN: 978-1-4503-0913-4

[27] E. Gelenbe and F. Wu., "Future Research on Cyber-hysical Emergency Management Systems", Future Internet 2013, vol. 5, pp. 336-354.

[28] M. Szczodrak, Y. Yang, D. Cavalcanti, L. Carloni., "An Open Framework to Deploy Heterogeneous Wireless Testbeds for Cyber-Physical Systems", Proc. of SIES, 2013, pp. 215-224.

[29] Juniper Networks, "Networks that know how to think outside the box", www.juniper.net/us/en/dm//virtualrevolution

[30] D. Das, O. O'Malley, S. Radia, K. Zhang., "Adding Security to Apache Hadoop", Horton Technical Report 1, www.Hortonworks.com.

[31] Y. Reddy., "Access Control for Sensitive Data in Hadoop Distributed File Systems", Third International Conference on Advanced Communications and Computation, INFOCOMP 2013, November 17 - 22, 2013 - Lisbon, Portugal.

[32] Y. Reddy., "Security Issues and Threats in Cognitive Radio Networks" AICT 2013, June 24-28, 2013, Rome, Italy.

[33] Y. Reddy., "Solving Hidden Terminal Problem in Cognitive Networks Using Cloud Application", SENSORCOMM 2012, August 19 - 24, 2012, Rome, Italy.

[34] A. Baliga, V. Ganapathy, and L. Lftode., "Detecting Kernel-Level Rootkits Using Data Structure Invarients", IEEE Transactions on Dependable and Secure Computing, Vol. 8, No. 5, sept 2011, pp. 670-684.

[35] A. Bianchi, Y. Shoshitaishvili, C. Kruegel, and G. Vigna., "Blacksheep: Detecting compromised Hosts in Homogeneous Crowds", ACM Conference on Computer and Communications Security, CCS '12, 2012, pp. 341-352.

[36] L. Zhang, S. Shetty, P. Liu, and J. Jing., "RootkitDet: Practical End-to-End Defense against Kernel Rootkits in a Cloud Environment", Europian Symposium on Research in Computer Security (ESORICS 2014), 2014, Sept 7-11, 2014. Pp. 475 -493.

[37] F. Gadaleta, N. Nikiforakis, Y. Younan, and W. Joosen., "Hello rootKitty: A lightweight invariance-enforcing framework", Proc. Of the 14th International Conference on Information Security, ISC'11, 2011, pp. 213-228.

[38] R. Broida, "Root out Rootkits with Free TDSSKiller", PCWorld, Feb 2012.

[39] McAfee White Paper, "Root out Rootkits, An inside look" http://www.mcafee.com/us/resources/white-papers/wp-root-out-rootkits.pdf

[40] Y. B. Reddy and Rastko Selmic., "Agent-based Trust Calculation in Wireless Sensor Networks", SENSORCOMM 2011, August 2011.

[41] Y. B. Reddy, Sanjeev Kafle, and Rastko Selmic., "Cooperative and Collaborative Approach for Secure Packet transfer in Wireless Sensor Networks", SENSORCOMM 2011, August 2011.

[42] Y. B. Reddy and Sanjeev Kafle., "Protecting data from unauthorized users using Honeypots Technique", CSOC 2011, January 24-31, 2011

[43] Y. B. Reddy and Rastko Selmic., "Secure Packet Transfer in Wireless Sensor Networks – A Trust-based Approach", IARIA- ICN 2011, January 23-28, 2011 - St. Maarten.

[44] Y. B. Reddy and Rastko Selmic., "Trust-based Packet Transfer in Wireless Sensor Networks", Communications and Information Security (CIS2010), IASTED, Nov 8-10, 2010,USA

[45] J. Carbo, J. M. Molina, and J. Davila., "Trust Management through Fuzzy Reputation", International Journal of Cooperative Information Systems", Vol. 12, Issue 1, 2003, pp. 135-155.

[46] H. Chen, H. Wu, J. Hu, and C. Gao., "Agent-based Trust Management Model for Wireless Sensor Networks", International Conference on Multimedia and Ubiquitous Engineering, 2008

[47] A. Boukerche, and X. Li., "An Agent-based Trust and Reputation Management Scheme for Wireless Sensor Networks", IEEE GLOBECOMM, 2005.2nd ACM workshop on Security of ad hoc and sensor networks (SASN '04), October 2004, pp 66-77.