Journal of
Information Technology & Software Engineering

Bisoyi and Reza, J Inform Tech Softw Eng 2017, 7:2
DOI: 10.4172/2165-7866.1000198

Research Article Open Access

Toward Securing Cyber-Physical Systems Using Exact Cover Set

Sameer Kumar Bisoyi and Hassan Reza*

School of Aerospace Sciences, Department of Computer Science, University of North Dakota, North Dakota, USA

Abstract

Cyber physical systems (CPS) are computer systems that integrate computing, coordination and communication systems in order to monitor physical entities in the physical world. As they interact with the critical systems and infrastructure that may impact real life. There are many issues in design and constructions of these types of systems. One of the key issue that receives so many attention is the security of such systems. Although security solutions for Information Systems handle the security issues associated with Traditional IT security, but the impact of a failure in a cyber-physical system demands a different approach to handle security issues related to the cyber world. In this work, we focus on using a key agreement technique known as Physical Signal Key Agreement (PSKA) technique using the Exact Cover method to generate the random key which will be embedded into an access control model known as the Modified Context-Aware Security The feasibility of our framework (MCASF) to handle both normal and critical situation on demand is demonstrated via a Pervasive Health Monitoring Systems (PHMS).

Keywords: Cyber-physical systems; Trusted computing; Context-aware security; Information security; Exact covering; Modified context-aware security; Framework; Software engineering

Introduction

Cyber-physical systems [1] (CPS) combine the computing and communication capabilities with the entities in the physical world in terms of monitoring as well as control. Typically, Cyber-physical system consists of the cyber systems and the physical world. The physical process can either be natural or artificial. The CPS is a combination of devices that incorporates computing and communication capabilities into physical processes to manage the physical activities of monitoring and control. The communication between the cyber system and the physical process creates new communication channels which make it more vulnerable to security issues. Some examples of such attacks are the recent attack on the air traffic control mission-critical systems [2], an attack on the power system that resulted in power outage [3], CarShark that can turn off a car engine remotely [4], Stuxnet (i.e., a powerful virus which attacked the whole Siemen's networks, almost crippled it, etc. [5]). The most dangerous of all would be a remote hacking on artificial human organs which can control all its activities from outside the body [6].

Cyber-physical Systems are extremely critical in nature due to its close ties with the real-time systems. So the security solutions have to be not only different, but efficient. Though the security solutions for Information Systems provide some level of security, it's still just not enough. For national critical systems like Supervisory Control and Data Acquisition systems (SCADA) that handle national interests like Oil and Natural Gas, Electric Power Grid; any sort of system failure can impact public domain irreparably.

However; it's not only limited to that but also the issue of communicating securely is an important feature of the Cyber Physical Systems in dire need to be addressed. They especially rely on the interoperation of different heterogeneous systems that the traditional systems lack. Although the security of CPS greatly focuses on reliability and prevention, utmost focus of CPS protection is to mitigate malicious cyber-attacks.

To fully analyze the security needs for Cyber Physical Systems, we need to discuss the needs of Secure Control and possible attacks or threats. Although security solutions from Information Security and Network Security measures can help mitigate these issues to some extent, they alone are certainly not sufficient. To achieve this, we need to address the issues that are related to security issues that are prone to malicious cyber-attacks.

At present, there are two security methodologies that work side by side with the CPS Security. Both computer and network security focus on how to prevent faults, however to recover a system already stuck due to unknown faults or uncertainties is addressed by control systems. However, the security of a system against a malicious adversary still needs plenty of work which we are going to outline in this paper.

Background

Even today, the focus on security still relies on improvising the existing mechanisms of traditional IT security for the mission-critical Cyber Physical Systems. Although these solutions work to an extent in providing security, we still need to underline the difference between a traditional Information Systems and a Cyber Physical Systems which will help outlining the security needs that are separately needed in order to ensure that the systems also handle security issues emerging from the attacks or faults in the cyber world. Traditional IT security focuses on central servers while the need for CPS security needs to emphasize on edge clients.

The major issue with CPS is to accommodate the software upgrades or patches. An example of this is the complete system shutdown of a nuclear power plant in Georgia in the year of 2008 [7]. The shutdown was a result of a software patch deployed to a system which was meant for monitoring. The patches reboot the system and reset the data which the system interpreted as a drop in water level of the reservoir meant to cool radioactive nuclear rods and shut down the system [7].

Real-time system properties of CPS pose another challenge [8]. It's not that real-time requirement is the only prerogative of the Cyber Physical Systems, rather it is a requirement of traditional IT systems as well. However; in CPS, the real-time requirement takes the topmost priority as failing to meet a deadline can prove to be completely hazardous, utmost failure of the system. In CPS, the response time to

***Corresponding author:** Hassan Reza, School of Aerospace Sciences, Department of Computer Science, University of North Dakota, North Dakota, USA, Tel: +701-777-4127; E-mail: reza@aero.und.edu

Received March 16, 2017; **Accepted** March 24, 2017; **Published** March 30, 2017

Citation: Bisoyi SK, Reza H (2017) Toward Securing Cyber-Physical Systems Using Exact Cover Set. J Inform Tech Softw Eng 7: 198. doi: 10.4172/2165-7866.1000198

meet any deadline is absolutely necessary and cannot be compromised at any instant.

Damage to the physical environment, faults in sensors and actuators, response time pose significant challenges that separates a CPS from traditional IT systems.

General Workflow of CPS

There are basically four steps in the workflow for CPS [9].

Monitoring: Monitoring the processes and environment is a primary function of the CPS. It is used to monitor the past activities and predict the future activities of the CPS.

Networking: Networking means collection of data through various means. Multiple sensors can be used to collect data to be aggregated to be analyzed further to provide computing capabilities to the CPS.

Computing: This step deals with the analysis as well as the verification of data which are collected during the Networking phases to see if it satisfies the pre-defined criteria. If the criteria have not been met, then appropriate action has to be taken.

Actuating: This is the final step in the workflow of CPS. This step is meant for actuating real actions formulated during the Computing phase. Actions are determined in terms of whether the criteria have been met.

Security goals and requirements of CPS

Confidentiality: It is an important feature that deals with the prevention of user's private data being revealed to unauthorized users [10]. Confidentiality is not just a requirement of the Information Systems, but also of CPS. To fully understand this, take the example of a banking user. The user has to log in using his own username and password and perform the transactions. These transactions should be revealed only to the user when he logs in. If an unauthorized user is able to view this data by snooping or by any other means, then it is a breach of confidentiality [11]. Though useful, confidentiality alone is not sufficient to handle the issues related to the breach in communication channels between user and controller. For this, the CPS has to impose better security on communication channels.

Integrity: It is the feature that deals with the modification of data with proper authorization [12]. When an unauthorized user or adversary is able to modify data without proper authorization and the user believes it to be true, then integrity is violated [10]. It is achieved by preventing such users to manipulate the existing data to malign the integrity.

Availability: It is the feature that deals with the availability of the system on demand [10]. In CPS, it is vital that the system is available whenever in demand.

Major types of attacks to CPS

We summarize the types of attacks to CPS as follows [9]:

Compromised-key: This attack happens when the secret code to access a CPS is compromised [13]. The adversary can use this key to enter into the system and modify data without authorization and knowledge of the sender or receiver. Along with manipulating data, the adversary can also obtain keys to several other systems by computing the available compromised key and gain access that is not meant for him. Most of compromised key attacks happen with the help of reverse engineering on available physical processes.

Man-in-the-middle: When false messages are sent to the operator, the operator, being unaware of the situation, acts on it. The operator maintains appropriate action based on protocols which are applicable to normal situations whereas that can be disastrous when applied at a time it's not needed or, not applied when it actually is needed. Because the operator fails to recognize a Man-in-the-Middle attack [14], so the actions he takes according to the protocol for normal situations can be hazardous to the CPS.

Eavesdropping: Eavesdropping happens when someone without authorization intercepts data communicated in a system [15]. While eavesdropping, the adversary does not interrupt the communication, rather intercepts the data communicated through the system. As CPS is prone to such attacks, so the eavesdropping usually takes place through the traffic analysis of the monitoring data transferred in the sensor networks that has been collected periodically through monitoring.

Denial-of-service (DoS): The Denial of Service, otherwise known as DoS, is a type of attack that occurs when an adversary is successful in making the system unavailable due to different circumstances [16]. Some of those circumstances are: flooding or blocking the communication channels to deny normal service to the system, sending invalid data to cause abnormal behaviour of the services. In short; DoS interrupts normal work or use of the services and; paralyzes the availability of the system.

Literature Survey of Available Solutions

For our proposed research, we have surveyed variety of solutions that exist today for the security of Cyber Physical Systems, some of which have been described in the following section.

Solution from information security

In this section, we discuss about the existing solutions from the Information Security and their shortcomings [17]. One of the most prominent features that can be used is authentication. It can be used to prevent user personalization so that no one else can impersonate the user. Access Control can also be used to prevent unauthorized access. It is also useful in limiting user's access to how much he/she is allowed to access. Encryption or digital signatures can be used to maintain data integrity. Different tools can also be used to verify the system's correctness and behavior. In case of CPS, principles of redundancy can also be used to prevent a single point of failure, to branch out backups. The system can employ the separation of privilege option to limit access of an unidentified entity that is trying to misuse the system for its own benefit. However; no matter how careful we become, it's impossible to maintain that a system can be a hundred percent full proof of any attack or adversary. Acknowledging that, some tools can be designed specifically with the purpose of intrusion detection and response. Though they are useful, still there can be cases of false alarms and cunning attacks that slip these detections.

However; it's still better to have some security rather than no security. To ensure data confidentiality, some mechanisms of soft cryptography can also be employed.

At the end, an adversary model can be designed in a way to get into an adversary's mindset, get some insight into the real reason of the problem and design a system to overcome such intents.

Though the above mentioned security solutions may mitigate the security issues, there can still be human errors, faulty design or bugs that can make the system vulnerable. To overcome this, we need to be able to design a system that continues even while under attack [18]. The term for this feature is known as Survivability of CPS. Survivability is defined as the graceful degradation of the CPS system when it's facing an attack. Most of the previous techniques that we discussed, focus on availability and integrity of the system under network point of view. They never addressed the issues of deception or DoS attacks on the system. These attacks can affect the estimation and control algorithms, and make the system susceptible to any adversary. Even the tools designed for intrusion detection and response have not considered algorithms for such attacks, especially when the deception attacks are originated from compromised controllers. Furthermore, most of the existing solutions force the design of a human response system. Also; CPS is almost always safety-critical and there is no margin for error. In such situations, waiting for human response to hazardous attacks is a lag in the security. What needs to be done instead, is to design an autonomous, real-time decision making algorithms that gets rid of the response delays by a human response system such that the safety of the safety-critical systems is never compromised.

Lastly, there is still a need of extensive research to fully understand and develop an adversary model so that the real nature of the problem is estimated in time and successive steps can be taken in advance to ensure the safety of the CPS.

Solution from control theory

One of the major problems in Control Theory is to design such a policy in order to keep an unstable system stable under the feedback loop. The major issue of the denial of service (DoS) attack can be raised from the constraints imposed on the CPS such as packet loss, delay in response time, bound capacity etc. Such constraints can lead to a DoS attack which is a major attack on availability which can make the system so vulnerable that it becomes impossible to bring it back to stable. This can also lead to the implementation of incorrect control policies. That is why there is a need to do some extensive research as in how to include network characteristics in case of a control policy design [19,20].

Another problem in Control Theory is the shutting down of the whole system due to a single point of failure. To continue operations while under a failure mode, redundancies need to be incorporated so that a single point of failure does not occur. Whenever a failure occurs, the system should be able to undergo a graceful degradation in performance limiting the negative effects. So, research in fault tolerant control also needs to be addressed [21].

Lastly; there is a need to design distributed algorithms to address distributed estimation for systems that are limited in transmission power and memory [22].

Control Theory is considered to be better than Information Security solutions. However; research on fault tolerant control is still needed. It should be able to provide better security under Deception and DoS attacks. What we mean is that, a robust control and estimation algorithm should be designed to handle such attacks. Under such attacks, worst-case performance should be optimized.

Along with the state of the system, state of communication network should be estimated. Especially; it should address the Quality of Service (QoS) and integrity of the data and control policies. The primary objective should be to optimize performance which is the essential key of the Control Theory.

Redundancies should be addressed properly so that any form of single point of failure does not occur at any moment. Instead these should be combined and let the system degrade its performance gracefully.

While the above redundancies are in place, we should design trust management schemes to handle worst-case performance. So; extensive research is needed to be done not only in designing the control policies, but also in developing a design to include worst-case performance.

Context-aware security framework

In this framework, the context of the application is determined to be incorporated into the system to handle the security features employed by the system. Such security measurements can be encryption, access control, and authentication and so on. This dynamic adapting of the environment by context coupling is known as the Context-Aware Security Framework [9].

Before we move on to further analysis of the framework, we need to define what we actually mean by context. Context is nothing, but a set of environments or physical attributes that determines the system's behavior on the application [23]. Context can be achieved via various sources and can vary from location to system and so on. Context can be divided into four categories which are as follows:

- System Context (CPU, Network etc.)
- User Context (Location, Medical History etc.)
- Physical Environment Context (Weather, Temperature etc.)
- Time Context (Time)

Most focus is on the context that are most applicable to characterize the situation and apply the context to handle the controls to prevent unauthorized access, leak of information, disruption, unwarranted termination of application etc. in order to provide the basic goals of Information Security that are integrity, availability and confidentiality. Under the attack, the system should employ the adversary model as one of its security-relevant contextual attributes. The attributes build the context of the application as in how to choose the most appropriate controls and configuration to mitigate these issues. The values of these attributes determine the choice of controls and configuration under a certain situation.

There are various schemas and security protocols which will be analyzed in the future of Context-Aware Security Framework. Some of which are Context-Aware User Privacy, Context-Aware Mutual Authentication Protocol, Context-Aware Access Control and Context-Aware Intrusion Detection. Context-Aware User Privacy prevents eavesdropping whereas Context-Aware Mutual Authentication Protocol prevents Man-in-the-Middle attacks. Context-Aware Access Control handles problems associated with the access control, and Context-Aware Intrusion Detection manages unwarranted intrusion and DoS attacks.

Trusted Computing in CPS

Trust can be defined as how much a trustor is willing to rely on the CPS even if breach of trust is a possibility. It is the confidence the user has on the performance of the system. When this confidence is justified to satisfy the user needs, it is known as a trusted application or system. The extent to which the user's expectation has been is termed as Trustworthiness [24].

A security model has been proposed to determine the trustworthiness of a system by the following criteria [24]:

The aspects that can affect our systems can never be one hundred percent predicted. Neither can rigorous testing and verification can prove its trustworthiness. So to operate a system successfully, trust to a certain extent on its design and implementation is essential. We can be confident on the functionality of a system based on evidence. Evidence depends on its past usage, performance and level of satisfaction. However; it can never be absolute. Trust is evaluated in context. Based on context or functionality, it can vary within the system.

Even though evidence can generate confidence on trustworthiness, however, the conditions and context of its evaluation is different than that of trustworthiness. So; to justify the trust on the system, only dynamic confirmation is relied upon.

To evaluate trust, evidences that are related to the current context, must be taken into account.

In what follows, we have listed the benefits which justify the use of Trusted Platform Module in securing the CPS [25]:

- CPS uses cloned signatures or session keys to make sure that the sensors and the actuators communicating with them are authentic. So; there is no margin for unauthorized access.
- Sensors collect the data at lower level, and intermediary nodes pass them to the upper level. While transmitting all of the CPS's nodes hold sensitive data. To make sure that the data is safe or protected, we can make use of TPM to encrypt it.
- When a replacement to an existing sensor or actuator is needed, then it has to be peripherally attested first which can be achieved by installing a TPM to the replacement device. Once it asks for a random key, the replacement device has to sign a random number and authenticate.
- CPS has to undergo periodic software and firmware updates. To verify the authenticity of these updates, TPM can be used.

Along with the above mentioned advantages, TPM also supports soft cryptography for encrypting data which is a key feature that makes its stand unique.

We discussed about the advantages of TPM. However; there is still scope for furthermore research. Especially pre-deployment of trusted keys, multilayer security mechanism, incorporating principle of least privileges and redundancy, and managing root and chain of trust in CPS are a few of the issues which does not make Trust computing an ideal choice for the security of CPSs at present. In the following section, we have emphasized the issues with the assumption of pre-deployment of keys to establish trust, which are as such [26]:

- For the key to be pre-deployed at the manufacturing center itself, the whole communication channel has to be trusted from the manufacturing center to the host itself [27].
- For the key has to be deployed by the host itself, important decisions will have to be made about the key which might result in poor quality of the generated keys.
- If the keys are pre-deployed, it would be hard to move or add the keys within the network especially resulting in all keys or nodes being updated within the network. Even removal of a compromised key would be difficult.

Though there are some solutions like message-in-a-bottle approach [27] to manage these problems and many more, they still require some side channels like Faraday's cage or something else to pass the key which makes them unsuitable and unsafe to use them for mission-critical cyber-physical systems.

Modeling and verifying intelligent automotive cyber-physical systems

The authors proposed the use of Machine learning techniques to collect time series data from the sensors of automobile cyber physical systems to record human reaction and behavior. Their proposed approach uses extensive cognitive psychology concepts to design a learning model of conditional probability distributions to maximize expectation and learn the parameters without adding complexity. Along with the theories in psychology, the authors also relied on low abstract learning skills like route selection or steering control to be incorporated [28]. They also developed an algorithm to minimize the overhead by using intelligent automotive cyber physical systems [29,30]. They analyzed the models of the cyber physical systems by proving the correctness of low dimensional abstractions in the linear hybrid automata, which is then used to verify the overall high. They proposed to distribute the verification of low dimensional abstractions as a solution.

Although the model works fine for the automotive intelligent systems, but the time series data have to be available at all times to carry out the proposal. Also, for physiological sensors defining the length for the passkey between the sender and receiver beforehand, though reduces complexity, however increases threats to the security. So, it poses the same threat of exposing the uniform randomness of the passkey to let the hacker be able to reconstruct the appropriate code, just like in the case of chaff points randomized over uniform data in the Fuzzy logic.

Fuzzy extractors

Other approach works with fuzzy Extractors, which rely on reproducing cryptographic keys precisely as well as distributing them in a uniform fashion. Using fuzzy extractors to obtain uniform randomness from the input is nearly optimal till the change in input remains close to the original input. To utilize this feature, the fuzzy vault incorporates error-tolerance in practice. When the user provides an input, the extractor pulls some random string from the input, however in a way that it remains noise-tolerant, which means that in the case where another input close, but not the same as the previous input is provided, still the extractor is able to reproduce the string from it. This random string is inverted into a key; however, it is not needed to store this key in the server. It is important to have this feature as it is highly insecure for a key to be stored in a server's long-term storage that is publicly stored.

Secure Sketch can also be used as a tool in fuzzy extractor as well as an independent cryptography construct to reproduce cryptographic keys. Using the secure sketch, it is possible to precisely reconstruct a noisy input. Given an input, a sketch is produced. Then, it is possible to retrieve the input, given another input close to the first one and instead of storing the actual input, only secure sketch is stored to preserve privacy of the input. Advantages also include confidentiality and entropy retention without compromising privacy, however non-uniformity is not addressed.

Therefore, both secure sketches and fuzzy extractors basically provided a fuzzy storage for the cryptographic key such that the actual key is not compromised due to privacy breach [31].

Fuzzy vault

Fuzzy vault was first proposed by Ari Juels and Madhu Sudan in 2002. Fuzzy vault operates in a way to generate a key that is well hidden in the domain of its chaff points. Using a fuzzy vault, a user is able to hide a secret key in an unordered sample. Then a polynomial is chosen to encode the key as well as to evaluate the polynomial on all elements in the sample. The user then has to manually select random chaff points which do not lie on the polynomial. These chaff points, together with the real points construct the secure vault. Usually, the more the number of chaff points, the merrier for the concealing of the genuine key. The degree of the encoding polynomial determines the error-tolerance of the system. To retrieve the key, the user needs to provide a second sample. When the second sample overlaps with the first one, then numerous points in the vault can be identified and when enough points are identified, then an error correction scheme can be utilized to decode the key. If the samples do not overlap with each other in terms of the points, then the fuzzy vault fails to authenticate, however it's not an issue if the samples do not match due to the incorporation of its randomness through its chaff points [32].

Nonetheless; it is still an unsafe choice due to its leaking of vast amount of data regarding the analog of its randomness, almost similar to the secure sketches in case of fuzzy extractors. Though the attacker has to search for valid options of the randomness incurred, it still lacks in a strong definition of the cryptographic object. Also; the storage and computation costs are exponentially high, especially when it comes a large dataset as well as fuzzy vaults without chaff points are discarded. Entropy loss is high and error tolerance only works in case of small Hamming Metric, which calls for better techniques in encoding as well as signal processing [31].

Proposed Approach

In this section, a solution is proposed to make better use of security protocols in two different domains. The first is to establish secure communication within a Body Area Network (BAN) on Pervasive Health Monitoring Systems (PHMS) [33], whereas the second is to develop a proactive access control model to manage a smart infrastructure during emergencies.

Body Area Network constitutes of small-scale sensors that gather the host's vitals, evaluate movements and properties, and send to the base station wirelessly. Body properties usually consist of location, pulse and body temperature. It's usually coupled with PHMS due to its properties in combining remote monitoring with ubiquitous computing. PHMS collects the data gathered by the sensors of BAN and performs real-time health monitoring for mobile patients [34].

These two domains are chosen frequently as they are good representation of CPS because of their environment coupled nature, and they present two variations for CPSs, BAN showing complete physical security, whereas smart-infrastructures demonstrating physical security to a minimum. For the system to be both secure communication and proactive in handling emergency situations, a modified context-aware security framework is proposed which not only takes into account, the context for the subject that requests the access, but the context of the whole system to determine what privileges to be deployed to which set of subjects and for how long depending on the specific kind of environment. To make the communication of privileges for a fixed duration between these nodes secure, we propose using an already established key agreement technique known as Physiological Signal-based Key Agreement (PSKA) [35], but using the exact cover techniques to generate the random key.

PHMS is used to monitor and collect real-time health data of a patient with the help of medical sensors worn by the host or patient. The Body Area Network (BAN) of sensors gather this data and transfer to the system. The sensors can be deployed in the presence of doctors or by the hosts themselves. As PHMS is becoming popular day by day, even by people with no chronic ailments, for example fitness monitoring, there is need for the use more interoperable sensors. The real overhead for secure communication is key distribution for which there is an urgent need for the development of key agreement technique to preserve the usability. However; this is just one side of the coin. The other side, in this regard to consider, is the response of PHMS in case of the smart-infrastructures or emergencies. Smart-infrastructures are used to provide real-time data to relief workers in order to save lives and property. As the data is sensitive, there is an urn to make the communication more secure from a malicious attack. To achieve this, of course access control techniques are used. However; during emergencies, these access controls are disabled to facilitate emergency management. However; this can be a grave issue as anyone can initiate an emergency to get unlimited access to sensitive info on patient data. So, there is also a need to address this issue by developing an access control model which not only controls access in normal situations, but also adapts its behavior to manage critical situations dynamically.

To overcome security issues related with BANs, an established key agreement solution is presented which is called Physiological Signal-based Key Agreement (PSKA) [35]. It utilizes specific physiological signals as a common key for sensors to enable security. Physiological signals are nothing but stimuli generated by different functions of the human body itself. Examples include the EKG, heart rate etc. Basically; both the communicating sensors specifically agree on one physiological signal, extract features from the signal and convert the features into a set of binary strings, generates a random key, then the sender node concatenates a message authentication code (MAC) to encrypt the data, then hides the key in the previously generated binary string of the physiological signal and sends both the key and data in a single message. The receiver node on the other end, receives the key utilizing a local version of the physiological signal, and checks it by decrypting the data received [36]. If the random key and MAC in both the sender and receiver are matched, then it is accepted, else rejected. Once, the steps are done, there is no need for explicit measurement of physiological signals to establish a secure communication unless the sensors are being reconfigured. It achieves security based on the random key generated by the unique physiological signal at a unique time. A malicious entity who is not in contact with the host will never be able to accurately measure the physiological signal as physiological signals are unique at unique time, so preserving security. This property of physiological signals is known as Time-Variance.

To choose this physiological signal, it has a certain criterion. To be able to get selected for generating the key, the signal has to be long and random, it should be captured in minimal time, it should be distinct and it should possess temporal variance i.e., even if an adversary is able to figure out the physiological signal at present somehow, still future executions of the scheme should not be compromised due to uniqueness of the signal at a time. However; as physiological signals are time-variant and vary unpredictably, so the system needs to ensure that two signals are seeing the same copy of the signal and proper synchronization between sensors needs to be figured out which in case of PSKA is 8mS according to [37]. Though it sounds similar to that of the biometric systems, however, the last feature i.e., Temporal Variance is the property that differentiates a PSKA from the biometric systems as biometric systems depend on not possessing the temporal variance [32].

To generate this key for PSKA, we propose the use of a set cover technique known as the Exact Cover Problem replacing the fuzzy vault in the form of a cryptographic construct [38]. The primary reason behind selecting exact cover techniques to replace fuzzy vault is its flexibility in choosing a length of the set randomly. Also, the combinations in the set to make the cryptographic key is not confined to the scope of the polynomial through the whole time. As soon as a different polynomial is chosen, the combinations can be rearranged accordingly, making the maximum number of such possible combinations to be 2n for length of the set n, below is how the whole process works in terms of an Exact Cover technique.

First; the sender and the receiver sample the physiological signal in current time and make use of the Exact Cover Problem to generate a random set of strings i.e., the polynomial. Given a set of values {1, 2, 3, ….., n} using the concept of natural language processing covering all languages known in the whole world, this scheme first determines the length of the string, which is to be shared by both the sender and the receiver node, and its common factors. Out of all the common factors, two factors are chosen, whose product constitute the length of the set. Out of those two factors, one factor gives the length of the subset and the other factor gives the number of subsets. The polynomial and its order or the number of polynomials are chosen, such that the product of the value of the polynomial and its order, or the order sum of the number of polynomials plus 1, always lie on the factors of the length of the set. However, while choosing the order, we also have to keep in mind that the higher the order, lower will be the chances of exposing the common features. Then the scheme generates a family of subsets in the multiples of nCk, where "k" is the length of the subsets. Among these subsets, the sender finds a subfamily whose union is the set itself such that all the sets in the cover are disjoint which constructs the exact cover with a sum of 2k−1 to be reduced to the subset sum problem to lock the key. Out of all exact covers discovered, the subsets that fulfils the exact cover principle as well as fall on the polynomial, are chosen. Apart from the exact cover, the family also consists of chaff points which are random subsets of the given set, which we are going to use so that the adversary won't be able to figure out the cover the key is constructed upon. Once the subsets are drawn, we will turn these sets into bitmaps of length n where "n" is the length of the set, then interpret these bitmaps to be binary numbers, then find out the disjoint subsets that construct the polynomial, with a sum of 2k – 1, to generate the random key with an exact cover. To unlock this key sent be the sender node, the receiver node constructs the exact cover for the same set and matches it with the set received from the sender node. As the key is pre-agreed between the sender and the receiver node, so the receiver should be able to figure out which are the actual subsets used for locking and which are the chaff point, which in case of the adversary, will be impossible to find out, especially within the given time-frame; as the key will constantly be modified. The chaff points will be used to confuse the adversary to hide the legitimate subsets and the actual set. In a way; it will almost be an almost impossible task for the adversary to reconstruct the polynomial to figure out the key. Once the key is matched, the receiver node can use the Message Authentication Code (MAC) received from the sender to decrypt the data received.

In order to facilitate the solution to manage the problems associated with the smart-infrastructures, we propose an access control model called Modified Context-Aware Security Framework (MCASF) which utilizes the features for emergencies, but with better security mechanisms. The goal of this model is to provide a proactive access control model to address emergency situations, to provide the set of privileges needed by specific subject in a specific situation for a specific amount of time. This awareness will be different from the context-awareness we encountered earlier. Context-awareness decides whether access should be granted to the subject making the access request, by taking into account the contextual information about the subject itself, whereas modified context-awareness will take into account the contextual information about the whole system. If permitted, then access will be granted without any explicit request for access by the subject. For this, it needs to be both adaptive to facilitate the response actions for the known criticalities and proactive in determining when to execute those actions without any explicit access request by the subject. One might ask how it will be any different than the Critically-Aware Access Control [39].

The Modified Context-Aware Security Framework (MCASF) will not just take the Context of the system and its subject into account, but also the physical interaction of the system with its environment such that not only for the smart-infrastructures, but also for establishing secure communication in case of a Body Area Network (BAN), we will be able to use one set of framework known as the Modified Context-Aware Security Framework. Through its interaction with the physical environment, it will be able to find out the demand of the situation and accordingly deploy the normal or special circumstances features to the system. The privileges will be embedded to the system to follow the two sets of protocols. So, basically it will contain different sets of privileges, one that is provided to subjects under normal situations and many alternate sets of privileges that is provided to subject in case of special circumstances to enable them to handle the urgency. These urgencies will again get subdivided into subcategories based on the type of urgency. The different types of urgencies we are considering in this research will be as follows:

- Urgency Level I: This urgency level will define life-threatening urgencies and notify the relief workers accordingly to prioritize the tasks. The set of privileges will be defined accordingly for the assigned duration to the assigned subjects.
- Urgency Level II: This level will define the level of overload faced by tasks as the next level of urgency and reassign them in the to-do list of relief workers as their next priority. The set of privileges will be defined accordingly for the assigned duration to the assigned subjects.
- Urgency Level III: This urgency level will define the critical tasks that were not able to be executed in proper time due to the faced overload by the system at busy hours. The tasks will be reassigned to appropriate authorities and right set of privileges will be assigned to right set of subjects for a given duration.

So; the initial task for the framework will be to figure out the gravity of the situation using the ductility matrix or flow network and notify the system to release appropriate sets of privileges. If it falls under the category of normal situations, the system will use the key agreement technique generated by the Exact Cover Method to generate the key and communicate the data using the Message Authentication Code (MAC). If the urgent or emergency situation is flagged, then the system will perform system ductility to determine the level of urgency and appropriate set of privileges along with the data will be passed to appropriate subjects with a different set of keys generated through the same technique for a fixed duration. The difference in managing a normal situation and an urgent situation will be that during the whole duration of the emergency situation, the key agreement will be modified such that the keys remains unchanged till the situation is handled or under control. However; in enabling subject for managing urgency, it will not provide them the alternate privileges forever as in case of traditional access control models, rather it will enable the response actions in four phases. Once it identifies gravity of the situation.

- First; it will identify the actions and subjects needed and for how long.

- Then it will enable the appropriate actions by appropriate privileges.
- It will notify the subjects of their responsibilities.
- Finally; once the situation is handled, it will rescind the privileges assigned to the subjects later.

For better clarity in how the system works, we will consider an example as below:

A Case Study: Security of Pacemaker

This section provides a simple case study to show the practicality of our proposed approach. To this end, we have provided an activity diagram as shown in Figure 1 to facilitate the process by which we implement our approach.

The pacemaker would consist of two basic set of components: Sensors and the base station. The patient data will be collected through the sensors and passed over to the base station. There are two types of sensors that will be used in this case. The physiological sensors will collect the physiological data whereas the contextual information such as temperature will be collected by the environmental sensors. The physiological data doesn't have to be collected at a specific rate rather different rates depending on type of sensors and the requirement. However; the environmental data has to be collected frequently to analyze the environmental factors such as temperature, light etc. which can have impact on patient conditions. The base station will maintain a database for storing these data and can be developed using JAVA or C#, depending on convenience. Sensors will follow a two-tier client-server architecture comprising of the collection of data, and the passing over of data to its appropriate destination. A specific topology can be used depending on the number of sensors. The collected data from the sensors will then be passed over to the data storage for storing purposes. Along with storage, the highest tier will also be responsible for detailed analysis and data retrieval. We will choose Oracle or SQL Server for the following scenario.

The base station will be connected to a physical device such as a smartphone to monitor the data on the patient and to allow the patient to move around. The entities responsible for monitoring the activities will be able to do so by querying the central server. The data will pass between the base station and the central served using an IP based network in XML format to maintain platform independence. No specific technology has to be mandated for the collection and communication of patient information, so long as the required functionalities are met.

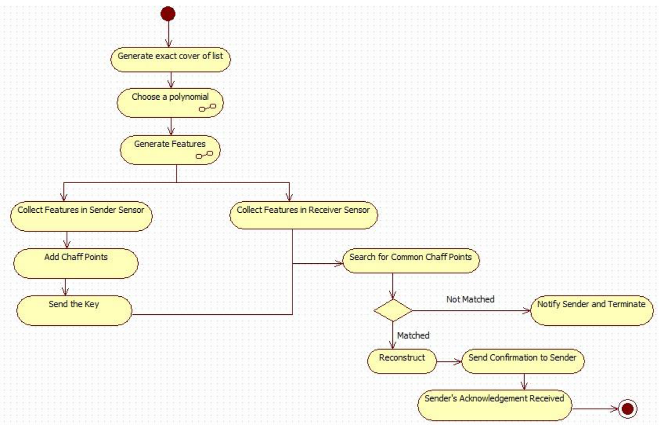
Generate exact cover of list
Choose a polynomial
Generate Features
Collect Features in Sender Sensor
Collect Features in Receiver Sensor
Add Chaff Points
Send the Key
Search for Common Chaff Points
Not Matched
Notify Sender and Terminate
Matched
Reconstruct
Send Confirmation to Sender
Sender's Acknowledgement Received

Figure 1: Activity diagram for pacemaker.

Central server will handle multiple ports so that specific ports can be assigned specific entities to query the server at the same time to access current as well as the past data about a patient. Threshold values can also be set for each data received by an entity to trigger an alarm in case of failure.

A pacemaker would work with the proposed system comprised of medical sensors. The sensors will need to monitor and send the data to the base station wirelessly.

They first will exchange some list for the physiological signals measured by the base station to set the measurement for the cryptographic key. The base station will be interfaced to the smartphone to execute the key agreement. To understand the case study better, we will go through a short example.

Suppose the list shared between the sender and the receiver is S = {1,2,3,4,5,6,7,8,9} where n=9 i.e., the length of the set. As shown in Figure 1, the first step will be to generate the exact cover of the list that is all possible combinations that are disjoint and when combined, form the list. For example, in this case, the combinatory subsets can be {(1,3,5), (2,4,8), (6,7,9)}, {(1,2,3), (4,6,8), (5,7,9)}, {(1,4,7), (2,5,8), (3,6,9)} etc. The length is 9 and the factors for length will be 1,3,9.

To select one factor to be considered, the next step in the Figure 1 is to use a random number generator to choose the polynomial instead of determining the length of the key manually as mentioned in using automotive intelligent systems [28]. The sender selects the order of the polynomial(s) or the number of polynomials to be used depending on the factors of length by executing the random number generator algorithm mentioned before.

Populate all the factors into an array.

- Assign the value generated by the new random number generator function Rand () to a new variable.
- Display the new variable.

Out of the three factors, suppose 3 has been chosen to create the first order polynomials such as f(x) = x+3 and f(y) = y+3. Then, product of the value of the polynomial i.e., 3 and its order sum 2 plus 1 constitute to be 9, which is one of the factors of the length of the set as per our approach. So the subsets will be of order (x, y=f(x), z=f(y)), then in the next phase as per the activity diagram, it will generate a family of subsets of nCk, where "k" is the length of the subsets and determine a subfamily of the subsets i.e., the features for the physiological signal using the exact cover techniques with a sum of 2k – 1, which will be as below:

$$y = f(x) = x + 3,\ z = f(y) = y+3$$

So the features will be in the format (x, y, z). Now, the subfamily of subsets according to the polynomial given will be T = {(1,4,7), (2,5,8), (3,6,9)}.

The steps used to generate these sets are given below:

- We turned the sets into bitmaps of length |S|
- Interpreted the bitmaps to be binary numbers as mentioned in Table 1.

As shown in Table 1, each of the features is first turned into a bitmap of 9-bits length. In this case, the set is 9, so in all positions mentioned in

Features	9 - bits	Binary Numbers
(1,4,7)	001001001	$2^0+2^3+2^6=73$
(2,5,8)	010010010	$2^1+2^4+2^7=146$
(3,6,9)	100100100	$2^2+2^5+2^8=292$

Table 1: Interpreted the bitmaps to be binary numbers.

a subset, 0 is replaced by 1. Next, bitmaps are converted to binary form to provide the number.

The total of all the binary values is 73+146+292 = 511 which is 29-1 compose of disjoint sets confirming to the exact cover requirements.

When the key is reconstructed based on successful matching of chaff points, then it performs the PSKA and a common key is agreed upon for a specific time period in a range depending upon the type of sensors used which will significantly improve the confidentiality for a given set of sensors in the pacemaker, in a sense to make accomplishment without outside intrusion and privacy violation. After the features are generated based on the polynomial, it is collected by both the sender and receiver node as shown in Figure 1. In the next step, chaff numbers will be added to randomize uniformness on the key as shown below:

Key, K = T + {(1,2,3}, (1,4,5), (3,4), (3,4,5,6), (2,6,8)}

= {(1,4,7), (1,2,3), (2,5,8), (1,4,5), (3,4), (3,6,9), (3,4,5,6), (2,6,8)}

Then the sender node sends this key combined with the chaff points and shares the features with the receiver.

A shown in Figure 1, when the key K = {(1,4,7), (3,4), (2,6,8), (3,6,9)} is send, then the receiver will search for the common chaff points added by the sender node, reconstruct the key, and is be able to match the two points (1,4,7) and (3,6,9) with the sender node. Once the key is reconstructed, the confirmation is sent back to the sender and an acknowledgement is received, which establishes the key until the next iteration. However, when the chaff points do not match, then the whole process gets terminated, and the sender sensor receives notification of unauthorized attempt in key establishment.

As soon as the key gets established, the data communication starts in a secure manner. These data will be collected by the base station and will be communicated to the server through secure internet channels, where it will be added to the electronic records pertaining to that patient.

Only the medical professional assigned to that patients will be able to receive input on patient condition or receive the alarm generated, for which the parameters are set by the professionals or attendants beforehand. The example parameter selection is given below:

Generate alarm if any of the following situation arises:

- The blood pressure is more than 140 over 90.
- The blood pressure is less than 120 over 80.
- Heart beat is less than 60 a minute.
- Heart beat is over 100 beats a minute.

To add them as authorized persons, we will use their EMPL IDs and create a sign on using session control as below:

- We will create a hash from the session start combined with the professional's EMPL ID and store it in the data storage on the first request.
- Every time the same user is notified, the hash will be cross verified with the stored hash.

Provided they are authorized to receive it in case of an emergency, they will be able to assist in sending an emergency team or some other emergency solutions.

The emergency team will receive authorization through permission and the session will be generated using the same algorithm as used for medical professionals, and once there is an emergency, the system will integrate its MCASF to enable the emergency team to connect to the server and, query and access the patient's current and past data till the time the patient reaches the facility after which the assigned medical professional takes charge. As soon as the charge is handed over, the session will get destroyed by using session destroy () function.

So, the complexity will be pretty high due to dependency of polynomial on the factors and the dependency of the factors on the length of the set. As the length of the set determines the number of factors to be generated, so the complexity of m is nk for some fixed k, where n is the length of the set and m is the largest value in the set. So the time complexity of the exact cover will be O (n.nm) i.e., O(n2m) [38], however in our case, as m is 2n due to generation of all the features irrespective of length to be fixed, so the complexity will exponential in n(O(n22n) [38], which can be called as pseudo-polynomial time.

Even though the complexity is high i.e., O (n2m) where n is the size of the set and m is the largest value, the integration works smoothly due to the fixed set of physiological signals as a threshold at both the sender and receiver node simultaneously, so in case of an emergency, the agreed key between the sender and receiver takes precedence in order to halt the subset matching.

Conclusion and Future Work

Cyber-physical systems need some additional level of security because of the involvement of the physical domain. The security solutions that have been discussed mostly prompt the user to use Traditional IT Security Solutions in providing security for CPS. Though these can be applied to the security of CPS, there still is need to look at the key difference between an Information System and a CPS before designing a security mechanism specifically for the CPS. Whether Context-Aware Security Framework or Trusted Computing in CPS, both have their advantages, however there are still other security protocols and multilayer security mechanisms that need to be addressed. That's why we proposed a security solution which will use the exact cover problem technique to generate a random key from the physiological signal received from the host and embed this key agreement technique to construct a modified context-aware security framework to manage access control which will make it absolutely hard for a malicious entity to manipulate the system as the key will be constantly modified and erase the traces any past or future instance so that even if the key is compromised at a given instant, the past or future instances are safe from the adversary. However; our proposed techniques still do not take into consideration how to protect the system from the Denial of Service (DoS) attack, which is a direct hit on the properties of availability, nor does it address the issue of interoperability in case of a Cyber-Physical Systems, which are still open areas of research which need to be addressed in the future. Also, the approach needs to be put to experimentation and simulation to prove its feasibility and overhead incurred is big. Also; as most of the authentication techniques require to be time-variant in nature, so scalability poses an issue as it does not take the notion of time into account. As the solutions need to be integrated from a number of domains, the complexity is increased. Also, the system becomes non-deterministic as there is no guarantee as in to provide the key at a specific number of tries because the exact cover might need to repeat itself to come up with another set of numbers to match the key generated.

References

1. Kaiyu W, Man KL, Hughes D (2010) Specification, analyzing challenges and approaches for cyber-physical systems (CPS). Engineering Letters.
2. Elinor Mills (2009) Hackers broke into FAA air traffic control system. The Wall Street Journal.
3. Kelly O'Connell (2008) CIA report: Cyber extortionists attacked foreign power grid, disrupting delivery. Internet Business Law Services.
4. Koscher K, Czeskis A, Roesner F, Patel S, Kohno T, et al. (2010) Experimental security analysis of a modern automobile. Proceedings of the 31st IEEE Symposium on Security and Privacy.
5. Fuhrmans V (2010) Virus attacks siemens plant-control systems. The Wall Street Journal.
6. Leavitt N (2010) Researchers fight to keep implanted medical devices safe from hackers. Computer 43: 11-14.
7. Krebs B (2008) Cyber incident blamed for nuclear power plant shutdown. Washington Post.
8. Alvaro AC, Saurabh A, Shankar S (2008) Research challenges for the security of control systems. HOTSEC.
9. Wang EK, Yunming Ye, Xiaofei Xu, Yiu SM, Hui LCK, et al. (2010) Security issues and challenges for cyber physical system. International Conference on Green Computing and Communications, IEEE/ACM International Conference on Cyber, Physical and Social Computing.
10. Shirey R (2000) Internet security glossary. Network Working Group.
11. Han J, Jain A, Luk M, Perrig A (2007) Don't sweat your privacy: Using humidity to detect human presence. International Workshop on Privacy in UbiComp.
12. Matt Bishop (2003) Computer security, art and science. Addison Wesley.
13. Chalkias K, Baldimtsi F, Hristu-Varsakelis D, Stephanides G (2008) Two types of key-compromise impersonation attacks against one-pass key establishment protocols. Communications in Computer and Information Science 23: 227-238.
14. Saltzman R, Sharabani A (2009) Active man in the middle attacks, a security advisory. IBM Rational Application Security Group.
15. Jung-Chun K, Marculescu R (2006) Eavesdropping minimization via transmission power control in ad-hoc wireless networks. 3rd Annual IEEE Communications Society on Sensor and Ad Hoc Communications and Networks.
16. Pelechrinis K, Iliofotou M, Krishnamurthy SV (2011) Denial of service attacks in wireless networks: The case of jammers. IEEE Communications Surveys & Tutorials 13: 245-257.
17. Cardenas AA, Saurabh A, Shankar S (2008) Secure control: Towards survivable cyber-physical systems. Distributed Computing Systems Workshops, ICDCS International Conference.
18. Marburger JH, Kvamme EF (2007) Leadership under challenge: Information technology R&D in a competitive world, an assessment of the federal networking and information technology R&D program. Technical report, President's Council of Advisors on Science and Technology.
19. Schenato L, Sinopoli B, Franceschetti M, Poolla K, Sastry SS (2007) Foundations of control and estimation over lossy networks. Proceedings of the IEEE 95: 163-187.
20. Hepanha JP, Naghshtabrizi P, Xu Y (2007) A survey of recent results in networked control systems. Proceedings of the IEEE 95: 138-162.
21. Blanke M, Kinnaert M, Lunze J, Staroswiecki M (2003) Diagnosis and fault-tolerant control. Springer-Verlag.
22. Olfat-Saber R (2005) Distributed kalman filter with embedded consensus filter. Proceedings of CDC and ECC, Seville, Spain.
23. Feng Gui (2009) Development of a new client-server architecture for context aware mobile computing. PhD Thesis, Florida International University.
24. Fisher DA (2012) Principles of trust for embedded systems. Technical Note CMU/SEI-2012-TN-007.
25. Moholkar AV (2014) Security for cyber-physical systems. International Journal of Computing and Technology 1: 257-262.
26. Venkatasubramanian KK, Banerjee A, Gupta SKS (2010) PSKA: Usable and secure key agreement scheme for body area networks. IEEE Transactions on Information Technology in Biomedicine 14: 60-68.
27. Kuo C, Luk M, Negi R, Perrig A (2007) Message-in-a-bottle: User-friendly and secure key deployment for sensor nodes. Proceedings of the ACM Conference on Embedded Networked Sensor System (SenSys 2007).
28. Jha SK, Sukthankar G (2011) Modeling and verifying intelligent automotive cyber-physical systems. EECS Department, University of Central Florida, Orlando, USA.
29. Jha SK, Langmead CJ, Ramesh S, Mohalik S (2010) When to stop verification? Statistical trade-off between cost of simulation and possible loss from erroneous designs. IEEE CS.
30. Jha SK (2008) d-IRA: A distributed reachability algorithm for analysis of linear hybrid automata. International Conference on Hybrid Systems Computation and Control, pp: 618-621.
31. Gupta SKS, Mukherjee T, Venkatasubramanian KK (2006) Criticality aware access control model for pervasive applications. Proceedings of the 4th IEEE Conference on Pervasive Computing.
32. Venkatasubramanian KK, Gupta SKS (2006) Security for pervasive health monitoring sensor applications. Proceedings of the 4th International Conference on Intelligent Sensing and Information Processing.
33. Banerjee A, Venkatasubramanian KK, Mukherjee T, Gupta SKS (2012) Ensuring safety, security, and sustainability of mission-critical cyber–physical systems. Proceedings of the IEEE 100: 283-299.
34. Kumbhare YL, Rangaree PH (2015) Patient health monitoring using wireless body area sensor network. International Journal of Engineering and Advanced Technology (IJEAT).
35. Cherukuri S, Venkatasubramanian KK, Gupta SKS (2003) BioSec: A biometric based approach for securing communication in wireless networks of biosensors implanted in the human body. Proceedings of Wireless Security and Privacy Workshop pages, pp: 432-439.
36. Venkatasubramanian KK, Gupta SKS (2010) Physiological value based efficient usable security solutions for body sensor networks. ACM Transactions on Sensor Networks.
37. Elson J, Girod L, Estrin D (2002) Fine-grained network time synchronization using reference broadcasts. Proceedings of the 5th symposium on Operating systems design and implementation 36: 147-163.
38. Papadimitriou CH (2003) Computational complexity. Encyclopedia of Computer Science, pp: 260-265.
39. Dodis Y, Ostrovsky R, Reyzin L, Smith A (2003) Fuzzy extractors: How to generate strong keys from biometrics and other noisy data. Conference Paper in SIAM Journal on Computing 38: 523-540.