A Survey of Specification-based Intrusion Detection Techniques for Cyber-Physical Systems

Livinus Obiora Nweke
Department of Information Security and Communication Technology,
Norwegain University of Science and Technology (NTNU),
Gjøvik, Norway

***Abstract*—Cyber-physical systems (CPS) integrate computation and communication capabilities to monitor and control physical systems. Even though this integration improves the performance of the overall system and facilitates the application of CPS in several domains, it also introduces security challenges. Over the years, intrusion detection systems (IDS) have been deployed as one of the security controls for addressing these security challenges. Traditionally, there are three main approaches to IDS, namely: anomaly detection, misuse detection and specification-based detection. However, due to the unique attributes of CPS, the traditional IDS need to be modified or completely replaced before it can be deployed for CPS. In this paper, we present a survey of specification-based intrusion detection techniques for CPS. We classify the existing specification-based intrusion detection techniques in the literature according to the following attributes: specification source, specification extraction, specification modelling, detection mechanism, detector placement and validation strategy. We also discuss the details of each attribute and describe our observations, concerns and future research directions. We argue that reducing the efforts and time needed to extract the system specification of specification-based intrusion detection techniques for CPS and verifying the correctness of the extracted system specification are open issues that must be addressed in the future.**

***Keywords*—Cyber-physical systems; intrusion detection systems; specification-based intrusion detection mechanism; security**

I. Introduction

The recent years have witnessed an increasing growth in the development and deployment of different types of cyber-physical systems (CPS). CPS have shaped every aspect of our lives as their applications span through several domains including electrical power grids, water and wastewater management, oil and gas sector, traffic systems and many other domains. Considering the nature of CPS, security incidents could lead to physical harm to people, destruction of property or environmental disasters. For this reason, the secured operation of CPS is a major concern for all stakeholders.

According to Gartner analysts [1], CPS security incidents are expected to rise in the coming years due to a lack of security focus and spending that are aligned to CPS. They also observe that the liability for CPS security incidents will not only affect the corporate entity but will also lead to a personal liability for 75% of CEOs by 2024. This is a wakeup call for all those charged with the responsibility for the secured operation of CPS and for greater attention to the development and deployment of appropriate security controls for CPS.

One of the security controls for CPS involves the use of intrusion detection systems (IDS). Traditionally, there are three main approaches to IDS, namely: anomaly detection, misuse detection and specification-based detection. However, due to the unique attributes of CPS, the traditional IDS need to be modified or completely replaced before it can be deployed for CPS. A discussion of the techniques and challenges on the use of IDS in CPS have been provided by Han et al. in [2] . Our interest in this paper is to survey the use of specification-based intrusion detection techniques for CPS.

Some works in the literature have conducted surveys related to the use of IDS for CPS [3], [4], [5]. Mitchell and Chen [3] presents a survey of IDS design principles and techniques for CPS. They categorize the existing CPS IDS techniques in the literature, describe their advantages and disadvantages and suggest future research areas. Zarpelão et al. [4] also conducted a survey of IDS in Internet of Things (IoT). They classify the IDS proposed in the literature according to the following attributes: detection method, IDS placement strategy, security threat and validation strategy. A much recent survey related to the use of IDS for CPS is presented by Wu et al. [5]. They conducted a survey of the proposed IDS designs for in-vehicle networks. However, to the best of our knowledge, none of the existing surveys have considered the use of specification-based IDS for CPS.

In this paper, we present a survey of specification-based intrusion detection techniques for CPS. In particular, we classify the existing specification-based intrusion detection techniques in the literature according to the following attributes: specification source, specification extraction, specification modelling, detection mechanism, detector placement and validation strategy. We also discuss the details of each attribute and describe our observations, concerns and future research directions. We argue that reducing the efforts and time needed to extract system specification of specification-based intrusion techniques for CPS and verifying the correctness of the extracted specification are open issues that must be addressed in the future.

The rest of this paper is organised as follows. Section II presents a discussion on CPS and specification-based intrusion detection, which provides an understanding for describing the suitability of specification-based intrusion detection techniques for CPS. Section III provides a survey of specification-based intrusion detection techniques for CPS and the proposed taxonomy. Section IV describes our observations, concerns and future research directions, which is one of the most relevant

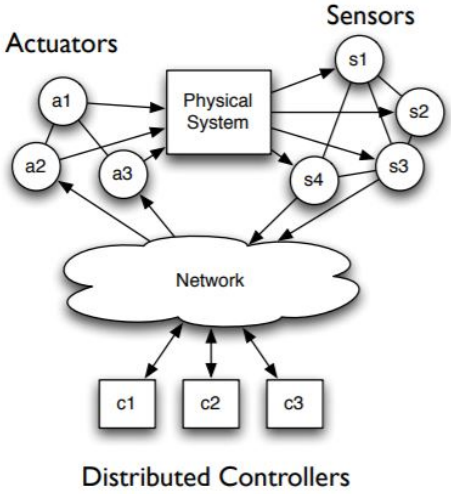
contributions of this work. Section V concludes the paper.

II. Background

A. Cyber-Physical Systems

CPS facilitate the integration of computation and communication capabilities to monitor and control physical systems. This enables the accomplishment of time-sensitive functions with different degrees of interaction with the environment, including human interaction [6]. As a result of this, CPS are called time-sensitive systems which makes timing a central theme in their design and implementation. CPS are also referred to as safety-critical systems because the failure of the system due to faults or other external influences, could endanger the lives of humans operating the physical systems, those embedded with the CPS (medical devices) or those within the radius of their operation (nuclear plants). The application of CPS span through several domains and they include modern vehicles, medical devices, industrial systems, etc., all with different standards, requirements, communication technologies, and time constraints.

The general architecture of CPS is depicted in Figure 1. CPS as showed in the diagram, typically have a physical system that is being monitored and controlled, a set of sensors that report the state of the physical system, a set of actuators that are used by the controllers to maintain the system in the desired state, and a set of controllers (or a controller) that monitors and controls the physical system using the sensors and actuators, and via a communication channel [7]. The interaction between these components of CPS is known to be vulnerable to cyber attacks. For example, a power station located north of the city of Kiev, Ukraine, suffered a cyber attack which blacked out a portion of the Ukrainian capital equivalent to a fifth of its total power capacity [8]. This calls for increased efforts towards addressing the security issues of CPS.



[7]

Fig. 1. The General Architecture of CPS.

There are several security challenges in the operation of CPS. These challenges can be attributed to the unique features of CPS which makes the traditional security solutions ineffective in addressing the security challenges of CPS. For example, CPS have time constraints because the physical processes are generally time-aware and deadline sensitive [9]. Also, the complexities in the analysis and design of security solutions for CPS are further exacerbated by the need to understand and address the upstream and downstream dependencies of the component systems [6]. Therefore, the current information technology (IT) security controls would have to be modified significantly or to be completely replaced because they are unable to address the security challenges of CPS.

One of the security solutions for CPS involves the use of intrusion detection systems (IDS). There are three main approaches to IDS, namely: anomaly detection, which relies on comparing current behaviour with the pre-established normal behaviour to detect an intrusion; misuse detection, which use intrusion signatures to detect an intrusion; and specification-based detection, which depends on the monitoring of the specified system behaviour to detect an intrusion [10]. A review of the existing intrusion detection techniques for CPS has been provided by Mitchell and Chen in [3] and Han et al. in [2] discuss the techniques and challenges of intrusion detection in CPS. We are interested in the use of specification-based IDS for CPS in this paper. The following subsections provide an in-depth discussion on specification-based IDS and its suitability for CPS, so as to motivate our survey of the existing specification-based intrusion detection techniques for CPS.

B. Specification-based Intrusion Detection

The notion of specification-based intrusion detection was first introduced by Ko et al. in [10]. It leverages the specification of a system, which describes the expected behaviour of the system. Any deviation of the system operations from the defined correct behaviour is flagged as a security violation. In general, the specification-based intrusion detection process involves the use of a specification source to extract the expected behaviour of a system, which in turn is modelled. A detection mechanism is then applied to the modelled specification for monitoring the system behaviour for any deviation. Figure 2 provides a diagrammatic illustration of the specification-based intrusion detection process.

Specification-based intrusion detection has shown to be a better approach to IDS than anomaly detection and misuse detection [11]. Even though anomaly detection is able to detect novel attacks, it suffers from a high rate of false alarm because unseen legitimate system behaviours are classified as anomalies. Misuse detection, on the other hand, does not generate false alarms but it is unable to detect novel attacks. Hence, specification-based appears to be the mean between misuse detection and anomaly detection because it combines the advantages of both approaches. Its false positive rate is similar to misuse detection as it does not generate false alarms when unusual system behaviours are discovered. Similar to anomaly detection, specification-based intrusion detection is able to detect novel attacks because it detects attacks as deviations from the defined correct system behaviours.

The use of specification-based intrusion detection spans through several domains. Initially, it was intended for execution

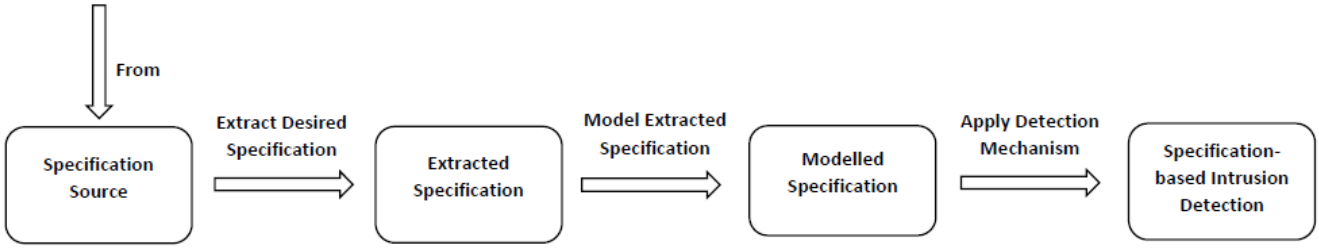


Fig. 2. Specification-based IDS Process.

monitoring of security-critical programs in distributed system [10]. However, it has been applied to routing protocols such AODV [12], [13], [14] or OSLR [15], DNP3 protocol [16], [17], [18] Voice over IP [19], [20], [21] and other areas of CPS as discussed in section III. A practical experience in the use of specification-based intrusion is presented by Uppuluri and Sekar in [11]. In this work, the experiments conducted show that specification-based intrusion detection is able to detect 80% of the attacks without knowledge about the attacks or the attacker behaviour. They observe that the combination of specification-based intrusion detection with some misuse specification increases the detection ability to 100% with 0% false positive rates.

Specification-based intrusion detection can also be combined with anomaly detection. This is the method adopted by Sekar et al. in [22] and Stakhanova et al. in [23]. Sekar et al. [22] use state-machine specification in combination with information about statistics that need to be maintained to detect anomalies. They evaluate effectiveness of the approach is using 1999 Lincoln Labs intrusion detection evaluation data and the results show that the proposed intrusion detection approach detects all of the probing and denial of service attacks with a low rate false alarm. In the case of Stakhanova et al. [23] the proposed technique facilitates the automatic development of the normal and abnormal behaviour specification in a form of variable-length pattern classified using anomaly-based method. They assess the proposed technique via simulations using publicly available synthetic data and the results show that the approach can detect unknown anomalous behaviour and known anomalous behaviour with a low rate false alarm.

C. Suitability of Specification-based Intrusion Detection for Cyber-Physical Systems

There are several characteristics of CPS that makes specification-based intrusion detection the most suitable type of intrusion detection approach for CPS. One of these characteristics is the laws of physics that govern the physical systems in CPS. The IDS deployed in CPS are expected to monitor physical processes for intrusion. These physical processes are governed by the laws of physics, which makes certain behaviours of the physical systems more likely to be seen than others [3]. Thus, specification-based intrusion detection technique can be used to define these behaviours and to monitor the physical systems for any deviation from these expected behaviours.

Another feature of CPS environment is that activities are usually automated and time driven in a closed-loop settings [3]. This provides some regularity and predictability in the CPS environment which can be used for monitoring. It is different from the IT environment where activities are user triggered and users' behaviours can be very unpredictable. Consequently, the regularity and predictability of CPS environment can be exploited by specification-based intrusion detection to define the correct behaviours of the system, which is subsequently used to monitor behaviours outside the defined behaviours.

Moreover, the protocols deployed in CPS are well-known and widely used which makes it easy to extract the correct behaviour of the system. As a result of this, it is attractive to use specification-based intrusion technique for CPS. This is because the protocol specifications which are readily available can be used as specification source to extract the expected behaviour of the system. Also, specification modelling and detection mechanism can then be employed to complete the specification-based intrusion detection process.

III. Specification-based Intrusion Detection Techniques for Cyber-Physical Systems

In this section, we present a survey of specification-based intrusion detection techniques for CPS. We observe that a common feature of the specification-based intrusion detection techniques for CPS is as follows: a set of properties, which indicates the correct system behaviour is sourced, extracted and modelled; and then, a detection mechanism is used to monitor for any deviation from the defined system specification. Using this understanding, we classify the existing literature according to the following attributes: specification source, specification extraction, specification modelling, detection mechanism, detector placement and validation strategy. The proposed taxonomy of specification-based intrusion detection techniques for CPS is depicted in Figure 3 and Table I summarizes the existing works on specification-based intrusion detection techniques for CPS.

A. Specification Source

Specification source refers to how the set of properties that indicates the correct system behaviour is obtained. There are three major specification sources of specification-based intrusion detection techniques for CPS, namely: protocol specification, reference model and observed behaviour.

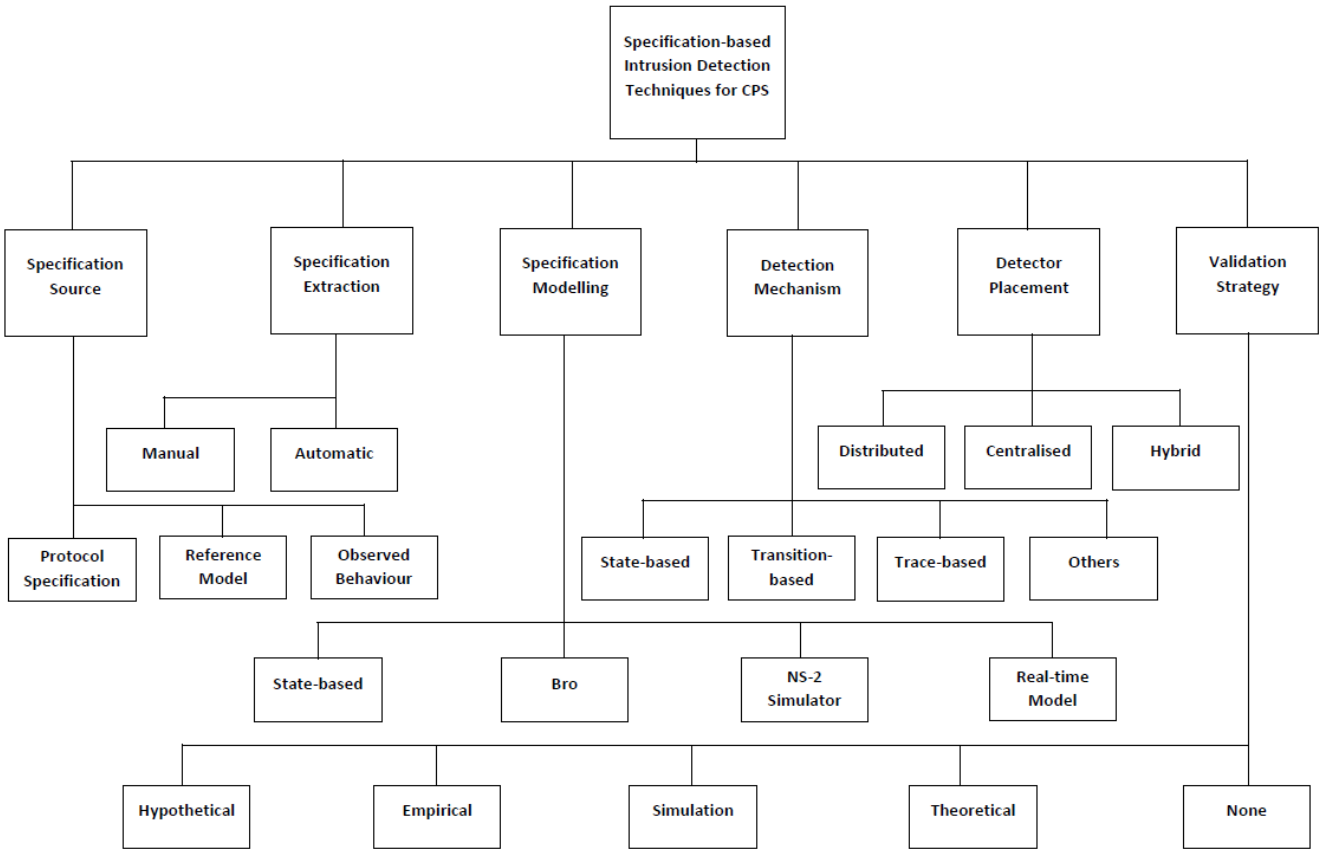


Fig. 3. Taxonomy of Specification-based Intrusion Detection Techniques for CPS.

1) Protocol Specification: Protocol specification is a formal document that defines the expected behaviour of a system. Given the well-defined behaviour of CPS, several protocol specifications have been deployed as the specification source to describe its correct behaviour in many studies. For example, Tseng et al. in [12] utilise the Ad hoc distance Vector (AODV) routing protocol specification as specification source. Other works that have employed AODV routing protocol specification as specification source include Hansson et al. in [13] and Hassan et al. in [14].

Gil et al. in [24] have used IEEE 802.11 protocol and the extensible authentication protocol (EAP) specifications as specification source to define the desired behaviour of wireless local area network. Song et al. in [25] combine both informal protocol specification and other documents from dynamic registration and configuration protocol as specification source. The spanning tree protocol (STP) specification has been leveraged as specification source by Jieke et al. in [26] to describe the expected behaviour for carrier Ethernet network infrastructure. And Tseng et al. in [15] use H.323 protocol specification as specification source.

McParland et al. in [18] deploy protocol guidelines for both ModBus TCP and DNP3 as specification source. They abstract the specific details away of the protocols to focus on the physics models of the system. Unlike them, Lin et al. in [16] and [17] employ only DNP3 as specification source to extract the normal behaviour of the system. Further, Berthier and Sanders in [27] use C12.22 standard protocol specification as specification source to ensure that all violations of the specified security policy of the system will be captured.

The controller area network (CAN) protocol specification has been utilised by Olufowobi et al. in [28] as specification source. Larson et al. in [29] employ the CAN protocol version 2 and the CANOpen application layer draft standard 3.01 as specification source to extract the expected behaviour of electronic control unit of an in-vehicle network. Also, Esquivel-Vargas et al. in [30] exploit the Building Automation and Control Networks (BACnet) protocol as specification source to depict the normal behaviour of each device in the BACnet network.

2) Reference Model: The reference model of the system under consideration has also been employed in several studies as specification source, to obtain the correct system behaviour [31], [32], [33], [34]. Mitchell and Chen in [31] employ the reference model of a modern electrical grid CPS embedding physical components as specification source. They also use the reference model of unmanned air vehicles and reference model of medical CPS in [32] and [33] respectively as specification sources. Also, Sharma et al. in [34] utilize the reference model of unmanned air vehicles CPS as specification source.

3) Observed Behaviour: Observed behaviour of the system under consideration is another method that can be employed as specification source, to define the correct behaviour of a system. It involves the monitoring of a system during its

TABLE I. SUMMARY OF THE EXISTING WORKS ON SPECIFICATION-BASED INTRUSION DETECTION TECHNIQUES FOR CPS

Reference	Specification Source	Specification Extraction	Specification Modelling	Detection Mechanism	Detector Placement	Validation Strategy
[12]	Protocol Specification	Manual	State-based	State-based	Distributed	Hypothetical
[13]	Protocol Specification	Manual	Stated-based	Other Methods	Distributed	Simulation
[14]	Protocol Specification	Manual	NS-2 Simulator	Other Methods	Distributed	Simulation
[15]	Protocol Specification	Manual	State-based	State-based	Distributed	Simulation
[16]	Protocol Specification	Manual	Bro	State-based	Centralised	Simulation
[17]	Protocol Specification	Manual	Bro	State-based	Centralised	Simulation
[18]	Protocol Specification	Manual	Bro	Transition-based	Centralised	Simulation
[24]	Protocol Specification	Manual	State-based	Transition-based	Centralised	Simulation
[25]	Protocol Specification	Manual	State-based	Trace-based	Centralised	Theoretical
[26]	Protocol Specification	Manual	State-based	Other Methods	Distributed	None
[27]	Protocol Specification	Manual	State-based	State-based	Centralised	Empirical
[28]	Protocol Specification	Automatic	Real-time model	Trace-based	Centralised	Simulation
[29]	Protocol Specification	Manual	Not Specified	Other Methods	Hybrid	Hypothetical
[30]	Protocol Specification	Automatic	Bro	Not Specified	Centralised	Simulation
[31]	Reference Model	Manual	State-based	State-based	Distributed	Simulation
[32]	Reference Model	Manual	State-based	State-based	Distributed	Simulation
[33]	Reference Model	Manual	State-based	State-based	Distributed	Simulation
[34]	Reference Model	Automatic	State-based	State-based	Distributed	Simulation
[35]	Observed Behaviour	Manual	State-based	Transition-based	Centralised	Simulation
[36]	Observed behaviour	Manual	ISML	State-based	Centralised	Simulation

normal operation and then using the knowledge obtained as specification source, to specify the correct behaviour of the system. For example, Pan et al. in [35] use time-synchronized data from synchrophasor and observable events from audit logs as specification source to define the correct behaviour for the cyber-physical environment in electric power system. Also, the specification source utilized by Carcono et al. in [36] is based on monitoring the evolution of the target system states.

B. Specification Extraction

Specification extraction is the method that can be deployed to extract the correct behaviour of the system using the specification source. This can either be accomplished manually or automatically.

1) Manual: Most of the specification extraction methods adopt a manual approach for the extraction of the correct system behaviour from the specification source [18], [27], [16], [12], [17], [24], [25], [26], [13], [14], [15], [35], [36], [33], [32], [31]. This method has been shown to be an expensive and very tedious process [27]. As a result of this limitation, there have been attempts in the past few years towards the automatic extraction of the correct system behaviour from specification sources.

2) Automatic: Efforts have been made in recent years to extract the correct system behaviour from the specification source automatically [30], [34], [28]. Esquivel-Vargas et al. in [30] made the first attempt to extract specification automatically. In this work, they implement automated specification extraction in two steps: a subset of the devices capabilities is observed in the network traffic; and based on this observation, an algorithm is used to extract all the devices capabilities from the specification source. Automated specification extraction has also been employed by Sharma et al. in [34] to derive the behaviour rules of IoT device using the operational profile as specification source. And most recently, Olufowobi et al. in [28] exploit real-time schedulability analysis of messages to automate specification extraction.

C. Specification Modelling

Specification modelling describes the modelling approach that is adopted to model the specification extracted from a specification source, to describe the correct system behaviour. This subsection presents the different methods that are currently being used for specification modelling.

1) Specification Modelling Using State-based Approach: State-based approach is the most common method for specification modelling. There are several variants of the state-based approach currently in use. The standard state machine has been used by Mitchell et al. in [31], [32], [33] for specification modelling where the extracted specification is transformed into state machines. Jeike et al. in [26] employ state machine for specification modelling. In this work, the states of the machine are states of the protocol, and the state transitions are caused by the receptions of BPDUs or expiration of timeouts. Standard state machines have also been deployed by Berthier and Sanders in [27] to capture the expected system behaviour. And Sharma et al. in [34] have converted the extracted specification into state machines for specification modelling.

Another variant of the state-based approach that has been adopted for specification modelling is the finite state machine. Tseng et al. in [12], [15] use finite state machine for specification modelling. They specify the correct AODV routing protocol behaviour using the finite state machine in [12] and describe the valid routing behaviour of a network node based on Optimised Link State Routing (OLSR) protocol in [15]. The extended finite state machine has been applied by Hansson et al. in [13] and by Song et al. in [25] for specification modelling. Gill et al. in [24] utilise state transition model to describe the extracted specification and state transition patterns are employed by Pan et al. in [35] for specification modelling. Also, a sector specific state modelling language referred to as Industrial State Modelling Language (ISML) has been employed in [36] for specification modelling.

2) Specification Modelling Using Bro: Another tool that can be used for specification modelling is the open source Bro network security monitor (now known as Zeek) [37]. McParland et al. in [18] use Bro scripts for specification modelling but the specific details of the communication protocols and technologies are removed to concentrate on the physics models of the devices being investigated. Similarly, the security specifications of DNP3 protocol have been modelled as a parser and integrated into Bro by Lin et al. in [16], [17]. And Esquivel-

Vargas et al. in [30] use Bro for specification modelling of the automatically extracted correct system behaviour.

3) Specification Modelling Using NS-2 Simulator: NS-2 stands for Network Simulator Version 2 and it is an open-source event-driven simulator for modelling the dynamic nature of communication networks [38]. Hassan et al. in [14] employ NS-2 simulator for specification modelling. In this work, the extracted specification for the runtime behaviour of AODV protocol is implemented using the NS-2 simulator, which allows the detection of any violations from the correct system behaviour.

4) Specification Modelling Using Real-time Model: A recent work by Olufowobi et al. in [28] has proposed the use of a real-time model for specification modelling. In this work, CAN traces that describe the normal behaviour of the network is used to extract real-time parameters as the features which represent the desired specification. Then, the real-time model of the CAN is deployed to specify the expected system behaviour and to flag the violations of the model as indications of a compromised network.

D. Detection Mechanism

Detection mechanism refers to the method that can be adopted to ascertain if there is any deviation from the expected system behaviour. Such deviations are flagged as malicious and since it only relies on the defined specification, this approach is able to detect zero-day attacks. We classify the detection mechanism based on the taxonomy suggested in [39] and the recent developments in the field.

1) State-based Detection Mechanism: Most of the detection mechanism deployed by specification-based intrusion detection techniques for CPS are based on states. The desired state of the system is defined using the specification source that have been extracted and modelled. The goal of the detection mechanism is to detect any deviation from the desired state. For example, Tseng et al. in [12], [15] use a finite state machine for detecting incorrect route request and route reply messages of the AODV routing protocol. They employ predefined finite state machine constraints in [12] which are based on the sourced, extracted, and modelled correct specification; any deviation from these constraints are flagged as malicious. And in [15] the detection mechanism involves checking whether the network node violates the constraints based on the finite state machine.

Mitchell et al. have also used state-based method as detection mechanism in [31], [32], [33]. In these works, they transform the behaviour rules into state machines, which are then used to monitor the system for deviations from the specified system behaviour. Similarly, Berthier and Sanders in [27] use a state machine module to keep track of the state of each device for which traffic is capture, to ensure that stateful constraints are not violated. And Sharma et al. in [34] transforms behaviour rules into a C-language state machine labelled with safe and unsafe states; against which normal and malicious behaviours of the IoT device can be statistically described.

The DNP3 analyser used by Lin et al. in [17], [16] as detection mechanism is based on states. They observed that the DNP3 analyser can maintain states from the parsed network packets and using this states, the incoming packets can be corrected and analysed to ensure there are no violations. Also, Carcano et al. in [36] propose the concept of critical state analysis and state proximity as detection mechanism. They argue that the critical states of a CPS are well documented and that by monitoring the evolution of the physical process states and keeping track of when the CPS enter into a critical state, it is possible to detect attack patterns (known or unknown) likely to drive the CPS into a critical state.

2) Transition-based Detection Mechanism: The detection of malicious behaviour can also be accomplished by monitoring the transition between states. McParland et al. in [18] describes operational protocols using pre- and post- conditions of physical state transitions and any transition that does not lead to a good state is flagged as a potential failure or attack on sensors or actuators. The detection mechanism presented by Gill et al. in [24] used as state transition modelling. In this work, the detection mechanism is achieved by monitoring any anomalous transition in the observed state transition model. And temporal-state transitions are used by Pan et al. in [35] as the detection mechanism. The method adopted in this work involves the monitoring of transition from state to state to detect patterns that are likely to interrupt the protection scheme.

3) Trace-based Mechanism: Trace-based method is another detection mechanism that can be used to monitor deviations from the specified system behaviour. For example, Song et al. in [25] define a set of valid network traces that indicates all finite traces of a network accepted by the specification. They then employ these traces as detection mechanism by monitoring for any trace violating the specification. Olufowobi et al. in [28] use CAN traces as detection mechanism. The CAN traces used in this work depict the normal behaviour of the network, and the detection mechanism involves checking to see if the CAN traces conform with the specification.

4) Other Methods: There are other methods that can be used as detection mechanism which is neither state-based, transition-based, nor trace-based. One of such method presented by Jieke and Redol in [26] and Hansson in [13] combines the attributes of state-based method and transition-based method. In this works, the detection mechanism depends not only on the state of the system but also on the transition between states. Another method is the detection mechanism that has been described by Hassan et al. in [14] which involves identifying misuses to routing messages based on the derived specification. Also, Larson et al. in [29] employ a detection mechanism that checks protocol violations by monitoring the ECU object directory for illegal modifications.

E. Detector Placement

In the use of specification-based intrusion detection techniques for CPS, the detector placement strategies can be distributed, centralised, or hybrid (a combination of both the distributed and the centralised detector placement). This type of classification has been used by Zarpelão et al. in [4] to describe the possible placement strategies for intrusion detection systems in Internet of Things. Hence, this subsection presents the three types of detector placement methods that can

be used in specification-based intrusion detection techniques for CPS.

1) Distributed Detector Placement: The use of distributed detector placement is the most desired placement strategy of specification-based intrusion detection for CPS. This is because of the distributed nature of CPS and the need for an IDS which allows every device to be monitored by other devices and ensures there is no single point of failure. For this reason, the use of distributed detector placement in specification-based intrusion detection for CPS has been proposed in [33], [12], [26], [15], [31], [32], [26], [13], [14], [15], [34].

2) Centralised Detector Placement: Centralised detector placement refers to the detector placement where the detector is located at a centralised component, for example, a dedicated host or a network router. This is the strategy employed by most of the survey works [18], [27], [16], [30], [28], [35], [17], [24], [25], [36]. Even though the use of centralised detector placement creates a single point of failure, the ease of its implementation is responsible for its prevalence.

3) Hybrid Detector Placement: Hybrid detector placement is an approach that attempts to combine the benefits of distributed detector placement and centralised detector placement. This approach has been deployed by Larson et al. in [29]. They observe that placing a detector in the network device would make the use of specification-based intrusion detection impossible in CAN environment because it cannot ascertain if the source of the message is allowed to transmit, or if the destination is allowed to receive. As of result of this, they combine distributed detector placement and centralised detector placement to remedy the limitation of centralised detector placement.

F. Validation Strategy

This subsection aims to present the validation strategy that have been employed in the use of specification-based intrusion detection techniques for CPS. Validation is the process of ascertaining if the developed model behaves with acceptable accuracy according to the objectives of the study [40]. To classify the existing validation strategy in the use of specification-based intrusion techniques for CPS, we use the classification of validation methods proposed by Verendel in [41] namely: hypothetical, empirical, simulation, theoretical, and none.

1) Hypothetical: Here, hypothetical examples are used for the validation of the proposed techniques. This is the approach that is adopted by Larson et al. in [29] and Tseng et al. in [12]. Larson et al. [29] use hypothetical example where assumption about the capability of an attacker is made. They apply this to a conceptual network model connecting two networks through a common Gateway to validate their proposed specification-based intrusion detection technique. Similarly, Tseng et al. [12] employ a hypothetical example of how the network monitors trace AODV packets based on the AODV scenario they described to validate their proposed specification-based intrusion detection method.

2) Empirical: Empirical methods have also been used as validation strategy of specification-based intrusion detection for CPS. Berthier and Sanders [27] utilise empirical evaluation and observe that the objectives of such verification are two folds: verifying that the implementation is correct, and measuring the performance of the implementation under various conditions.

3) Simulation: Simulation is the most popular validation strategy used by the existing literature surveyed in this paper [18], [33], [16], [30], [28], [34], [35], [17], [24], [13], [14], [15], [36], [31], [32]. For example, McParland et al. [18] in the validation of their proposed approach use a collection of Modbus master and salve simulation tools and DNP3 simulation tools. Mitchell and Chen in [31], [32], [33] use Monte Carlo simulation for the validation of their proposed techniques. Lin et al. [16] employ a test-bed to simulate SCADA-specific attack scenarios in the bid to validate their proposed method. And Carcano et al. [36] simulated a prototype of the approach they described as validation strategy.

Moreover, the validation strategy using simulation may require the development of a specialised tool. This is the approach adopted by Hansson et al. in [13]. They develop a simulation environment in C++ called Aquarius, which is then deployed for the validation of their proposed technique. Well-known tools have also been deployed as validation strategy. For example, Hassan et al. [14] use NS-2 network simulator, Tseng et al. [15] use GloMoSim simulation platform and Gill et al. [24] use a custom Snort-Wireless preprocessor.

Pan et al. [35] implemented a test-bed to simulate an electric transmission system which they used to validate the specification-based intrusion detection framework proposed in their work. Esquivel-Vargas [30] also simulate a prototype which is implemented using third-party software tools and custom scripts to validate their proposed approach. The validation of the method proposed by Sharma [34] is accomplished using UAV-CPS simulated in MATLAB. And the validation strategy employed by Olufowobi [28] involves the simulation of their proposed method with real CAN logs collected from two passenger cars and on an open-source CAN dataset collected from real-world scenarios.

4) Theoretical: Theoretical methods as validation strategies involve the use of formal or precise theoretical arguments to support the obtained results. This method has been used by Song et al. in [25] to validate specification-based intrusion detection technique. They utilise ACL2 theorem prover [42] and the enforcement of security requirements is defined and proved as theorems in ACL2.

5) None: None refers to the papers where no validation methods are deployed. Among the works we surveyed in this paper, only the work by Jieke and Pan [26] falls in this category.

IV. Observations, Concerns and Future Research Directions

We observe from this study that specification-based intrusion detection technique has been applied in several domains of CPS. For example, it has been employed by McParland [18] for monitoring security of networked control systems. Mitchell and Chen [33] have proposed the use of specification-based intrusion detection for safety critical medical cyber physical systems. Also, specification-based intrusion detection has been proposed for monitoring in-vehicle networks by Larson et al.

[29] and Oluwofobi et al. [28]. Bertheir and Sanders [27] propose the use of specification-based intrusion detection to monitor traffic at the edge of an advanced metering infrastructure. Other applications of specification-based intrusion detection techniques for CPS include SCADA systems [16], [17], [36], building automation systems [30], mobile ad hoc networks [12], [25], [13], [14], [15], IoT devices [34], power system [31], [35], unmanned air vehicles [32] and wireless local area networks [24].

There are several protocols that have been deployed in the operation of CPS. For this reason, it is natural to see that many of the existing literature of specification-based intrusion detection techniques for CPS involve the monitoring of protocols used in CPS. For instance, CAN protocol which is used for in-vehicle networks has been studied by Larson et al. in [29] and Oluwofobi et al. in [28]. Also, specification-based intrusion detection has been proposed for monitoring DNP3 protocol [16], [17], [18]. Other protocols that have been considered by the surveyed papers include C12.22 standard protocol [27], BACnet protocol [30], IEEE 801.11 protocol [24], spanning tree protocol [26], OLSR protocol [15], dynamic auto-configurations protocol [25], and AODV protocol [12], [13], [14].

We also note that only the works by Berthier and Sanders [27], Sharma et al. [34] and Song et al. [25] employed formal modelling for the verification of the specified behaviour. The use of formal modelling is an important aspect of specification-based intrusion detection technique as it enables the verification of the extracted specification. Since specification-based intrusion detection techniques depend on the specified system behaviours, it is imperative that these behaviours represents the correct behaviour of the system and formal modelling provides a tool for such verification. Unfortunately, only a few of the existing literature on specification-based intrusion detection for CPS attempted to verify the derived system specification.

Moreover, we notice that the traditional IDS performance metrics have been used in some of the existing works on specification-based intrusion detection techniques for the evaluation of their proposed technique. Performance metrics are used to measure the performance of IDS. For example, false positive rate has been used in [27], [24], [13], [36], [15] and the combination of false positive rate and false negative rate have been used in [33], [30], [28], [31], [34], [32]. In addition, Lin et al. in [17], [16] use throughput as the performance metric.

One of the biggest concerns in the use of specification-based intrusion detection techniques for CPS is the efforts and time required for specification extraction. As we have already observed, most of the existing works in the use of specification-based intrusion detection techniques for CPS employed the manual approach for specification extraction. This method is prone to errors and could jeopardize the intrusion detection ability of the specification-based IDS. Although efforts have been made by Esquivel-Vargas et al. in [30], Olufowobi et al. in [28], and Sharma et al. in [34] to address the problem through the use of automatic specification extraction, it still remains an open research issue.

Another concern when deploying specification-based intrusion detection techniques for CPS is verifying the correctness of the extracted specification. The ability of a specification-based IDS to detect anomalous behaviour depends on how correct the extracted specification represents the normal system behaviour. One of the ways to verify the correctness of the extracted specification is through the use of formal modelling. Out of the 20 works we surveyed, only Berthier and Sanders [27], Sharma et al. [34] and Song et al. [25] have deployed formal modelling for the verification of the correctness of the extracted specification. Thus, future research works need to consider the best methods for verifying the correctness of the extracted specification so as to encourage the practical application of specification-based IDS for CPS.

V. Conclusion

In this paper, we presented a survey of specification-based intrusion detection techniques for CPS. We selected 20 papers in the literature that proposed the use of specification-based intrusion detection mechanism for CPS. These papers were published between 2005 and 2020. We proposed a taxonomy to classify these papers, which is based on the following attributes: specification source, specification extraction, specification modelling, detection mechanism, detector placement and validation strategy. We observed that to fully realize the potentials of specification-based intrusion detection techniques for CPS, more work needs to be done in the future to reducing the efforts and time required to extract the system specification and to verifying the correctness of the extracted system specification.

References

[1] Gartner, "Gartner predicts 75cyber-physical security incidents by 2024," Sep. 2020. [Online]. Available: https://www.gartner.com/en/newsroom/press-releases/2020-09-01-gartner-predicts-75–of-ceos-will-be-personally-liabl

[2] S. Han, M. Xie, H.-H. Chen, and Y. Ling, "Intrusion detection in cyber-physical systems: Techniques and challenges," *IEEE Systems Journal*, vol. 8, no. 4, pp. 1052–1062, dec 2014.

[3] R. Mitchell and I.-R. Chen, "A survey of intrusion detection techniques for cyber-physical systems," *ACM Computing Surveys*, vol. 46, no. 4, pp. 1–29, apr 2014.

[4] B. B. Zarpelão, R. S. Miani, C. T. Kawakani, and S. C. de Alvarenga, "A survey of intrusion detection in internet of things," *Journal of Network and Computer Applications*, vol. 84, pp. 25–37, apr 2017.

[5] W. Wu, R. Li, G. Xie, J. An, Y. Bai, J. Zhou, and K. Li, "A survey of intrusion detection for in-vehicle networks," *IEEE Transactions on Intelligent Transportation Systems*, vol. 21, no. 3, pp. 919–933, mar 2020.

[6] E. R. Griffor, C. Greer, D. A. Wollman, and M. J. Burns, "Framework for cyber-physical systems: volume 1, overview," National Institute of Standards and Technology, Tech. Rep., jun 2017.

[7] A. A. Cardenas, S. Amin, and S. Sastry, "Secure control: Towards survivable cyber-physical systems," in *2008 The 28th International Conference on Distributed Computing Systems Workshops*. IEEE, jun 2008.

[8] A. Greenberg, "'crash override': The malware that took down a power grid," 2017. [Online]. Available: https://www.wired.com/story/crash-override-malware/

[9] A. Shrivastava, P. Derler, Y.-S. L. Baboud, K. Stanton, M. Khayatian, H. A. Andrade, M. Weiss, J. Eidson, and S. Chandhoke, "Time in cyber-physical systems," in *Proceedings of the Eleventh IEEE/ACM/IFIP International Conference on Hardware/Software Codesign and System Synthesis*. ACM, oct 2016.

[10] C. Ko, M. Ruschitzka, and K. Levitt, "Execution monitoring of security-critical programs in distributed systems: a specification-based approach," in *Proceedings. 1997 IEEE Symposium on Security and Privacy (Cat. No.97CB36097)*. IEEE Comput. Soc. Press.

[11] P. Uppuluri and R. Sekar, "Experiences with specification-based intrusion detection," in *Recent Advances in Intrusion Detection, 4th International Symposium, RAID 2001 Davis, CA, USA, October 10-12, 2001, Proceedings*, ser. Lecture Notes in Computer Science, W. Lee, L. Mé, and A. Wespi, Eds., vol. 2212. Springer, 2001, pp. 172–189.

[12] C. Tseng, P. Balasubramanyam, C. Ko, R. Limprasittiporn, J. Rowe, and K. N. Levitt, "A specification-based intrusion detection system for AODV," in *Proceedings of the 1st ACM Workshop on Security of ad hoc and Sensor Networks, SASN 2003, Fairfax, Virginia, USA, 2003*, S. Setia and V. Swarup, Eds. ACM, 2003, pp. 125–134.

[13] E. Hansson, J. Grönkvist, K. Persson, and D. Nordquist, "Specification-based intrusion detection combined with cryptography methods for mobile ad hoc networks," *Command and Control Systems Technical Report*, 2005.

[14] H. M. Hassan, M. Mahmoud, and S. El-Kassas, "Securing the AODV protocol using specification-based intrusion detection," in *Q2SWinet'06 - Proceedings of the Second ACM Workshop on Q2S and Security for Wireless and Mobile Networks, Terromolinos, Spain, October 2, 2006*, A. Boukerche, H. Chen, and M. S. M. A. Notare, Eds. ACM, 2006, pp. 33–36.

[15] C. H. Tseng, T. Song, P. Balasubramanyam, C. Ko, and K. N. Levitt, "A specification-based intrusion detection model for OLSR," in *Recent Advances in Intrusion Detection, 8th International Symposium, RAID 2005, Seattle, WA, USA, September 7-9, 2005, Revised Papers*, ser. Lecture Notes in Computer Science, A. Valdes and D. Zamboni, Eds., vol. 3858. Springer, 2005, pp. 330–350.

[16] Z. K. Hui Lin, Adam Slagell and R. K. Iyer, "Using a specification-based intrusion detection system to extend the dnp3 protocol with security functionalities," *Coordinated Science Laboratory, University of Illinois at Urbana-Champaign*, 2012. [Online]. Available: http://hdl.handle.net/2142/90434

[17] H. Lin, A. Slagell, C. D. Martino, Z. Kalbarczyk, and R. K. Iyer, "Adapting bro into SCADA," in *Proceedings of the Eighth Annual Cyber Security and Information Intelligence Research Workshop on - CSIIRW '13*. ACM Press, 2013.

[18] C. McParland, S. Peisert, and A. Scaglione, "Monitoring security of networked control systems: It's the physics," *IEEE Security & Privacy*, vol. 12, no. 6, pp. 32–39, nov 2014.

[19] P. Truong, D. Nieh, and M. Moh, "Specification-based intrusion detection for h.323-based voice over IP," in *Proceedings of the Fifth IEEE International Symposium on Signal Processing and Information Technology, 2005.* IEEE, 2005.

[20] H. Sengar, D. Wijesekera, H. Wang, and S. Jajodia, "VoIP intrusion detection through interacting protocol state machines," in *International Conference on Dependable Systems and Networks (DSN'06)*. IEEE, 2006.

[21] T. PHIT and K. ABE, "A protocol specification-based intrusion detection system for VoIP and its evaluation," *IEICE Transactions on Communications*, vol. E91-B, no. 12, pp. 3956–3965, dec 2008.

[22] R. Sekar, A. Gupta, J. Frullo, T. Shanbhag, A. Tiwari, H. Yang, and S. Zhou, "Specification-based anomaly detection," in *Proceedings of the 9th ACM conference on Computer and communications security - CCS '02*. ACM Press, 2002.

[23] N. Stakhanova, S. Basu, and J. Wong, "On the symbiosis of specification-based and anomaly-based detection," *Computers & Security*, vol. 29, no. 2, pp. 253–268, mar 2010.

[24] R. Gill, J. Smith, and A. Clark, "Specification-based intrusion detection in wlans." IEEE, 2006, pp. 141–152.

[25] T. Song, C. Ko, C. H. Tseng, P. Balasubramanyam, A. Chaudhary, and K. N. Levitt, "Formal reasoning about a specification-based intrusion detection for dynamic auto-configuration protocols in ad hoc networks," in *Formal Aspects in Security and Trust*. Springer Berlin Heidelberg, 2006, pp. 16–33.

[26] P. Jieke, J. Redol, and M. Correia, "SPECIFICATION-BASED INTRUSION DETECTION SYSTEM FOR CARRIER ETHERNET," in *Proceedings of the Third International Conference on Web Information Systems and Technologies*. SciTePress - Science and and Technology Publications, 2007.

[27] R. Berthier and W. H. Sanders, "Specification-based intrusion detection for advanced metering infrastructures," in *2011 IEEE 17th Pacific Rim International Symposium on Dependable Computing*. IEEE, 2011, pp. 184–193.

[28] H. Olufowobi, C. Young, J. Zambreno, and G. Bloom, "Saiducant: Specification-based automotive intrusion detection using controller area network (can) timing," *IEEE Transactions on Vehicular Technology*, vol. 69, pp. 1484–1494, 2020.

[29] U. E. Larson, D. K. Nilsson, and E. Jonsson, "An approach to specification-based attack detection for in-vehicle networks," in *IEEE Intelligent Vehicles Symposium*. IEEE, 2008, pp. 220–225.

[30] H. Esquivel-Vargas, M. Caselli, and A. Peter, "Automatic deployment of specification-based intrusion detection in the bacnet protocol," in *Proceedings of the 2017 Workshop on Cyber-Physical Systems Security and PrivaCy, Dallas, TX, USA, November 3, 2017*, B. M. Thuraisingham, R. B. Bobba, and A. Rashid, Eds. ACM, 2017, pp. 25–36.

[31] R. Mitchell and I.-R. Chen, "Behavior-rule based intrusion detection systems for safety critical smart grid applications," *IEEE Transactions on Smart Grid*, vol. 4, no. 3, pp. 1254–1263, sep 2013.

[32] ——, "Adaptive intrusion detection of malicious unmanned air vehicles using behavior rule specifications," *IEEE Transactions on Systems, Man, and Cybernetics: Systems*, vol. 44, no. 5, pp. 593–604, may 2014.

[33] ——, "Behavior rule specification-based intrusion detection for safety critical medical cyber physical systems," *IEEE Transactions on Dependable and Secure Computing*, vol. 12, pp. 16–30, 2015.

[34] V. Sharma, I. You, K. Yim, I.-R. Chen, and J.-H. Cho, "BRIoT: Behavior rule specification-based misbehavior detection for IoT-embedded cyber-physical systems," *IEEE Access*, vol. 7, pp. 118 556–118 580, 2019.

[35] S. Pan, T. H. Morris, and U. Adhikari, "A specification-based intrusion detection framework for cyber-physical environment in electric power system," *Int. J. Netw. Secur.*, vol. 17, no. 2, pp. 174–188, 2015. [Online]. Available: http://ijns.femto.com.tw/contents/ijns-v17-n2/ijns-2015-v17-n2-p174-188.pdf

[36] A. Carcano, A. Coletta, M. Guglielmi, M. Masera, I. N. Fovino, and A. Trombetta, "A multidimensional critical state analysis for detecting intrusions in SCADA systems," *IEEE Transactions on Industrial Informatics*, vol. 7, no. 2, pp. 179–186, may 2011.

[37] Zeek (formerly Bro), "An open source network security monitoring tool," 2020. [Online]. Available: https://www.zeek.org/

[38] T. Issariyakul and E. Hossain, *Introduction to Network Simulator NS2*. Springer US, 2009.

[39] H. Debar, M. Dacier, and A. Wespi, "A revised taxonomy for intrusion-detection systems," *Ann. des Télécommunications*, vol. 55, no. 7-8, pp. 361–378, 2000.

[40] R. G. Sargent, "Verification, validation, and accreditation: verification, validation, and accreditation of simulation models," in *Proceedings of the 32nd conference on Winter simulation, WSC 2000, Wyndham Palace Resort & Spa, Orlando, FL, USA, December 10-13, 2000*, P. A. Fishwick, K. Kang, J. A. Joines, and R. R. Barton, Eds. WSC, 2000, pp. 50–59.

[41] V. Verendel, "Quantified security is a weak hypothesis," in *Proceedings of the 2009 workshop on New security paradigms workshop - NSPW '09*. ACM Press, 2009.

[42] P. C. Dillinger, P. Manolios, D. Vroon, and J. S. Moore, "ACL2s: "the ACL2 sedan"," *Electronic Notes in Theoretical Computer Science*, vol. 174, no. 2, pp. 3–18, may 2007.