Energy Informatics

RESEARCH Open Access

Improving anomaly detection in SCADA network communication with attribute extension

Mahwish Anwar*, Lars Lundberg and Anton Borg

*Correspondence:
mahwish.anwar@bth.se

Department of Computer Science, Blekinge Institute of Technology, 371 79, Karlskrona, Sweden

Abstract

Network anomaly detection for critical infrastructure supervisory control and data acquisition (SCADA) systems is the first line of defense against cyber-attacks. Often hybrid methods, such as machine learning with signature-based intrusion detection methods, are employed to improve the detection results. Here an attempt is made to enhance the support vector-based outlier detection method by leveraging behavioural attribute extension of the network nodes. The network nodes are modeled as graph vertices to construct related attributes that enhance network characterisation and potentially improve unsupervised anomaly detection ability for SCADA network. IEC 104 SCADA protocol communication data with good domain fidelity is utilised for empirical testing. The results demonstrate that the proposed approach achieves significant improvements over the baseline approach (average F_1 score increased from 0.6 to 0.9, and Matthews correlation coefficient (MCC) from 0.3 to 0.8). The achieved outcome also surpasses the unsupervised scores of related literature. For critical networks, the identification of attacks is indispensable. The result shows an insignificant missed-alert rate (0.3% on average), the lowest among related works. The gathered results show that the proposed approach can expose rouge SCADA nodes reasonably and assist in further pruning the identified unusual instances.

Keywords: Supervisory control and data acquisition, Network intrusion detection, Machine learning, IEC 60870-5-104, Attribute extension

Introduction

Critical infrastructure is under constant threat (Tariq et al. 2019). A critical infrastructure (CI) is a system or part of a system that maintains vital societal functions. Examples of CI sectors include; energy, oil and gas, water and waste treatment, and transportation. The disruption or destruction of such a system would result in failure for the society to function and can negatively affect its economy and safety.

CIs widely rely on supervisory control and data acquisition (SCADA) systems to manage and control CI operations (Tariq et al. 2019). For example, the SCADA system in the energy power grid would be responsible for the transmission and distribution of electricity. A SCADA system performs centralised monitoring and control for geographically distributed remote units, often scattered over thousands of square kilometers. The gathered data results in automated or operator-driven supervisory commands for the field units, e.g., open and close valves/breakers, share sensor data or monitor the local environment for alarm conditions (Zhu et al. 2011). Since the SCADA system is an essential element within the CI, it becomes vital to protect it from the threats that exist in the cyber-landscape. As Industrial Control System (ICS) / SCADA system security experts warn, "it is not a matter of if it (ICS/SCADA system) will fail, but when it will fail" (Assante and Lee 2015).

SCADA systems usually are zoned out from the external cyber-threats through air-gapping, intrusion detection, and prevention systems, and firewalls (Pliatsios et al. 2020). However, by exploiting SCADA-specific protocol vulnerabilities and launching a successful malware attempt, the intruder can bypass the security measures and gain unauthorised access to the critical network (Assante and Lee 2015; Pliatsios et al. 2020). Stuxnet and BlackEnergy attacks on control systems highlighted the lack of awareness of the security of these systems. It showed that the hacker could passively listen to the SCADA communication and deliver the attack successfully once inside the network (Assante and Lee 2015).

On the one hand, the SCADA systems have become intelligent, real-time, and interconnected with the integration of the Internet of Things and Cloud. On the other hand, these advancements have made the SCADA system more prone to network vulnerabilities (Tariq et al. 2019). It is, therefore, imperative to detect anomalies proactively in SCADA networks and meet the growing security challenges. Thus, continuous effort is required by industry and academia alike to monitor and safeguard SCADA networks.

Generally, SCADA intrusion detection systems rely on the network traffic data, the host process data, or the data related to the physical event or operation. The approaches to intrusion detection include signature-based detection, machine learning-based anomaly detection, and deep learning-based anomaly detection. Suricata is an example of signature-based detection that utilises SCADA network traffic data to detect cyberattacks (Wong et al. 2017). In Robles-Durazno et al. (2018), various machine learning-based anomaly detection methods are applied to classify signal deviations in a water supply system. Whereas, in Gaggero et al. (2020), the undesired working conditions of the distributed energy control system are identified using a deep learning-based anomaly detection technique. We also find a hybrid intrusion detection approach that applies both network protocol traffic data and physical behaviour characteristics to isolate SCADA network anomalies (Yang et al. 2016). Our work focusses on SCADA network traffic data and the application of a machine learning-based anomaly detection approach.

Canonical data-driven approaches for CI can detect new anomalies at the cost of a high error rate (Rakas et al. 2020; Panagiotis et al. 2021). This is because of the overlapping nature of the normal and anomalous communication packets, making it difficult for the detector to separate the network anomalies effectively. To reduce machine learning-based network anomaly detection errors, we approach the issue by extending the input set (or attribute set) of a standard SCADA communication protocol.

We see the application of composing advanced attributes for IEC 61870 SCADA protocol in Linda et al. (2009), where the authors propose neural networks to extract the trends in network communication to perform intrusion detection. In Mantere et al.

(2013), an analysis of IP traffic traces in SCADA is presented, and an intrusion detection system using machine learning-based techniques is suggested as future work. To the best of our knowledge, attribute extension has not been investigated for anomaly detection in the IEC 60870-5-104 (or IEC 104) SCADA protocol. Hence, in this study, we investigate the possibility of analysing the SCADA network through topological behaviour and extending the attribute space for improving anomaly detection performance.

The intuition behind attribute extension is to represent the SCADA network behavior by modeling the relationship between interacting SCADA nodes. We perform the detection of attacks for IEC 60870-5-104 communication protocol, both with and without attribute extension. IEC 104 is a widely implemented telecontrolling protocol and is prone to vulnerabilities (György and Holczer 2020). In this study, we focus on IEC 104 SCADA protocol and derive new attributes to improve one-class SVM anomaly detection performance.

One-class support vector machine (SVM) algorithm is a popular machine learning intrusion detection algorithm (Tsai et al. 2009; Thakkar and Lohiya 2021). The learning algorithm is also an acknowledged choice for intrusion detection in the SCADA network (Rakas et al. 2020). Furthermore, recent works on standard SCADA-specific protocol (IEC 104) relayed the algorithm's stable performance for detecting different attacks (Egger et al. 2020; Anwar et al. 2021). Egger et al. (2020) compared intrusion detection of the signature-based method with machine learning methods. Supervised and semi-supervised (with one-class SVM) learning performed better intrusion detection, while Snort signature-based gave worse (Egger et al. 2020). The same protocol dataset is systematically evaluated with other learning algorithms in Anwar et al. (2021). Mahwish et al. evaluated the SCADA network intrusion detection ability of distance-based, density-based, and kernel-based learning methods in an unsupervised setting for IEC 104 communication protocol. The comparison of detection methods revealed that on average one-class SVM method performs steadily for the given SCADA protocol data in reference to other candidate learning methods. In the current work, we draw a comparison with study (Anwar et al. 2021). Realising the predictable and steady performance of one-class SVM for SCADA protocol and its ability to segregate communication network data, we intend to amplify the outlier detection capability of one-class SVM for the IEC 104 protocol. Briefly, we explore the following research question: To what extent can attribute extension improve one-class SVM anomaly detection in IEC 104 protocol communication within SCADA network?

More explicitly, we make the following contributions:

- A method for extending the attributes to project the SCADA network behaviour is presented.
- The impact of the extended attribute set is evaluated using machine learning-based anomaly detection technique with the Support Vector Machine algorithm. The study describes the improved machine learning model design and implementation; and compares the performance with the baseline results and previous research.

Background and related work

Introduction to SCADA system

SCADA system (Fig. 1) is instilled in critical infrastructure architecture. It is a process monitoring and controlling system that perform geographically distributed operations. One of the system's main components is the remote terminal unit (RTU). The RTU is an intermediate node between field devices and a master unit that connects with the SCADA human machine interface. RTU exchanges sensory data with the master unit and sends specified control commands to the field devices. The human machine interface (HMI) sits between the SCADA operator and RTUs. The master unit gathers the data, which the HMI translates to enable interaction with the operator. The operator monitors the system via SCADA HMI, troubleshoots alerts, and performs the necessary control operations. The operator can access the SCADA HMI remotely, or through the Internet (Zhu et al. 2011).

SCADA network communication protocols are adopted to facilitate continuous and reliable communication within the SCADA system. These communication protocols consider the processing capabilities of SCADA nodes and the communication requirements of industrial applications. Standard protocols used in electrical applications and power system automation for remote control and monitoring include a set of IEC 60870

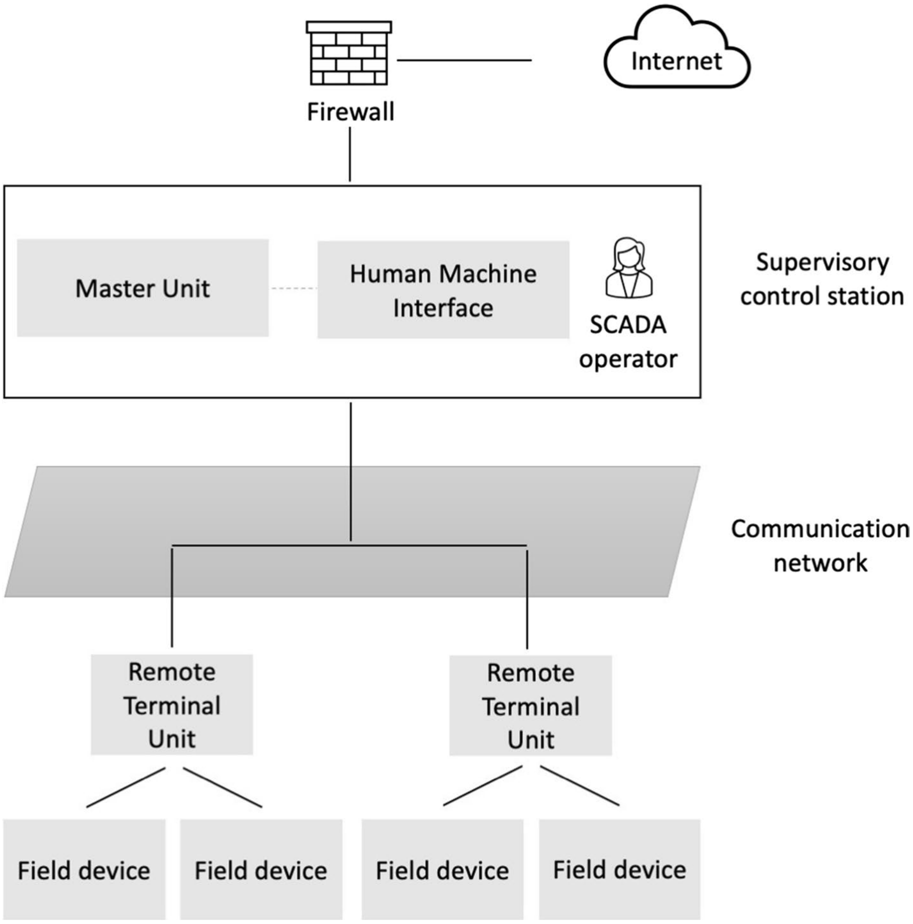


Fig. 1 Abstraction of SCADA system (Zhu et al. 2011; Maynard et al. 2018)

protocols, Modbus and DNP3 (more common outside of Europe) (Zhu et al. 2011; Pliatsios et al. 2020). IEC 60870-5-104 (part of the IEC 60870 standard) is a widely adopted protocol for telecontrol in European power transmission, distribution, and control systems, despite its security vulnerabilities, which include lack of authentication, integrity checking, and encryption (Matousek 2017; Radoglou-Grammatikis et al. 2019; György and Holczer 2020). Due to the widespread interconnectivity and complexity of IEC 60870-5-104 (or IEC 104), the vendors and utility operators are reluctant to roll-out its successor IEC 62351, which is more secure than IEC 104.

Here we focus on the IEC 104 protocol. IEC 104 operates using the client-server communication model. Under the protocol, every node in the network is either a controlling station (master) or a controlled station (slave) (Matousek 2017). The transmission happens in the monitor direction, i.e., from the controlled station (typically an RTU) to the controlling station (e.g., SCADA HMI). Or the control direction, i.e., from the controlling station to the controlled station (Matousek 2017).

The IEC 104 protocol defines the Application layer of the OSI model and uses Ethernet technology for the link layer. IEC 104 enables the communication between the controlling node and the controlled nodes via a TCP/IP communication network. The IEC 104 protocol data transmits in either of the following three frame formats: (i) format-U is for the control functions, e.g., the controlling node issues START and STOP commands to control the data transfer from a controlled node. (ii) format-S is for supervisory commands, e.g., to indicate time-out in case of longer data transmission. (iii) format-I is to transfer information in both directions, e.g., interrogation command in the control direction or to send measured value in the monitor direction (Matousek 2017).

Anomaly detection in SCADA communication network

It is common for SCADA system operators to protect the SCADA communication network by gathering and parsing the communication protocol packets, e.g., from SCADA nodes, and forward them to the intrusion detection system (IDS). The IDS takes parsed SCADA protocol packets (i.e., packets where key fields from the protocol frames have been identified and dissected, e.g., payload length, IP address, port, etc.) and performs monitoring and detection based on the predefined signatures. In the case of a flag, the filtering of the protocol packet is performed. Such IDSs perform active monitoring and deep packet inspection often on the edge due to high processing requirements, thus, limiting the scope to external threats (Pliatsios et al. 2020). However, the internal SCADA network goes unchecked. Similarly, firewalls and anti-virus software shield the critical SCADA system only partially from security threats (ENISA 2017).

The European Union Agency for Cybersecurity (ENISA) emphasises the need to monitor the internal and external SCADA communications in the following words, "without active network monitoring, it is very difficult to detect suspicious activity, identify potential threats, and quickly react to cyber attacks" (ENISA 2017). An adversary in the past accessed the SCADA system by sending an email with malware to an authorised SCADA user. The malware helped the attackers to listen to SCADA communication, plot and execute the attack and create a backdoor. The attack caused an outage of 6 h and affected over 200,000 customers (CISA 2016). Similar other incidents (Assante and

Lee 2015; Pliatsios et al. 2020) stresses the need to monitor the internal SCADA protocol communication traffic regularly.

Regular analysis of the internal SCADA communication can enrich the operators to get visibility of the SCADA traffic which in turn can aid in understanding the routine network behavior, thus, enabling outlier identification (Mahmood et al. 2010; Matousek et al. 2019). A SCADA architecture to monitor inside and outside network traffic is presented in Mahmood et al. (2010). A similar course of action is proposed in Matousek et al. (2019) where the research highlights gaining visibility of the network characteristics and operations (such as transmission data, connected nodes, malfunctioning nodes, etc.) through analysing network traffic. The authors later extended their work by proposing an anomaly detection approach based on an analysis of SCADA protocol communication to point resource scanning, rogue devices, and unusual traffic (Matousek et al. 2020). They employ finite state automata to infer the IEC 104 communication flow profile of two SCADA nodes. If the probability of the candidate nodes is lower than the defined threshold, the detector will flag it as an unknown communication sequence (Matousek et al. 2020).

The sequence attacks in IEC 104 protocol are detected with the use of Discrete-time Markov Chains in Ferling et al. (2018). To identify malicious IEC 104 communications in SCADA networks a signature-based method is given in Yang et al. (2013), where the authors propose inspection of the incoming communication packets based on the customised rules and correlations between different protocol fields that represent usual SCADA communication flow. Robert Udd et al. (2016) suggest a hybrid approach for anomaly detection, where initially, the SCADA protocol packet passes through allowlists (node pairs, TCP control, etc.). If no alert is issued from the initial step, a statistical analysis of the packet's timing characteristics is executed. Their work resulted in anomaly detection for IEC 104 zero-day attacks. The use of spontaneous packet analysis for IEC 104 SCADA protocol is utilised for anomaly detection in Lin and Nadjm-Tehrani (2019), where the authors investigate the inter-arrival time of the packet. If the inter-arrival time value is outside the training interval boundary, an alarm is raised, and the second detection phase begins. The time-interval flags for individual SCADA nodes are correlated to create a time-series in the second phase. The system labels the corresponding node anomalous if the threshold exceeds the warning-threshold. This approach is more suitable for intermittent anomalies.

An IEC 104 intrusion detection approach similar to Udd et al. (2016) can be seen in a recent publication (Grammatikis et al. 2020). In the latest work, an access control mechanism is enforced initially to filter unknown ports, Internet Protocol, and Media Access Control addresses. Afterward, based on 7 aggregated features (e.g., total packets in the forward direction, the total size of the packets in the backward direction, standard deviation size of the packets in the forward direction, etc.) based on different flow intervals, outlier analysis is discharged. At higher flow intervals, F_1 score slightly increases. In the absence of outlier ratio and error rates, it is ambiguous to contextualise the detector's true capability.

Anomaly detection for IEC 104 protocol with supervised machine learning methods, such as Decision Tree, Nearest-neighbour, etc., is given in Hodo et al. (2017). Egger et al. compared Snort-based intrusion detection with machine learning-based intrusion detection methods (Egger et al. 2020). The supervised and semi-supervised machine learning methods for IEC 104 SCADA protocol outperformed signature-based intrusion detection, and unsupervised learning (Egger et al. 2020). Later, systematic performance evaluation of IEC 104 anomaly detection with unsupervised learning approaches was accomplished in Anwar et al. (2021). Both studies (Egger et al. 2020; Anwar et al. 2021), utilised the same IEC 104 dataset. However, the dataset lacks multiple SCADA nodes; therefore, additional exploration is required to assess the performance of the unsupervised learning approach and, if required enhance the outcome. In the present research, we address the same knowledge gap.

Evaluations from Egger et al. (2020); Anwar et al. (2021); Grammatikis et al. (2020) reveal that for IEC 104 protocol communication, the Support Vector Machine method offers stable results for unsupervised anomaly detection. Accordingly, we focus on improving SVM unsupervised anomaly detection performance for IEC 104 SCADA protocol.

Attribute processing

Machine learning-based network anomaly detection solutions (Tsai et al. 2009) often manipulate the attributes to make better predictions and sometimes to reduce computational costs of processing large datasets (Flach 2012; Thakkar and Lohiya 2021). To underline the need for attribute processing, we diverge it into four modus operandi (Fig. 2). Peter Flach defines the observations or instance space as a set of all possible objects of interest in machine learning. The instance space can be inconceivably expansive; therefore, a fraction of instances commonly formulate a dataset. Since each instance in the dataset is described by a fixed number of attributes, we refer to it as attribute set (Flach 2012).

The attributes in the attribute set can be manipulated or processed in one or a few of the following methods. Attribute decomposition enables the creation of new

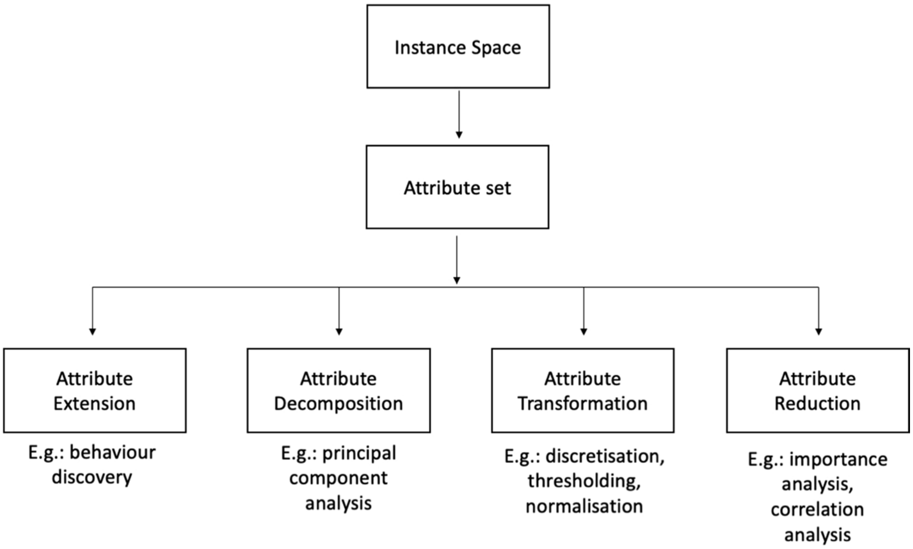

Instance Space
Attribute set
Attribute Extension
Attribute Decomposition
Attribute Transformation
Attribute Reduction
E.g.: behaviour discovery
E.g.: principal component analysis
E.g.: discretisation, thresholding, normalisation
E.g.: importance analysis, correlation analysis

Fig. 2 Modus operandi of attribute processing in machine learning network anomaly detection

attributes that are linear combinations of available attributes, e.g., through principal component analysis (Flach 2012). The same projection method is named differently in Thakkar and Lohiya (2021), but both explain the notion of projecting higher-dimensional or sparse attribute space to a lower-dimensional attribute space. Attribute transformation includes various mechanisms with which the attribute kind is transformed. For example, thresholding transforms a quantitative attribute into a Boolean attribute by finding a split threshold value. Discretisation transforms a continuous attribute into an ordinal attribute kind. The transformation mechanisms, generally, are required to scale the attribute values, indicate the presence of a certain attribute, or make the attribute meaningful for prediction task (Flach 2012). Attribute reduction mainly involves attribute selection (Flach 2012; Thakkar and Lohiya 2021), for example based on attribute importance or relevance. It also includes dropping redundant attributes based on correlation analysis. We append a fourth method to the list called Attribute extension, which forms the basis of improving the machine learning prediction ability of one-class SVM within the context of the IEC 104 protocol. We define it as a method to construct new attributes based on domain knowledge to enrich the available attribute set with more representative attributes.

Topological attribute extension

Graph-based anomaly detection approaches are a branch of data mining and machine learning techniques that capture and analyse the interactions between data objects of a network or graph to detect potential anomalies (Pourhabibi et al. 2020). Such approaches can analyse the connectivity patterns and graph object behaviour in communication networks to flag suspicious graph nodes, irregular connectivity between nodes, or unusual subgraphs by drawing intra-graph comparisons (Pourhabibi et al. 2020). Our approach to model SCADA networks resembles the structural-based graph method, as described in Pourhabibi et al. (2020), where we exploit topological graph structure and characterise the SCADA network nodes with node and edge attributes, thus extending the attribute space.

In Akoglu et al. (2010) the authors exploit graph node and node-neighbourhood characteristics to model the egonet laws and to identify nodes violating the laws. Topological and temporal graph attributes are measured in Henderson et al. (2010) to analyse volatile network behaviour. The work uses a multi-level approach, where the network is analysed from a topological global-level, such that if an unusual event is discovered, the analysis moves to the next level (node-level). Application of graph node characteristics to group similar nodes was put-forth in Henderson et al. (2012), where the nodes with similar degrees and edges were unified under a single role. The role assigned to each node can be utilised to find strange nodes within a network.

We exploit the structural attribute discovery for the SCADA network nodes participating in the communication network. The characterisation of the SCADA nodes and node neighbours yields additional attributes—attribute extension—that enrich the attribute space.

Method

This section describes the research process undertaken (Fig. 3), starting from the extraction of the original IEC 104 protocol attributes through the machine learning experiment's design choices. We describe the reconstruction of IEC 104 attribute set and the application of the single-class SVM learning algorithm to cluster anomalous exchanges in the SCADA protocol communication (step 1 through 11).

Step 1: Data extraction

We extract IEC 104 instances from a simulated IEC 104 protocol communication (Maynard et al. 2018). The authors in Maynard et al. (2018) generate the protocol communication data from their standard compliant implementation of testbed framework that mimics a real SCADA system. Furthermore, they simulate attacks and make the complete dataset openly available. The log file of the packet capture encapsulates IEC 104 attributes, including the application layer fields. Due to these strengths, the authors in Maynard et al. (2018) recommend using the provided dataset to verify the effectiveness of a network-based intrusion detection for SCADA networks, thus, making the dataset suitable for our study.

Other than comprehensiveness and imitation of real-world deployment of SCADA networks, the chosen dataset is suited for the work since the SCADA network protocol, IEC 104, adheres to a shared network master-slave topology (Maynard et al. 2018), making it possible to apply the approach and attributes to other IEC 104 datasets and without prior network details.

The initial protocol attribute set (Table 1) is elicited from previous work (Egger et al. 2020) and knowledge gathered from the domain experts.

The main limitation with IEC 104 dataset in Egger et al. (2020) is that it does not define the direction of the transmission of IEC 104 packets, nor does it provide Ethernet address information of the nodes in the SCADA network. IEC 104 communication logs include these data and are deemed helpful by domain experts when designing a network anomaly detector. Thus, to build our dataset, we consider the transmission direction along with the time difference between two transmitted packets, source, and destination Ethernet addresses.

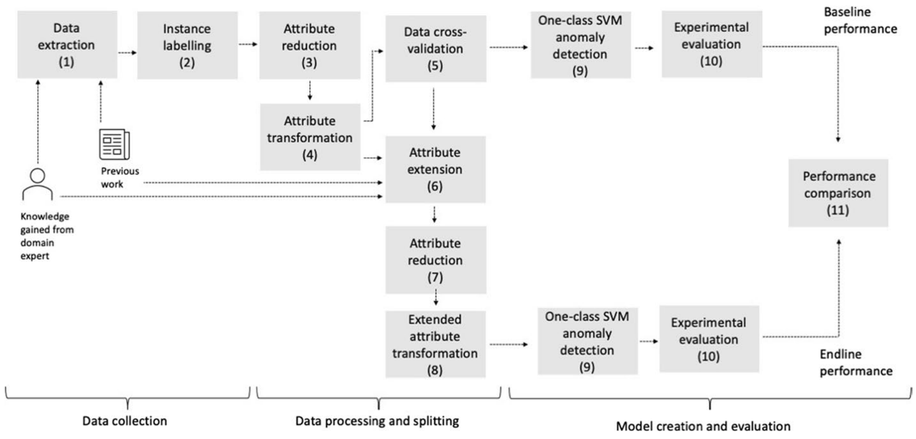

Data extraction (1)
Instance labelling (2)
Attribute reduction (3)
Data cross-validation (5)
One-class SVM anomaly detection (9)
Experimental evaluation (10)
Baseline performance
Attribute transformation (4)
Attribute extension (6)
Previous work
Knowledge gained from domain expert
Performance comparison (11)
Attribute reduction (7)
Extended attribute transformation (8)
One-class SVM anomaly detection (9)
Experimental evaluation (10)
Endline performance
Data collection
Data processing and splitting
Model creation and evaluation

Fig. 3 Process flow

Table 1 IEC 104 attributes

Attribute	Description
Destination	Destination Ethernet address
Source	Source Ethernet address
dirFrame	Transmission direction of frame
deltaTime	Time difference between 2 consecutive frames
Length	Ethernet frame length
ipTtl	Time to live
tcpHdrLen	TCP header length
tcpWinSize	TCP window size
tcpPduSize	TCP frame size
ipFlag	Indicates don't fragment bit
Type	Format type of frame—U, S, I
TypeID	Type Identification number of format-I telegram
CauseTx	Cause of the Transmission of format-I telegram

Table 2 Dataset class composition

Class	No. of IEC 104 packets
Normal	41,948
Anomalous	2425

Step 2: Instance labelling

The emulated IEC 104 protocol communication includes two attack simulations: Man-in-the-Middle (MITM) and Reconnaissance (Maynard et al. 2018). The protocol logs represent 150 min of IEC 104 communication (44373 packets) between 8 nodes: 1x Controlling Node; 5x Controlled Nodes; and 2x Attackers.

Since Maynard et al. (2018) described the attacks, we are able to label the individual frames: Label 0: normal; Label 1: MITM intrusion, and Label 2: Reconnaissance intrusion. However, the main objective is to segregate normal IEC 104 packets from anomalous frames for anomaly detection. Therefore, all attack instances are regrouped as anomalous.

After manual labelling of the packets, the dataset contains 41948 normal IEC 104 protocol packets and 2425 packets with anomalies (Table 2).

Step 3: Attribute reduction

Our IEC 104 dataset has both categorical and continuous data. For missing categorical values (*TypeID* and *CauseTx*), 'none' is substituted. It indicates the transmission does not have a format-I frame. There are no missing continuous attributes.

We perform correlation analysis for non-categorical attributes, and find *Length* and *tcpPduSize* have near-perfect correlation. Hence, only *Length* is retained. Also, this analysis reveals, *ipTtl* and *tcpHdrLen* have no coorelation with any other attribute nor with the target class. Further exploration indicates that values for both, *ipTtl* and *tcpHdrLen*, are constant throughout the simulation, and therefore, are dropped.

Step 4: Attribute transformation

The remaining continuous attributes (*Length, tcpWinSize* and *deltaTime*) are discritised using ordinal uniform binning. The process transforms the attribute values into ordinal values, such that each ordinal value or bin corresponds to an interval of the actual quantitative values. All the attributes are encoded as dummy variables before implementing the next steps.

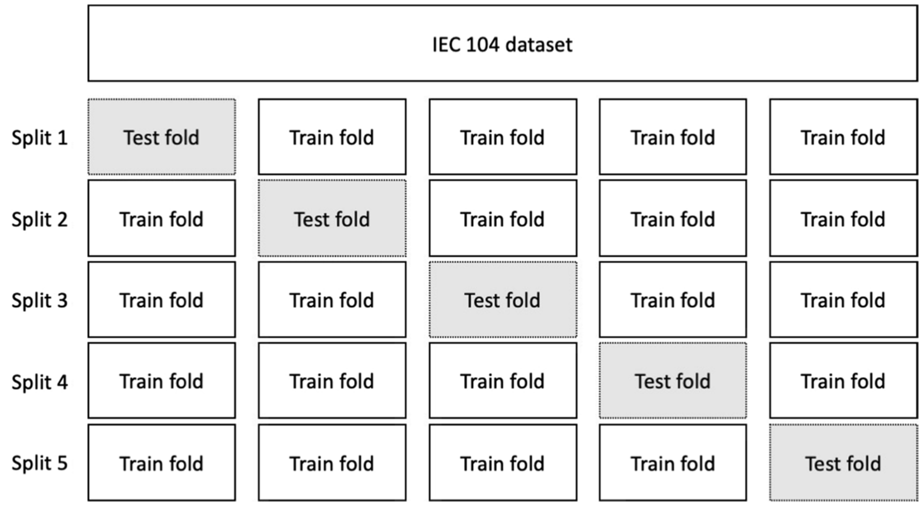
Step 5: Cross-validation

The dataset is sliced into two parts: train and test sets to measure the machine learning models' detection ability. The first set is used to fit the detection solution, while the second set is used to realise if the model will function on new or unseen data. To circumvent over-fitting, we split the entire dataset 10-times using 5-fold cross-validation. We summarise the working of 5-fold cross-validation in the following steps: (i) the entire dataset is resampled into 5-folds (Fig. 4), where one fold becomes the test fold and the remaining folds are used for training one-class SVM anomaly detection model. (ii) the detection performance on each test fold is calculated. For endline approach the extended features obtained from the training set are used when classifying the test set instances. When new nodes appear in the test set, we assign a default value of zero to the respective attribute. (iii) after cross-validating 5 test folds, the dataset is again split into 5-folds. We perform *k*-fold cross-validation 10 times, where *k* is equal to 5. This process is also known as 10x5 fold cross-validation.

Evaluating performance on the test folds indicates if the built models will generalise. We enforce the class composition in all the split folds to retain the normal to anomalous ratio.

Step 6: Attribute extension

We examine training sets from cross-validation to capture the extended features. To improve the network anomaly detection ability of one-class SVM for IEC 104 protocol communication, we extend the original IEC 104 attributes (Table 3). We propose



IEC 104 dataset

Split 1	Test fold	Train fold	Train fold	Train fold	Train fold
Split 2	Train fold	Test fold	Train fold	Train fold	Train fold
Split 3	Train fold	Train fold	Test fold	Train fold	Train fold
Split 4	Train fold	Train fold	Train fold	Test fold	Train fold
Split 5	Train fold	Train fold	Train fold	Train fold	Test fold

Fig. 4 5-Fold cross-validation on IEC 104 dataset

Table 3 Extended IEC 104 attributes

Attribute	Description
Degree (deg)	Node degree (node neighbours)
Weight (wt)	Node weight (node participation)
PairEx	Nodes have two-way transmission

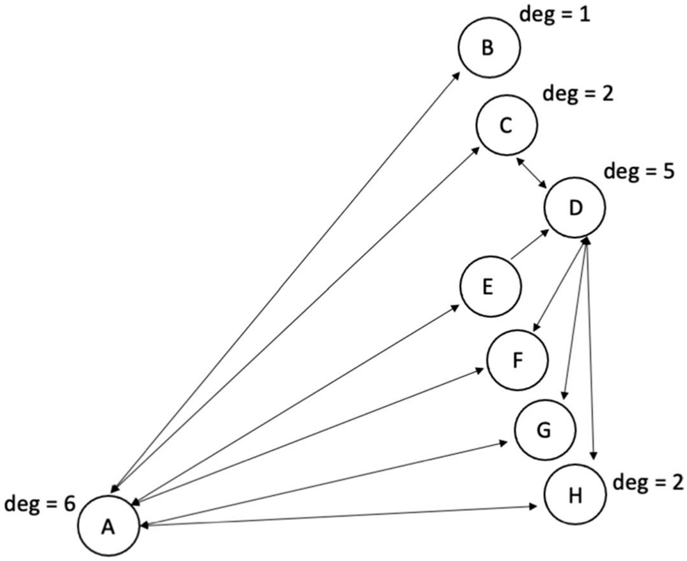


Fig. 5 Example SCADA network nodes with corresponding degree attributes

characterisation of the SCADA communication network such that the topology of the participating nodes is represented in the form of extended attributes. The intuition of utilising the topological features is founded on the knowledge gained from domain experts and the fact that IEC 104 SCADA communication network complies with a common master-slave topology (Matousek 2017).

Since the IEC 104 protocol adheres to the standard network master-slave topology, it is possible to process other IEC 104 packet capture files without prior network details. We automatically extract the graph attributes using the network node's source and destination Ethernet addresses. A similar approach should be applicable to other IEC 104 SCADA protocol datasets.

Considering the SCADA network topology knowledge, we regard the SCADA network as a graph—a structure composed of connected vertices. The vertices are the nodes in the SCADA network. Since two-way communication exists in IEC 104 protocol, a node can be a sender and a receiver. Thus, we model each node from the perspective of the sender and receiver of the communication packet. We represent each vertex (or node) of the graph (or network) by a measure of its neighbouring nodes, attributed as *deg* (node degree). For example, the volume of neighbours for node A when node A is the packet receiver is equal to 6 (Fig. 5).

Another attribute that explains the participation of a node within the network is node weight. Node weight demonstrates the distinct behavior of the given node in terms of its relative IEC 104 packet frequency. The attribute allows modelling the respective node participation with the communication frequency of other nodes in the network. Like node degree attribute, each node will be featured as *wt* (node weight). In IEC 104 protocol communication, the slave nodes typically fall under the same frequency interval. For example (Fig. 5), weight (*wt*) of nodes E, F, G and H, ideally, would have less variance.

The logical assumption is to secure the master or the controlling nodes in the SCADA network (which also resonates with the domain expert's preference). We model the point-to-point communication between two nodes assuming the receiving node in the communication frame is potentially a master or serving node and is vulnerable to attacks. Correspondingly, we assume the opposite node in the communication is a slave or the client node and is passively gathering network knowledge or actively attempting a MITM. In regular circumstances, the IEC 104 network topology would ideally show the slave nodes to follow a similar participation behaviour. Thus, distinguishing an unusual participating node behaviour could be interesting to isolate. Therefore, we consider the source node participation behaviour (*wt*) and the corresponding node's neighbourhood volume (*deg*) to complement the communication between a pair. Both these attributes will model two-way point-to-point communication between the nodes in the network.

Hundreds of IEC 104 protocol packets are exchanged within the SCADA network daily. We capture the evidence of two-way communication between two nodes by adding an attribute called *pairEx* that records the existence of a response packet. For example, if node A sends format-I packet to node B, node B sends IEC 104 packet to node A with the same type ID, we can establish that pair communication exists. This attribute has binary values. Such extended behavioural node attributes characterise the SCADA network's function, thereby enriching the dimensional space for unary SVM based anomaly detection.

Step 7: Extended attribute reduction

After we project the network nodes with extended attributes, the node addresses are disregarded. This is because each node has been modeled with newly constructed behavioural features. In a real SCADA network, where hundreds of nodes are present, such reduction would reduce computational costs, besides maintaining the characteristics of the respective node.

Afterward, we perform correlation analysis, similar to Step 3. This is done to understand the relationship between newly constructed attributes. The analysis reveals that new attributes have a strong linear correlation.

Step 8: Extended attribute transformation

We transform the new node degree attribute using the user-defined threshold (considering the network architecture knowledge). Consider a SCADA network with one controller node and three monitoring nodes. In an intruder-free example scenario, the node degree threshold becomes two. If any node has a degree greater than half of the nodes in the network, then it may be anomalous, implying possible master impersonation.

The node weight attribute is transformed using a user-defined threshold of the 40th percentile. This indicates that if the nodes in the SCADA network have a relative weight less than the relative mode weight (weight of the majority of nodes in the network), they should be segmented. More than half of the network nodes (60%) will have relative participation of at least threshold node weight in a normal network. At last, the extended binary attribute and all the transformed attributes are encoded as dummy variables.

Step 9: One-class SVM anomaly detection

To identify potential anomalies, we opt for one-class support vector machine (SVM) learning algorithm because it has been systematically evaluated to be stable and better when classifying anomalies in IEC 104 communication in an unsupervised setting (Anwar et al. 2021). The results (Anwar et al. 2021) show the potential of the chosen algorithm and call for attention to boost its usefulness for the given context.

The algorithm separates the instances by computing the relationship between each pair of observations using the Radial Basis Kernel. This function projects the observations in a higher dimension and then dissects the projection with a hyperplane (Schölkopf et al. 1999). The algorithm uses the default parameter settings with PyOD (Zhao et al. 2019).

We execute one-class SVM anomaly detection learning in an unsupervised setting for binary prediction; for original and reconstructed IEC 104 protocol attributes.

Step 10: Experimental evaluation

The test folds give detection performance of the 50 candidate one-class SVM anomaly detection models resulting from 10x5 cross-validations. Subsequently, we average the performance of the candidate models and calculate the standard deviation over all folds. We report the evaluation of IEC 104 data on cross-validated test folds with the help of below described metrics.

- False negative rate (FNR);
- False positive rate (FPR);
- F_1 score;
- Matthews correlation coefficient (MCC);
- AUC score.

False negative rate (FNR) and False positive rate (FPR) indicate the incorrect decisions of the anomaly detection approach, also known as costs. Therefore, it is essential to gauge the skill of the approach in reference to the errors. Ideally, the anomaly detector should have no errors. Due to the criticality of the context, our focus is drawn toward FNR.

False negative rate (FNR) gives an insight into miss-classifications. It is the error ratio of the number of packets that are misclassified as normal (FN) to the sum of false negative and true positive (TP) values (Eq. 1). This is a crucial metric since it tells how well the model detects anomalies. FNR close to 0 means the model is good at detecting the anomalies.

$$FNR = FN/(FN + TP) \tag{1}$$

False positive rate (FPR) also gives insight into positive miss-classifications. It is the ratio of the number of packets that are misclassified as anomalous (FP) to the sum of false positive and true negative (TN) values (Eq. 2). In other words, it is the rate of normal packets that are incorrectly labelled as anomalous. FPR close to 0 is indicative of good detection performance. However, it is common for unsupervised machine learning-based anomaly detection systems to suffer from high FPR, where often each false positive case requires human investigation. For our evaluation, FPR lower than 5% and at the cost of non-existent missed anomalous packets is considered satisfactory.

$$FPR = FP/(FP + TN) \tag{2}$$

Identifying the attack class is crucial in the current context, which is represented by the recall—ratio of correctly identified attacks to total (actual) attacks. At the same time, the result produced by the detector should reflect the precision—ratio of correctly identified attacks to total predicted attacks. To capture a balanced view of recall and precision, we rely on the F_1 score—harmonic mean of recall and precision (Eq. 3). Considering the need to represent the ability of the detector in terms of both classes, we measure the F_1 score for both classes and then average them (referred to as macro-average F_1 score). An acceptable macro-average F_1 score value for the given context is greater than 0.8 (where 1 is maximum and worst is 0).

$$F_1 score = 2 * TP/(2 * TP + FP + FN) \tag{3}$$

Macro-average F_1 score gives equal weight to both classes but ignores true negatives, i.e., the correctly separated routine IEC 104 packets. Additionally, its magnitude bents toward true positives, i.e., the correctly separated rare IEC 104 packets. To overcome this deficiency of macro-average F_1 score, we also calculate the Matthews correlation coefficient (MCC). MCC is an educative score to evaluate binary classifications as compared to accuracy and F_1 score (Chicco and Jurman 2020).

MCC is a correlation coefficient between the actual values and the values the detector outputs. To do so, it considers errors (missed classifications) and correct classifications as well as the variable composition of classes (Eq. 4). It ranges from +1 to −1; where a coefficient of +1 indicates perfect classification, a coefficient of 0 indicates average classification, and −1 indicates worst classification.

$$MCC = \frac{TP * TN - FP * FN}{\sqrt{(TP + FP)(TP + FN) * (TN + FP)(TN + FN)}} \tag{4}$$

Another measure that demonstrates the skill of the anomaly detection system is a receiver operating curve plot or ROC plot, where the rate of true positives (TPR), i.e., the rate of correctly detected anomalies, is plotted in contrast to FPR. The performance measure is generally represented as an area under curve (AUC) score. Simply put, AUC score gives insight into the trade-off between correctly detected attacks (true positives) and errors of miss-classifying attacks (false positives). A good AUC score is close to 1.

Step 11: Performance comparison

To discern if endline approach performs better than the baseline, or vice versa, we perform significance hypothesis testing. Though we can consume any (or all) of the evaluation metrics for reporting comparative evaluation, we consider two—macro-average F_1 score and MCC, mainly for their comprehensiveness but also for brevity. The normality test on macro-average F_1 score and MCC samples over 50 candidate test-folds for both approaches yield that the samples are likely drawn from Gaussian distributions.

The preceding deduction converges our choice to Student's t-test that outputs p-value (Flach 2012). The p-value is compared with the significance level to establish evidence for the null hypothesis. The null hypothesis of Student's t-test state that two related samples have identical average values, which in our case refers to both macro-average F_1 score and average MCC values for both approaches. The level of significance is set to 1% as a criterion for accepting the null hypothesis.

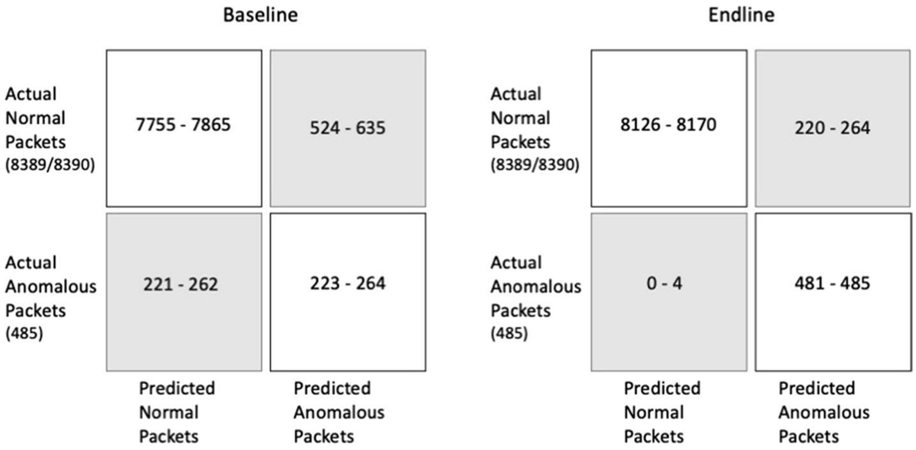
The significance test is followed by Cohen's d effect size test with the intent to quantify the significance of the magnitude of difference between the two approaches. Cohen classifies effect sizes as small, medium and large, where $d > 0.8$ indicates large effect size (Sullivan and Feinn 2012).

Results

Initially, we executed the experiment with original IEC 104 attributes, which provides a baseline unary SVM anomaly detection evaluation. In the second run, the machine learning experiment performs anomaly detection using the reconstructed attribute set, which results in endline performance evaluation. Ultimately, the performance summary of IEC 104 one-class SVM anomaly detection in an unsupervised setting for both approaches is compared (Fig. 3).

We perform 10x5-fold cross-validations to assess the ability of the one-class SVM anomaly detector for the IEC 104 protocol communication. Each cross-validation model comprises a test set of approximately 8390 typical and 485 anomalous IEC 104 protocol packets. The result of the candidate anomaly detection models is represented in the form of an interval confusion matrix (Fig. 6). Each contingency matrix quadrant indicates the minimum and maximum IEC 104 packets for correct predictions and errors.

The results from the confusion matrices are used to calculate values for the evaluation metrics (Table 4). The table represents the models' performance on all test folds for both approaches. Each row reports the average error rates—false negative rate (FNR) and false positive rate (FPR), along with mean detection ability in terms of macro-average F_1 score, Matthews correlation coefficient (MCC), and area under the receiver operation characteristic curve score, shortened as AUC score.



Baseline

	Predicted Normal Packets	Predicted Anomalous Packets
Actual Normal Packets (8389/8390)	7755 - 7865	524 - 635
Actual Anomalous Packets (485)	221 - 262	223 - 264

Endline

	Predicted Normal Packets	Predicted Anomalous Packets
Actual Normal Packets (8389/8390)	8126 - 8170	220 - 264
Actual Anomalous Packets (485)	0 - 4	481 - 485

Fig. 6 Resulting confusion matrices from 10x5 cross-validations of one-class SVM for anomaly detection on IEC 104 test sets for baseline and endline approaches

Table 4 Baseline and endline experimental evaluation results for IEC 104 protocol with unsupervised one-class SVM anomaly detection on cross-validated test folds

	FNR	FPR	F_1 score	MCC	AUC score
Baseline					
Minimum	0.453	0.062	0.643	0.303	0.694
Maximum	0.540	0.075	0.677	0.373	0.739
Average (SD)	0.492 (0.020)	0.068 (0.002)	0.663 (0.007)	0.344 (0.015)	0.719 (0.010)
Endline					
Minimum	0.000	0.026	0.884	0.790	0.980
Maximum	0.008	0.031	0.900	0.816	0.986
Average (SD)	0.003 (0.002)	0.028 (0.001)	0.891 (0.004)	0.802 (0.006)	0.983 (0.001)

SD: standard deviation

Baseline one-class SVM anomaly detection results for IEC 104 protocol data

Upon testing the detection ability of the approach with initial IEC 104 attributes (Table 4), the FNR lingers between 45% (0.45) and 54% (0.54), which indicates, on average, almost half of the anomalous IEC 104 packets (49%) are undetected. The FPR on average remained around 6.8%, i.e., out of approximately 8390 normal IEC 104 protocol packets in each cross-validation test fold, 524 - 635 frames were falsely categorised as anomalous.

The macro-average F_1 score of 0.6 for the given imbalanced IEC 104 communication shows the initial approach is separating the normal as well as anomalous IEC 104 packets poorly. Correspondingly, the average MCC (0.3) and average AUC (0.7) relay the same inefficiency of baseline one-class SVM anomaly detection models for the given IEC 104 protocol data.

Endline one-class SVM anomaly detection results for IEC 104 protocol data

For our evaluation, an FPR is satisfactory only when there is non-existent FNR and when the FPR remains lower than 5%. Both hold for our approach. The FNR remains between 0 and 0.8% throughout the cross-validation folds (Table 4). The average false alert rate reduced to 2.8% from the baseline average of 6.8%. The overall endline FPR is about 3%, i.e., 2% less than the threshold of 5%.

A good anomaly detector for this context should correctly isolate malicious IEC 104 protocol traffic and, at the same time, produce fewer false alerts. The macro-average F_1 score metric reflects this behavior of the detector. The macro-average F_1 score for all the folds remained above 0.88, indicating better performance than the baseline approach. The AUC score of 0.98 on average, shows the detector is skillfully discriminating the IEC 104 protocol packets in the given dataset. To understand the detection performance of correct predictions while considering the errors, FNR and FPR, we calculate MCC. The average MCC value of 0.8 depicts near perfect detection performance for the endline case.

Performance comparison results

The results are analysed with the Student t-test and reveal that baseline has a mean macro-average F_1 score of 0.6 and MCC of 0.3; and that endline have a mean macro-average F_1 score of 0.9 and MCC of 0.8. The p-value close to 0 indicates that the average performance of both approaches over 50 candidate models is not identical, failing to accept the null hypothesis at a 1% significance level.

We calculate the magnitude of difference between the performance of baseline and endline approaches with the help of Cohen's d test. The test is carried on macro-average F_1 scores and MCCs values. The test result indicates the existence of a large effect size of over 20 Standard Deviations between the two configurations of one-class SVM algorithm. Hence, we establish the endline anomaly detection for IEC 104 has significant improvement over baseline approach.

Discussion

When one-class SVM is applied to IEC 104 dataset (Egger et al. 2020) in an unsupervised setting, an AUC score of 0.49 (default algorithm setting) was reported (Table 5) and 0.64 (after parameter tuning) on unseen data when final cross-validated candidate models are used for training (Anwar et al. 2021). Also, both instances have ensued a meager correct classification rate (Anwar et al. 2021) and are plagued with prediction errors (Table 5). In comparison to the aforementioned previous work, this study presents an improved one-class SVM anomaly detection approach for IEC 104 protocol communication. The average cross-validated AUC score for endline approach is 0.98, higher than the average cross-validated baseline AUC score. Other associated metrics, FNR, FPR, and MCC, show similar trends and are relayed for comparative purposes. Crucial criteria to assess the anomaly detector's ability is to isolate suspicious IEC 104 protocol packets correctly and not miss any suspicious IEC 104 packets. Both criteria for the given context are crucial and are satisfied in the endline approach, providing an average TPR of 99.6% and an average FPR of 2%. The endline approach does not miss attack communications for some test folds, as seen from the FNR, i.e., the best among other values (Table 5).

The anomaly detection algorithm in the learning phase forms a boundary for the given data. The SVM hyperplane cannot form an optimal decision boundary because our training data is polluted (to replicate a real scenario). Having some sanitised data for the learning phase may reduce prediction errors. For example, the case of semi-supervised learning where prior knowledge about some datapoints is used to train the classifier. However, this additional processing may require more effort as compared to our approach.

Prediction errors require additional analysis, which can be a hassle in production anomaly detection systems. We perform a preliminary analysis on the 50th candidate

Table 5 Comparison of related one-class SVM anomaly detection results on 2 IEC 104 protocol datasets

		FNR	FPR	MCC	AUC Score
Dataset Egger et al. (2020)	Unsupervised learning^d Anwar et al. (2021)	0.98	0.03	−0.01	0.49
	Unsupervised learning^t Anwar et al. (2021)	0.69	0.01	0.30	0.64
Dataset Maynard et al. (2018)	Unsupervised learning^d (baseline)	0.49	0.06	0.34	0.72
	Unsupervised learning^d (endline)	0.00	0.02	0.80	0.98

Superscript *t* indicates tuned parameter setting

Superscript *d* indicates default parameter setting model of the endline approach to highlight how the approach can assist in further analysis of the anomalous IEC 104 packets. Further analysis reveals that the detected anomalous exchanges are mainly between four SCADA nodes. Two of the identified nodes, of which one is a MITM attacker, are transmitting information to a high-degree node (third node). The MITM attacker tries to synchronise clock times like other nodes, possibly RTUs. It goes undetected as the protocol does not verify senders. Upon interrogation request from the high-degree node (possible attack target), the attacker replaces the cause of transmission with invalid data and terminates the connection.

The second isolated node is a legitimate RTU but is separated as it demonstrates low participation in the network. Further analysis and opinion of domain expert are crucial to investigate the reasons behind low participation. If low participation is acceptable for the particular RTU, the analyst can ignore the identified node. This falsely identified SCADA node constitutes about 99.6% of the FPs in the last candidate model.

The rare participation behaviour can help detect reconnaissance attackers. We see that the endline approach separated the reconnaissance attacker (fourth node). Reconnaissance attack nodes are passively observing the network and can contribute to advance persistent threats (Assante and Lee 2015); hence, their isolation can potentially delay or disrupt the following attack sequence.

Due to the lack of new nodes appearing in the test sets, it is difficult to confirm or deny the detection performance of the approach. As an alternative, we intentionally added two new nodes such that they only appear in the test set. The communication frames were flagged as an anomaly due to their rare characteristic, for example, the absence of communicating nodes.

Conclusions

Graph-based attribute extension of SCADA network nodes with one-class SVM algorithm has the potential to isolate the rouge network nodes in IEC 104 protocol communication. The work extracts meaningful relations between the network nodes to model the behavior of the network. Consequently, the representation allows isolating strange nodes, e.g., passive intruders trying to ping neighbouring nodes. Since it is possible to classify a new instance immediately when it arrives without considering other instances, it is feasible to use the approach for active detection in real-time. We compare the potential of attribute extension by presenting baseline and endline results. The cross-validation models retain the highest average F_1 score (0.90), MCC (0.80), and AUC score (0.98), while giving modest false-alert and miss-rates in comparison to related works, as well as the baseline detection method.

Keeping miss-alerts and false-alerts to a minimum is crucial for deploying an anomaly detector for critical infrastructures. The endline results produce fewer errors overall. The missed-alerts are almost negligible, with a drastic drop in the false alerts, depicting a holistic boost in the endline method significantly over the baseline scores. Hence, through topological attribute extension of IEC 104 protocol features, one-class SVM can likely identify anomalies in the SCADA network.

One-class SVM is a popular choice for anomaly detection in communication networks (Tsai et al. 2009; Thakkar and Lohiya 2021; Rakas et al. 2020). Moreover, it demonstrated stable outcomes when assessed on a SCADA network communication dataset (Anwar et al. 2021). Future work will benefit by including other classifying methods, such as Auto-encoders or neural networks.

It is necessary to iterate that the approach is implemented and evaluated as an unsupervised learning method and that the detection models are created in the presence of routine and anomalous data. For future work, sanitised SCADA protocol attributes could be used for modelling the detector. We can also test the presented approach for similar isolated topological networks to identify eavesdroppers, for example, in the Modbus SCADA protocol.

Often attribute processing is dependent on human intervention, creating scalability concerns. The proposed approach relies on automatic extraction of attributes and, thus, is possible to be scaled. Notable advances are made towards graph embedding techniques and stacked auto-encoders to reveal hidden and intricate attributes, i.e., without manual effort, to model complex networks (Pourhabibi et al. 2020; Corizzo et al. 2021). For this reason, we expect that the acceptance of other methods to infer network behaviour will continue to grow.

Abbreviations

CI	Critical infrastructure
DNP3	Distributed network protocol 3
FNR	False negative rate
FPR	False positive rate
HMI	Human machine interface
ICS	Industrial control system
IDS	Intrusion detection system
IEC	International Electrotechnical Commission
IEC 104	IEC 60870-5-104
MCC	Matthews correlation coefficient
OSI	Open systems interconnection
ROC-AUC (or AUC)	Receiver operating curve area under curve
RTU	Remote terminal unit
SCADA	Supervisory control and data acquisition
SVM	Support vector machine
TCP/IP	Transmission control protocol/internet protocol
TPR	True positive rate

Acknowledgements
The authors would like to thank Henrik Johansson and Anders Karlberg at Techinova for sharing their domain knowledge.

Author contributions

Conceptualisation: MA and LL.; methodology: MA, AB and LL.; software: MA.; validation: MA, LL, AB; formal analysis: MA, AB and LL.; investigation: MA; resources: MA.; data curation, MA; writing—original draft preparation: MA.; writing—review and editing, MA, AB and LL.; visualization, MA, LL and AB.; supervision, LL and AB. All authors have read and approved the final manuscript.

Funding
Open access funding provided by Blekinge Institute of Technology.

Availability of data and materials

We utilise the dataset that is available under the following link: https://figshare.com/articles/dataset/dataset-v1_pcap/6133457/1

Declarations

Ethics approval and consent to participate

Not applicable.

Competing interests

The authors declare that they have no competing interests.

Received: 13 October 2022 Accepted: 9 December 2022
Published online: 21 December 2022

References

Akoglu L, McGlohon M, Faloutsos C (2010) Oddball: Spotting anomalies in weighted graphs. In: Zaki MJ, Yu JX, Ravindran B, Pudi V (eds) Advances in knowledge discovery and data mining. Pacific-Asia conference on knowledge discovery and data mining (PAKDD). Lecture notes in computer science, Vol 6119. Springer, Berlin, Heidelberg, pp. 410–421

Anwar M, Borg A, Lundberg L (2021) A comparison of unsupervised learning algorithms for intrusion detection in IEC 104 SCADA protocol. In: 20th International conference on machine learning and cybernetics (ICMLC), IEEE, pp. 1–8. https://doi.org/10.1109/ICMLC54886.2021.9737267

Assante MJ, Lee RM (2015) The industrial control system cyber kill chain. Technical report, SANS Institute InfoSec Reading Room

Chicco D, Jurman G (2020) The advantages of the Matthews correlation coefficient (MCC) over F1 score and accuracy in binary classification evaluation. BMC Genomics 21(1):6. https://doi.org/10.1186/s12864-019-6413-7

CISA (2016) ICS Alert (IR-ALERT-H-16-056-01). Cyber-attack against Ukrainian critical infrastructure; Cybersecurity and Infrastructure Security Agency. Cybersecurity and Infrastructure Security Agency (CISA).&nbsp;&nbsp;https://www.cisa.gov/uscert/ics/alerts/IR-ALERT-H-16-056-01. Accessed 9 May&nbsp;2022

Corizzo R, Ceci M, Pio G, Mignone P, Japkowicz N (2021) Spatially-aware autoencoders for detecting contextual anomalies in geo-distributed data. In: International conference on discovery science, pp. 461–471. Springer

Egger M, Eibl G, Engel D (2020) Comparison of approaches for intrusion detection in substations using the IEC 60870–5-104 protocol. Energy Inform 3(S1):1–17. https://doi.org/10.1186/s42162-020-00118-4

ENISA (2017) Communication Network Dependencies for ICS/SCADA Systems. European Network and Information Security Agency, Athens. https://doi.org/10.2824/397676

Flach P (2012) Machine learning: the art and science of algorithms that make sense of data. Cambridge University Press, Cambridge

Ferling B, Chromik J, Caselli M, Remke A (2018) Intrusion detection for sequence-based attacks with reduced traffic models. In: International conference on measurement, modelling and evaluation of computing systems, pp. 53–67. Springer

Gaggero GB, Rossi M, Girdinio P, Marchese M (2020) Detecting system fault/cyberattack within a photovoltaic system connected to the grid: a neural network-based solution. J Sens Actuator Netw 9(2):20. https://doi.org/10.3390/jsan9020020

Grammatikis PR, Sarigiannidis P, Sarigiannidis A, Margounakis D, Tsiakalos A, Efstathopoulos G (2020) An anomaly detection mechanism for iec 60870-5-104. In: 9th International conference on modern circuits and systems technologies (MOCAST), IEEE, pp. 1–4. https://doi.org/10.1109/MOCAST49295.2020.9200285

György P, Holczer T (2020) Attacking iec 60870-5-104 protocol. In: 1st Conference on Information Technology and Data Science (CITDS), pp. 140–150. http://ceur-ws.org/Vol-2874/paper13.pdf

Henderson K, Gallagher B, Eliassi-Rad T, Tong H, Basu S, Akoglu L, Koutra D, Faloutsos C, Li L (2012) Rolx: structural role extraction & mining in large graphs. In: 18th ACM SIGKDD International conference on knowledge discovery and data mining, pp. 1231–1239. https://doi.org/10.1145/2339530.2339723

Henderson K, Eliassi-Rad T, Faloutsos C, Akoglu L, Li L, Maruhashi K, Prakash BA, Tong H (2010) Metric forensics: a multi-level approach for mining volatile graphs. In: 16th ACM SIGKDD international conference on knowledge discovery and data mining, pp. 163–172. ACM, NY. https://doi.org/10.1145/1835804.1835828

Hodo E, Grebeniuk S, Ruotsalainen H, Tavolato P (2017) Anomaly detection for simulated IEC-60870-5-104 Trafiic. In: 12th International conference on availability, reliability and security, pp. 1–7. ACM, Reggio Calabria. https://doi.org/10.1145/3098954.3103166. Accessed 1 Jul&nbsp;2021

Lin C-Y, Nadjm-Tehrani S (2019) Timing patterns and correlations in spontaneous scada traffic for anomaly detection. In: 22nd International symposium on research in attacks, intrusions and defenses (RAID), pp. 73–88

Linda O, Vollmer T, Manic M (2009) Neural network based intrusion detection system for critical infrastructures. In: 2009 International joint conference on neural networks, IEEE,&nbsp; pp. 1827–1834

Mahmood AN, Leckie C, Hu J, Tari Z, Atiquzzaman M (2010) Network traffic analysis and scada security. Handbook of Information and Communication Security. Springer, Berlin, pp 383–405. https://doi.org/10.1007/978-3-642-04117-4

Matousek P (2017) Description and analysis of IEC 104 Protocol. Technical Report FIT-TR-2017-1, Faculty of Information Technology, Brno University of Technology, Brno, Czech Republic. https://www.fit.vut.cz/research/publication-file/11570/TR-IEC104.pdf

Matousek P, Ryšavý O, Grégr M (2019) Increasing visibility of iec 104 communication in the smart grid. In: 6th International Symposium for ICS & SCADA Cyber Security Research, pp. 21–30. https://doi.org/10.14236/ewic/icscsr19.3

Mantere M, Sailio M, Noponen S (2013) Network traffic features for anomaly detection in specific industrial control system network. Future Internet 5(4):460–473. https://doi.org/10.3390/fi5040460

Matousek P, Ryšavý O, Grégr M, Havlena V (2020) Flow based monitoring of ics communication in the smart grid. J Inf Secur Appl 54:1–16. https://doi.org/10.1016/j.jisa.2020.102535

Maynard P, McLaughlin K, Sezer S (2018) An open framework for deploying experimental scada testbed networks. In: 5th International symposium for ICS & SCADA cyber security research 2018, pp. 92–101. https://doi.org/10.14236/ewic/ICS2018.11

Panagiotis F, Taxiarxchis K, Georgios K, Maglaras L, Ferrag MA (2021) Intrusion detection in critical infrastructures: a literature review. Smart Cities 4(3):1146–1157. https://doi.org/10.3390/smartcities4030061

Pliatsios D, Sarigiannidis P, Lagkas T, Sarigiannidis AG (2020) A survey on SCADA systems: secure protocols, incidents, threats and tactics. IEEE Commun Surv Tutor 22(3):1942–1976. https://doi.org/10.1109/COMST.2020.2987688

Pourhabibi T, Ong K-L, Kam BH, Boo YL (2020) Fraud detection: a systematic literature review of graph-based anomaly detection approaches. Decis Support Syst 133:113303. https://doi.org/10.1016/j.dss.2020.113303

Radoglou-Grammatikis P, Sarigiannidis P, Giannoulakis I, Kafetzakis E, Panaousis E (2019) Attacking iec-60870-5-104 SCADA systems. In: IEEE World Congress on Services (SERVICES), IEEE, pp. 41–46. https://doi.org/10.1109/SERVICES.2019.00022

Rakas SVB, Stojanović MD, Marković-Petrović JD (2020) A review of research work on network-based scada intrusion detection systems. IEEE Access 8:93083–93108. https://doi.org/10.1109/ACCESS.2020.2994961

Robles-Durazno A, Moradpoor N, McWhinnie J, Russell G (2018) A supervised energy monitoring-based machine learning approach for anomaly detection in a clean water supply system. In: 2018 International Conference on Cyber Security and Protection of Digital Services (Cyber Security), IEEE, pp. 1–8. https://doi.org/10.1109/CyberSecPODS.2018.8560683

Schölkopf B, Williamson RC, Smola A, Shawe-Taylor J, Platt J (1999) Support vector method for novelty detection. In: 12th International conference on neural information processing systems (NIPS), pp. 582–588. MIT Press, Colorado. https://doi.org/10.5555/3009657.3009740. https://proceedings.neurips.cc/paper/1999/file/8725fb777f25776ffa9076e44fcfd776-Paper.pdf

Sullivan GM, Feinn R (2012) Using effect size-or why the p value is not enough. J Grad Med Educ 4(3):279–282. https://doi.org/10.4300/JGME-D-12-00156.1

Tariq N, Asim M, Khan FA (2019) Securing scada-based critical infrastructures: challenges and open issues. Proc Comput Sci 155:612–617. https://doi.org/10.1016/j.procs.2019.08.086

Thakkar A, Lohiya R (2021) A survey on intrusion detection system: feature selection, model, performance measures, application perspective, challenges, and future research directions. Artif Intell Rev. https://doi.org/10.1007/s10462-021-10037-9

Tsai C-F, Hsu Y-F, Lin C-Y, Lin W-Y (2009) Review: intrusion detection by machine learning: a review. Expert Syst Appl 36(10):11994–12000. https://doi.org/10.1016/j.eswa.2009.05.029

Udd R, Asplund M, Nadjm-Tehrani S, Kazemtabrizi M, Ekstedt M (2016) Exploiting bro for intrusion detection in a scada system. In: 2nd ACM international workshop on cyber-physical system security, pp. 44–51. ACM, Xian. https://doi.org/10.1145/2899015.2899028

Wong K, Dillabaugh C, Seddigh N, Nandy B (2017) Enhancing suricata intrusion detection system for cyber security in SCADA networks. In: 2017 IEEE 30th Canadian Conference on Electrical and Computer Engineering (CCECE), IEEE, pp. 1–5. https://doi.org/10.1109/CCECE.2017.7946818

Yang Y, McLaughlin K, Littler T, Sezer S, Pranggono B, Wang H (2013) Intrusion detection system for iec 60870-5-104 based scada networks. In: 2013 IEEE power & energy society general meeting, IEEE, pp. 1–5. https://doi.org/10.1109/PESMG.2013.6672100

Yang Y, Xu H-Q, Gao L, Yuan Y-B, McLaughlin K, Sezer S (2016) Multidimensional intrusion detection system for iec 61850-based scada networks. IEEE Trans Power Deliv 32(2):1068–1078. https://doi.org/10.1109/TPWRD.2016.2603339

Zhao Y, Nasrullah Z, Li Z (2019) Pyod: a python toolbox for scalable outlier detection. J Mach Learn Res 20(96):1–7

Zhu B, Joseph A, Sastry S (2011) A taxonomy of cyber attacks on scada systems. In: 2011 International Conference on Internet of Things and 4th International Conference on Cyber, Physical and Social Computing, IEEE, pp. 380–388. https://doi.org/10.1109/iThings/CPSCom.2011.34

Publisher's Note

Springer Nature remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.