FINGERPRINTING CYBER PHYSICAL SYSTEMS: A PHYSICS-BASED APPROACH

A Thesis
Presented to
The Academic Faculty

by

Preethi Srinivasan

In Partial Fulfillment
of the Requirements for the Degree
Masters of Science in the
School of Electrical and Computer Engineering

Georgia Institute of Technology
August 2015

FINGERPRINTING CYBER PHYSICAL SYSTEMS: A PHYSICS-BASED APPROACH

Approved by:

Dr. Raheem Beyah, Advisor
School of Electrical and Computer Engineering
Georgia Institute of Technology

Dr. John Copeland
School of Electrical and Computer Engineering
Georgia Institute of Technology

Dr. Jonathan Rogers
The George W.Woodruff School of Mechanical Engineering
Georgia Institute of Technology

Date Approved: July 24, 2015

Dedicated to my father C. Srinivasan, mother Kalyani Srinivasan, fiancé Shream Sundarrajan, brother Srivatsan Srinivasan and aunt Dr C.Vijayalakshmi

Specially dedicated to my Grandparents

Thank you for your love, support, prayers, trust and patience

ACKNOWLEDGEMENTS

I would like to express my special appreciation and thanks to my advisor and committee chair Professor Dr. Raheem Beyah. I have been fortunate enough to have an advisor who gave me freedom to explore my research domain on my own and at the same time provided guidance to recover whenever I stumbled because of a roadblock. During all our meetings he listened to my ideas, commeneded me for them and chaperoned me towards implementing the same. I will be forever indebted to his support and guidance without which my research would not have completed successfully.

I am also thankful to Ms. Yamille Del Valle and Mr. Kerry C Mills from NEETRAC for all their help in providing support to develop a test bed to perform my emprical tests.

I would like to thank Mr.Mike McCoy for his constant availability and for taking time to clarify questions about SEL relay operation.

I would like to thank Dr. John Copeland and Dr. Jonathan Rogers for agreeing to serve in my thesis committee. I am also thankful for their suggestions and comments on my thesis work.

I would like to specifically acknowledge and thank my research group partner David Formby for his constant support, advice and comment throughout the tenure of my research.

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

SUMMARY

Industrial Control System (ICS) networks used in critical infrastructure networks like the power grid represent a different set of security challenges when compared to traditional IT networks. The electric power grid comprises several components most of which are critical physical devices and have to be safeguarded to ensure reliable operation. The devices in the field are remotely controlled via the control network of the plant from the control center. The distributed nature of these networks makes it almost impossible to perform the same common security practices as done in traditional IT networks (e.g., regular security upgrades). It is partially due to the fact that these legacy devices are incapable of supporting future upgrades and because of the remote location of these devices. Cyber attacks on an electric grid can originate from an external intruder who has gained access to the control network or from a disgruntled employee who already has access to the network. Among several possible attacks on an electric grid, this work specifically proposes to tackle the false data injection issue during control command requests to the field devices in the substation. The thesis work proposes to help to ensure the authenticity of the responses by analyzing the observed response against the fingerprints developed by operation times associated with each device in the plant. Also, in this work, the accuracy of the proposed fingerprinting technique is evaluated from a dataset generated from controlled lab experiments.

CHAPTER I

INTRODUCTION

The smart grid is an extension of the traditional electrical power grid because of the connection of various subsystems of the grid distributed over different geographical areas by modern communication components to form a complex Cyber Physical Systems (CPS). Current research in CPS ranges from exposing the absence of security practices and policies in operator environments that affects the data integrity of the information in the grid system; to identifying protocol vulnerabilities inherent in control networks. A new research direction in the security domain for CPS is to look at the effect of these vulnerabilities on operational reliability and physical infrastructure. It is important to assess these effects because in addition to resulting in damage to physical equipment it might result in injury or loss of life.

Most protocols in control environments were not designed with consideration for security. Even with the introduction of a security layer as a part of the protocol stack, the possibility of physical system compromise was not completely eliminated, necessitating Deep Packet Inspection (DPI) to analyze the application layer payload. Even though several techniques have been proposed using DPI to identify malicious commands and false data in the grid system, their efficiency depends on information collected from all the subsystems at the time of analysis. In addition to ensuring the efficiency of the Intrusion Detection System (IDS), the technique proposed should also guarantee the real time requirements of the grid operation environment. Thus having complex methods of identifying intrusions might not always be the best solution for security in a smart grid.

The attacks on a grid subsystem are not always from an external malicious intruder attacking the system, but it might be an insider attack or an operator inadvertently issuing a command. Example consequences of such an intrusion can result in blackouts in the power grid [1] and environmental disasters like waste water sewage, oil and natural gas spillage [2] which is disastrous for both human life and the environment together. False injection of command and data are entirely possible in the electric grid. Several cryptographic solutions are currently available to identify intrusions into the IT networks but the same is not feasible in Industrial Control System (ICS) networks. Most of the legacy equipment available cannot be upgraded to the latest firmware to support these solutions due to their remote location and in some cases they do not even support such an upgrade. For example, previous research by our group found vulnerabilities in several power system devices and when they were reported to ICS-CERT, the resulting official advisory for one of the products stated that “There is no method to update [Schneider Electric SAGE RTUs] devices released prior to October 2014 ”[3]. Moreover, online upgrades of these equipment are impossible due to their critical nature of these equipment and temporarily suspending their functionality will result in unreliable operation of the plant. Due to these concerns, it is imperative that alternative methods like fingerprinting be used to ensure security and to provide intrusion detection.

The proposed work discusses a novel passive fingerprinting technique using the control messages in the ICS networks to generate signatures. This mainly relies on the fact that even though devices from two different vendors are similarly rated, the variations in physical characteristics will produce a unique physical response and behavior from each device. This fingerprinting is unique due to its ability to construct signature from the attributes dependent on physical characteristics of each device which can be further extended to a new domain of fingerprinting called “white box modeling” approach. An evaluation of this fingerprinting approach in a simple forgery attack is also summarized in this thesis work.

CHAPTER II

BACKGROUND

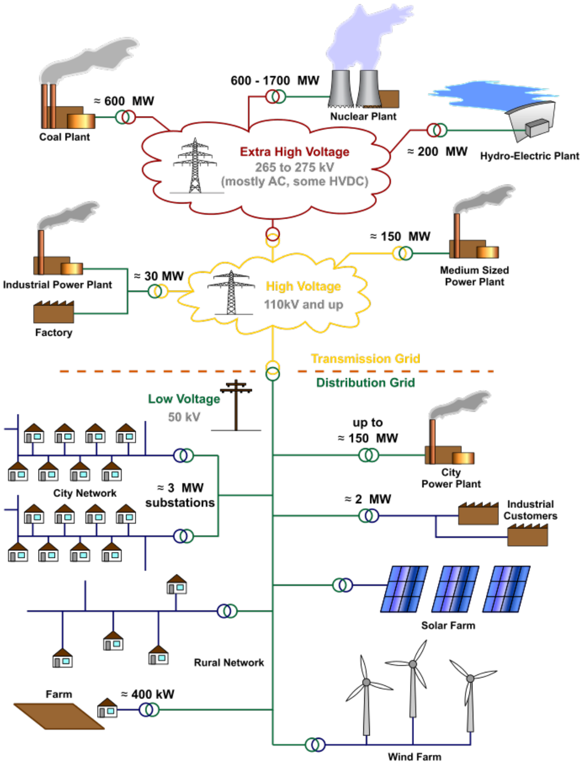
This section provides insight into Cyber Physical System (CPS) and its components. It also provides details of existing fingerprinting approaches and the proposed new modeling approach for signature generation.

2.1 Physical System in a Power Grid

An electrical grid (or a power grid) is an interconnected network for delivering electricity from suppliers to customers. It consists of generating stations that produce electric power, high-voltage transmission lines that carry power from distant sources to demand centers, and distribution lines that connect individual customers. A general layout of the electrical grid is shown in Figure 1.

2.2 Cyber System in a Power Grid

Over the years, the electric grid which contained only physical components transformed into a CPS containing both cyber and physical components. By utilizing modern information technologies, the electric grid is now capable of delivering efficient power by responding to a wide range of commands and events. Supervisory Control and Data Acquisition (SCADA) is a system that supports remote monitoring and control of various subsystems in a grid over communication channels through industrial protocols like DNP3, IEC61850, Modbus etc. SCADA system architecture has evolved over the years from a monolithic architecture to networked distributed architecture as shown in Figure 2. In the networked distributed architecture, complex SCADA system components are connected through standardized communication protocols, increasing the reliability and performance of the system. The various

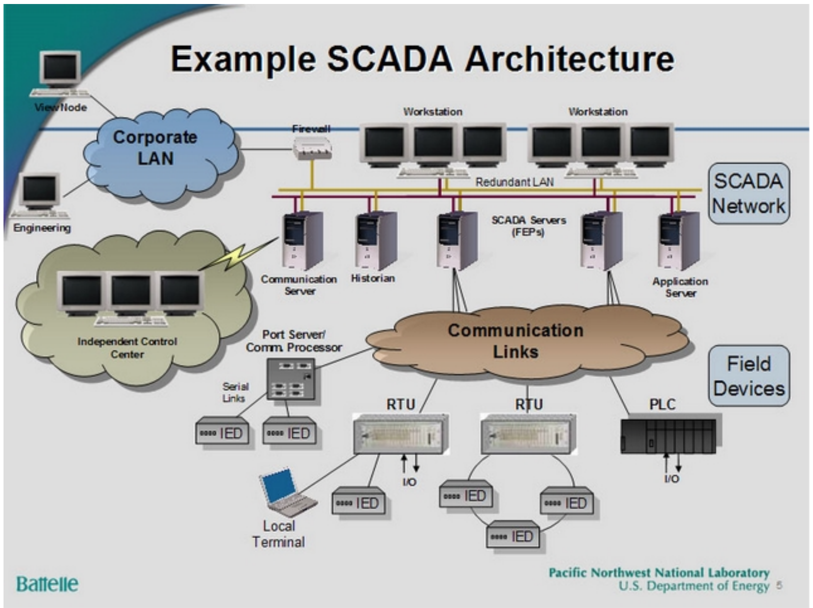


Source: [4]

Figure 1: A general electric grid layout

components of the SCADA systems are:

- PLC - Programmable Logic Controllers (PLC) or control master is a microprocessor based device used in the SCADA system to control the physical elements in the field.
- IED - Intelligent Electronic Devices (IED) are used in the power grid to provide a level of abstraction between actual physical equipment like circuit breakers in the field and the control master. The IEDs are digital devices used to monitor and control the breakers from the control master remotely.
- Historian - A Historian is a software service that accumulates time stamped boolean alarms, commands and events in a database which can be queried or used to populate graphic trends in the graphical interface. The historian client is used to access the historian server for data.
- RTU - Remote Terminal Units exist between control centers and end devices like IEDs to aid in data accumulation before transmitting the same to the control master.



Source: [5]

Figure 2: SCADA architecture

SCADA systems are equipped with cyber systems as mentioned above to monitor and control the field equipment. Usually IEDs are available at the last level in cyber system which communicates with the field equipment like circuit breaker, transformer, generator, motors etc. Monitoring and control messages flow between the master devices like PLCs and IEDs which act like slave devices. So the goal of the proposed technique in this thesis is to secure these control messages which can be falsified by performing a man in the middle attack.

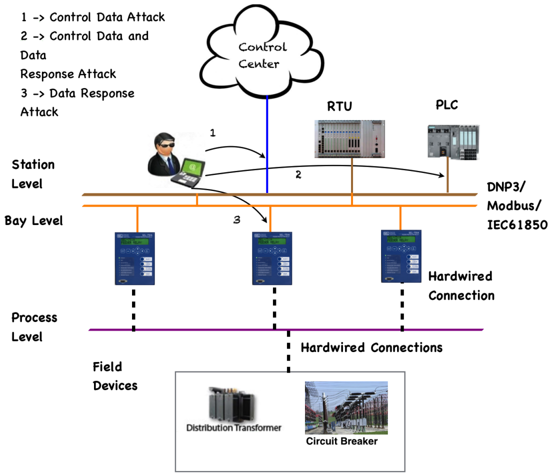


Figure 3: Substation network with attack points

Figure 3 illustrates a portion of the substation in the entire SCADA system to demonstrate the points of attack insertion. This includes Point 1, where the attacker can provide falsified control messages between the control center and the substation remote terminal unit (RTU); Point 2, where the attacker can provide falsified control messages between the RTU and IEDs, and Point 3 where the attacker can provide false data at the field devices like a circuit breaker etc. In this thesis, the case of falsification of data at Point 3 is assumed as the attacker's goal and authentication through device fingerprinting is provided to identify the intrusion.

2.3 Circuit Breaker

There are several types of field equipment in an electric grid, however in this work we focus on the circuit breaker to demonstrate the feasibility of the idea. A circuit breaker is a special switch which does the making and breaking of a circuit while carrying high current. The circuit breaker consists of a fixed contact and a moving contact. In the "Closed" condition state, the two contacts are connected and current flows. The breaker arrangement contains stored potential energy which when released aids in closing the contacts. Usually this potential energy is stored by deforming a metal spring by compressed air or by hydraulic pressure. All circuit breakers are equipped with closing coils and whenever this coil is energized, it dispatches the plunger releasing the potential energy. The plunger converts the stored potential energy into kinetic energy to move the contacts. The operating characteristic curve of the breaker is shown in Figure 4.

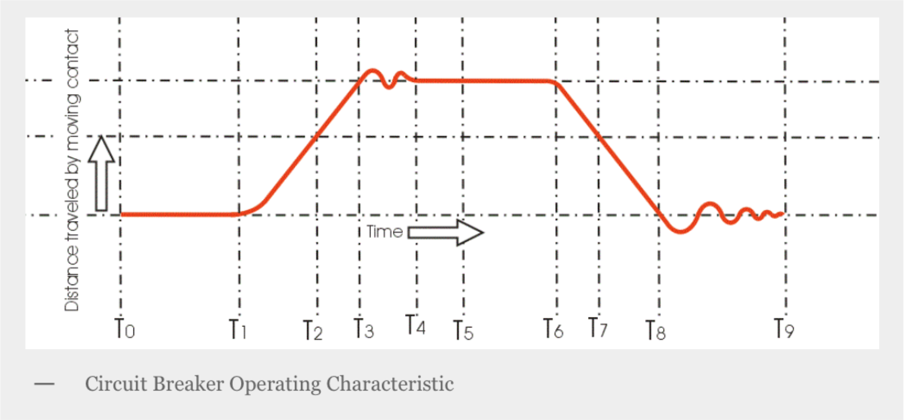


Figure 4: Operation characteristics of circuit breaker

2.3.0.1 Closing Operation

1. At time T0, current starts flowing through the closing coil.

2. Between time T0 to T1, the moving contact of the breaker starts moving towards the fixed contact.

3. From time T1-T3, the moving contact has travelled the gap distance and has touched the fixed contact.

4. The small distortion over the period T3-T4 shows the bounce back distance of the moving contact after it touches the fixed contact.

5. By the start of T4, the breaker has moved into closed position.

2.3.0.2 Tripping Operation

1. At time T5 current starts flowing through the tripping coil.

2. At time T6 the moving contact starts moving away from fixed contact.

3. By the end of time T8 the moving contact returns to its beginning position.

4. During time T8-T9 the moving contact oscillates due to the inertia of the moving contact before settling down.

5. At time T9 the moving contact finally reaches the rest position.

In order to generate a signature for each device, the operation time for *OPEN/CLOSE* commands of a circuit breaker are considered. Circuit breakers exist in all voltage ratings from 110V to 220kV but are too dangerous and costly to experiment with in lab. Hence, in this work we decided to use a latching relay to simulate the operations of a circuit breaker.

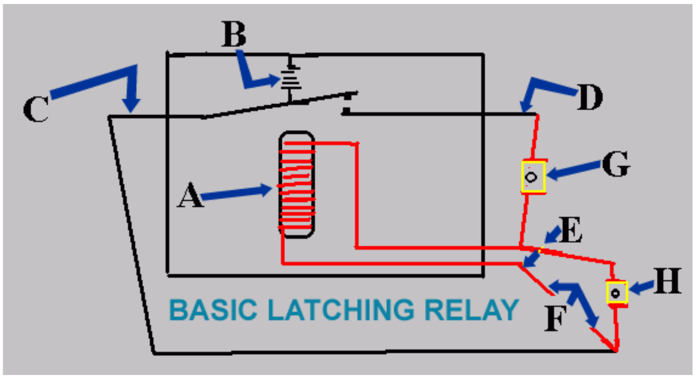
2.3.1 Latching Relay Operation

The latching relays are also referred to as “holding circuits”. Figure 5 shows the connection diagram of a generic latching relay. It contains

- *A* - Electromagnet

- *B* - Spring to retract the contact when the magnet is not energized

- *C & D* - Controlled circuit, on when the magnet is energized and off when the magnet is not energized
- *E* - Power to energize the electromagnet
- *F* - Trigger power source
- *G* - A push to disconnect button, normally is always on unless actually pushed, will reconnect when you let go of the button
- *H* - A push to connect switch, only connects the circuit when pressed, when you let go of the button, the connection is broken



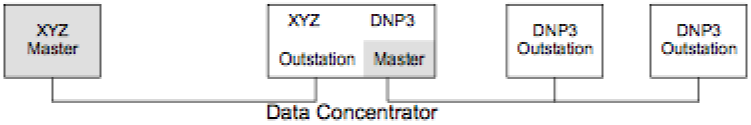
Source: [6]

Figure 5: Latching relay circuit

Pushing the button *H* will energize the electromagnet and close the load contacts in the relay, which will then stay latched after the *H* button is released because the load contacts have now provided another route to complete the trigger power for the electromagnet. To unlatch, the *G* button is pushed which will cut the trigger power and unlatch the relay. A slight modification of this type of relay is one that has a wiring configuration with multiple sets of contacts within them where, one set of latching contacts would be used for the latching circuit and another isolated set of load contacts would be the actual relay for an independent circuit.

2.4 DNP3 Protocol

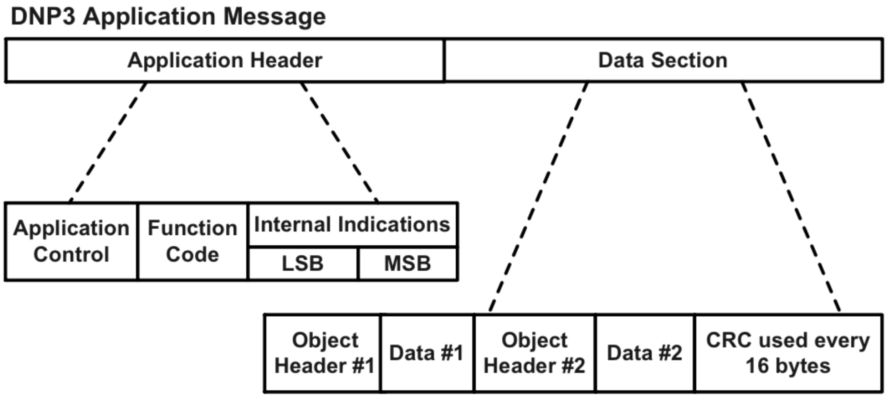
SCADA architectures rely on a communication model with multiple protocol layers to counter noise and signal distortion. Of the several legacy protocols, DNP3 was developed by Westronic Inc. in early 1990s. DNP3 was designed to optimize the transmission of data commands and data status between DNP3 devices. It is not a general purpose protocol like those found on the Internet for transmitting email, hypertext documents, SQL queries, multimedia or large files. In the SCADA environment, the DNP3 protocol is used to exchange control and event messages between master and the slave equipment. DNP3 supports unicast transactions between the DNP3 master and outstation devices, where the master sends a request message to an addressed outstation slave, which responds with a reply message. DNP3 supports different network configurations and the most common configuration is the "multi-drop" configuration where one master communicates with multiple outstations as shown in Figure 6.



Source: [7]

Figure 6: DNP3 multi-drop architecture

The DNP3 protocol has a physical layer for transmitting messages over a wired copper or fiber physical network. The data link layer provides reliable communication between devices to facilitate transfer of Ethernet frames. The link layer functionality is similar to link layer in the TCP/IP protocol stack. The pseudo-transport layer in the DNP3 protocol stack helps with fragmentation and reassembly. The application layer contains request and reply messages which define the role of the device i.e., master or outstation device. A request message comes from the master to a slave device to perform a write, collect and provide data or perform time synchronization. The messages from the application layer can be solicited/polling-based or unsolicited messages.



Source: [7]

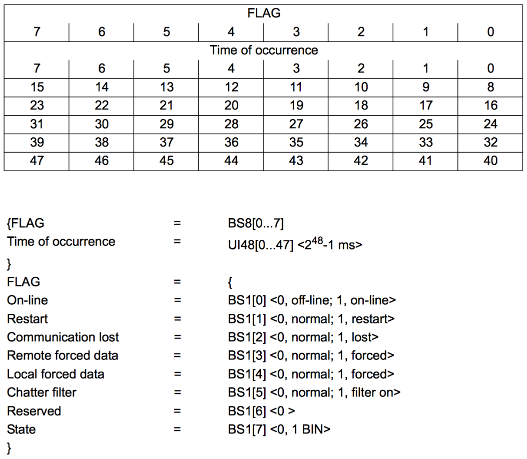
Figure 7: DNP3 application layer message structure

Figure 7 shows the application layer message format. The control field in the application header specifies a sequence number which is necessary for reassembly. The function code indicates whether the message is a request message or a reply message which uses internal indications to show if it is a confirmation message or a response message. The payload of the application layer message carries the data objects in form of binary outputs, analog inputs, analog outputs, binary inputs and counters.

2.4.1 DNP3 Event

DNP3 events are used to indicate important status changes in the field. The DNP3 protocol specifies the usage of an event buffer, but leaves its implementation to vendors. There are two types of event buffers that are available in DNP3 slave devices: Sequence Of Event (SOE) and Most Recent Event (MRE). The former type stores all received data in the event buffer and every new event is appended to the event buffer. The latter type stores the most recent event and the newly arrived data overwrite the previous data. Each DNP3 slave device is programmed to respond in one of the two modes: event Polling and unsolicited Response. The former mode involves the master periodically polling the slave devices in a round robin fashion. The latter mode involves the slave automatically responding to the master with its event changes during a critical event change. The DNP3 frame in the application layer contains information about type of event, value of event, event index, time stamp of the event, event variation and event class. Among all the binary event types in this thesis we specifically concentrate on binary input with time stamps. The change of binary input with time stamps is used to represent the changed state of the digital input as observed at the field device. It also indicates the status point as follows:

- The on-line bit indicates that the binary input point has been read successfully. If this field is set to off-line, the state of the digital point may be incorrect.
- The restart bit indicates that the field device that originated the data object is currently restarting. This device may be the device reporting this data object.
- The communication lost bit indicates that the device reporting this data object has lost communication with the originator of the data object.
- The remote forced data bit indicates that the state of the binary input has been forced to its current state at the device other than the end device.
- The local forced data bit indicates that the state of the binary input has been forced to its current state at the end device.
- The chatter filter bit indicates that the binary input point has been filtered in order to remove needless transitions in the state of the point.
- The state bit indicates the current state of the binary input point.
- The time of occurrence indicates the absolute time at which the end device detected the change of state. The accuracy of this time will depend on the accuracy of the individual device. Time of occurrence is recorded as milliseconds since midnight, January 1st, 1970, at zero hours, zero minutes, seconds and milliseconds. The format of a DNP3 event message encoding is shown below in Figure 8.



FLAG							
7	6	5	4	3	2	1	0
Time of occurrence							
7	6	5	4	3	2	1	0
15	14	13	12	11	10	9	8
23	22	21	20	19	18	17	16
31	30	29	28	27	26	25	24
39	38	37	36	35	34	33	32
47	46	45	44	43	42	41	40

{FLAG	=	BS8[0...7]
Time of occurrence	=	UI48[0...47] <2^{48}-1 ms>
}		
FLAG	=	{
On-line	=	BS1[0] <0, off-line; 1, on-line>
Restart	=	BS1[1] <0, normal; 1, restart>
Communication lost	=	BS1[2] <0, normal; 1, lost>
Remote forced data	=	BS1[3] <0, normal; 1, forced>
Local forced data	=	BS1[4] <0, normal; 1, forced>
Chatter filter	=	BS1[5] <0, normal; 1, filter on>
Reserved	=	BS1[6] <0 >
State	=	BS1[7] <0, 1 BIN>
}		

Source: [7]

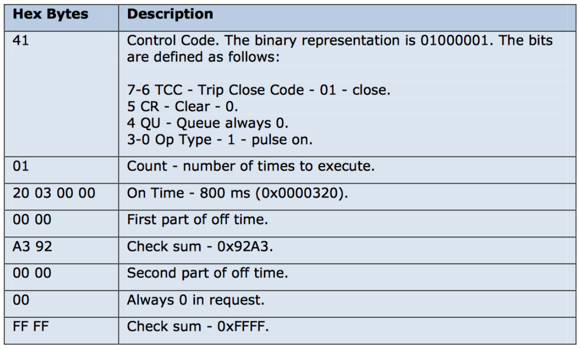
Figure 8: DNP3 event message encoding

2.4.2 DNP3 Control Command

DNP3 control commands provides binary output points that are used to provide level high or pulse signals to control output devices such as breaker. The DNP3 master issues control commands to the DNP3 slave in order to operate the breaker. The binary output commands are classified as:

- Single point output with 0 de-energizing latch coil (open) and 1 energizing latch coil (close).
- Double binary output with 01 energizing reset coil (open) and 10 energizing latch coil (close).

Figure 9 shows the data object of the packet transmitted by the DNP3 Master. The Control Code indicates trip/close signal in bits 6 and 7. Bit 1 indicates sending a pulse signal and bit 5 indicates clearing the latched signal in case of a level signal. Count indicates the number of pulses to be sent to the breaker. For each pulse, on time period and off time period are also chosen according to the rating of the breaker involved.



Hex Bytes	Description
41	Control Code. The binary representation is 01000001. The bits are defined as follows: 7-6 TCC - Trip Close Code - 01 - close. 5 CR - Clear - 0. 4 QU - Queue always 0. 3-0 Op Type - 1 - pulse on.
01	Count - number of times to execute.
20 03 00 00	On Time - 800 ms (0x0000320).
00 00	First part of off time.
A3 92	Check sum - 0x92A3.
00 00	Second part of off time.
00	Always 0 in request.
FF FF	Check sum - 0xFFFF.

Source: [8]

Figure 9: Transmit data object

The DNP3 slave device is an IED which in turn sends a signal to operate the breaker. This signal is a hardwired signal and the time it consumes is in order of nanoseconds. There are two types of binary control commands namely: direct operate and select before operate.

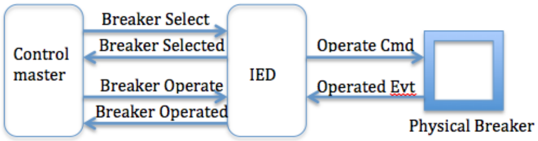


Figure 10: Two step select before operate

- Direct Operate - In this type of command, the master sends a command to the slave device to operate the breaker without a prior selection of the breaker for operation.

- Select Before Operate - In this type of command, the master sends a command to the slave device to operate the breaker in a two step process as shown in Figure 10.

In this work, we demonstrate the proposed idea through the direct operate command for both open and close. The completion of the field device's operation is indicated in the form of a hardwired signal to the DNP3 slave. The slave then responds back to the master via an unsolicited response or polling based response depending on the configuration. It is redundant to observe both the responses because as soon as the DNP3 slave sends the unsolicited response for a binary event change, a polling request to identify the binary event change will not receive a response packet as the event change has already been recorded. So in this work, unsolicited response is chosen to observe the event changes.

2.5 Fingerprinting

Device fingerprinting usually requires the collection of information from a remote computing device for the purpose of unique identification of the device. This is a well researched topic with several solutions already proposed. There are two types of fingerprinting techniques: passive and active. Active fingerprinting assumes that the fingerprinted device will tolerate some amount of invasive probing through crafted packets. Even though this solution has been in use for a very long time it is not suitable for the ICS environment. This is because ICS devices perform critical functions and active probing could potentially crash the device. So, it is preferred to use passive fingerprinting which is implemented by observing the packet communications between devices. This is usually done based on factors such as OS implementations of TCP/IP protocol stack, IEEE 802.11 (wireless) device driver implementation and hardware clock skew. This thesis proposes to extend the passive fingerprinting technique to ICS environment to fingerprint the field equipment in the grid systems.

The signature of a device is obtained by collecting the response times of the circuit breaker and representing these operation times as a probability density function (PDF). The signature of the devices can be obtained in one of the three methods: white box, black box and gray box modeling. In a black box approach, the PDF is constructed strictly from empirical data without any prior model and hence requires a large amount of measurements to construct the signature. This modeling approach is the common method used by all previous fingerprinting work. In a white box model, the PDF is constructed by building the device model through data sheets and CAD drawings of the device. This model is simulated and parameters are varied to create a PDF using uncertainty distributions. In a gray box approach, it takes the characteristics of both black and white box modeling to create a PDF. In this case uncertainty in white box modeling is improved by the experimental observations from black box modeling. This thesis proposes the usage of black box modelling to develop a signature for latching relays between two vendors but the underlying idea to develop signature using physical properties helped in creation of “white box model” as explained in [9].

CHAPTER III

RELATED WORK

Cyber Security in control systems became an important topic of research when a piece of malware called “Stuxnet” took advantage of “day Zero” vulnerabilities in Windows and targeted Industrial Control Systems (ICS) in uranium centrifuges in Iran. Related works such as [10] and [11] expose the attack model of Stuxnet and the extent of damage it caused in control systems, emphasizing the need for cyber security in SCADA and control systems. Later, works like [12], [13], [14], [15], [16], [17], and [18] provided a comprehensive overview of the various vulnerabilities and potential threats to SCADA systems. They call attention to the differences in the network architecture of SCADA systems from the standard IT systems and highlighted the set of security goals that need to be achieved to prevent physical damages to the subsystems. Wang et al. in [19] and Cardenas et al. [20], in addition to shedding light on security requirements and network vulnerabilities, also provide attack countermeasures to ensure smart grid security. They provide attack models targeting basic security objectives such as availability, integrity and confidentiality.

Even though the NERC standard provides security requirements for SCADA systems similar to standard IT systems, traditionally used signature-based intrusion detection is not a very viable option for cyber security in grid environments as there are not many registered signatures of attacks for smart grids. Instead, anomaly and specification-based intrusion detection systems seem more feasible solution for smart grids since the electrical systems have static predictable topology, a regular traffic pattern and a fixed set of legacy protocols.

Verba in [21] implemented a flow based intrusion detection technique using deep packet inspection and network traffic pattern matching to identify packet tampering. In this technique, man in the middle attacks caused by compromising an Application Server (AS) and Front End Processor (FEP) is detected by analyzing the network flow traffic pattern. Cheung et al. in [22] proposed a model based IDS for the Modbus TCP protocol. In their paper, the expected communication pattern was used to create protocol level models for characterizing requests and responses based on Modbus guidelines. Any deviation from this model was predicted to be an anomaly. Two main disadvantages prevented the model based approach to be widespread: the first one being its complexity in constructing models for proprietary implementations of protocols and the second one being the larger number of false alarms. To confront these challenges, the specification based intrusion detection technique was introduced which is similar to anomaly based techniques except it uses a manually specified model. The challenge in identifying features for making the perfect specification model was overcome by the introduction of data mining to extract features from the large volume of previously collected traffic. Sekar et al. in [23] proposed a specification based IDS by using state machine specifications of network protocols and information statistics to detect anomalies. The difference between previously proposed IDS techniques and the one proposed in [23] is to not rely on expert identification of network protocol features but to rather rely on protocol state machine specifications to detect intrusions. A prototype specification based intrusion detection system framework based on Bro to verify that semantics of data extracted from network packets conform to protocol definitions was proposed in [24].

A Neural Network based IDS proposed in [25] specifies a window based feature vector capture to accurately depict the trends and pattern of the packet stream. A specific combination of neural network learning algorithms helps in identifying the deviation from normal behavior. The work uses packet characteristics to detect abnormal network traffic in SCADA systems. More related data mining works in cybersecurity [26] demonstrate the usage of data mining techniques to detect SYN flood attacks and buffer overflow attacks in SCADA systems. In their paper, data set is collected based on attributes of the attack and several data mining methods were run based on Waikato Environment for Knowledge

Analysis (WEKA) to detect intrusions.

Two very common control protocols are Modbus and DNP3. DNP3 is open source and more often used in power related environments. The DNP3 group released an application note on validation of incoming DNP3 data through numerous checks of components as specified in the IEEE Std. in [27].

Samuel East et al. in [28] detailed the attacks possible in different layers of the DNP3 protocol stack including the application layer. These attacks target specific vulnerabilities in the DNP3 protocol stack and demonstrates how these vulnerabilities can be exploited. Dongsoo et al. in [29] have successfully created a cyber security testbed for DNP3 man in the middle attacks and Jin et al. in [30] successfully demonstrated attacks on the DNP3 event buffer with unsolicited messages.

Understanding the security concerns in a smart grid requires a deeper inspection of cyber-physical interactions to quantify attack impacts on physical systems and checking if the counter measures proposed are effective or not. Even though specification based IDS technologies proved to be a more viable option towards protecting the SCADA systems, it is not adequate to ensure reliable operation in a distributed coordinated attack. Power System physics like Ohm's and Kirchhoff's laws along with state estimation that are used to operate and monitor the power grid have been used to provide security by filtering the bad measurement values in energy management systems [31], [32]. A recent work [33] on the same thought process highlighted vulnerabilities of bad detection of state estimation in well constructed byzantine data injection attacks that provide physically valid measurements. Cardenas et al. [34] studied vulnerabilities in SCADA controllers to network attacks in process control systems. In their paper, they show how by incorporating knowledge of the physical system under control, network attacks changing the behavior of control systems can be detected. Their work was one of the first novel IDSs considering physical operation within the perimeter of the plant for potentially damaging commands rather than only cyber attacks. Lin et al. in [35] proposed to combine both cyber and physical infrastructure in the power grid to help to estimate consequences of control commands, thus to reveal an attacker's malicious intentions. Parvania M. in [36] specifies the usage of states of the control environment and the physical operation states as a baseline reference and detects the abnormality in operation to reflect an attack. It relies on monitoring specific physical operations in the electrical grid system and using an ordered sequential pattern of information exchange to identify abnormal patterns. Robert M. et al. in [37] proposed specification based behavior rules for intrusion detection systems derived from control loops which tie intrusion detection to critical rules in the physical system. Maarten Hoeve in [38] proposed detecting intrusions in encrypted control traffic. The approach searches for a series of packets based on edit distance from appropriate string matching, to recognize known insertions and alert on unknown insertions.

One of the well known fingerprinting tools is "NMap"[39] which employs an active fingerprinting technique to identify OS and server versions running on a machine based on how the end device responds. An example of an open source passive fingerprinting tool is "p0f" which examines TCP and HTTP header fields to determine information about a remote computing device such as OS and browser version [40]. The first attempt at formalizing methods for active and passive fingerprinting of network protocols was published in 2006, where authors used parameterized extended finite state machine (PEFSMs) to model the behavior of different protocol implementations [41]. Kohno et al. in [42] used TCP timestamps to detect individual clock skew to perform device fingerprinting. Devices in the ICS environment are static in nature and does not change over the period of time, thus making it feasible to perform device fingerprinting. This helps in identifying any device in the network that does not belong to the ICS network. Gao et al. in [43] performed device fingerprinting using wavelet analysis on passively observed traffic to fingerprint and identify the access point in the network. The wavelet analysis was designed and tested only on wireless access points under heavy loads, a scenario that does not occur in ICS where wired communication is preferred for its reliability. So the same technique might not be practical for ICS. Francois et al. in [44] used models of timing of a device's implementation of application layer protocols using Temporal Random Parameterized Tree Extended Finite State Machines (TR-FSMs). While using the finite state machines a large database of all sessions are needed and all possible states should be mapped. This is not fully feasible because the ICS environment is interactive in nature thus increasing the non-determinism and hence number of states in the finite state machine. In another work Ureten et al. in [45] proposed device fingerprinting by observing the inter arrival packet time (IAT) to identify devices and device types. This seems feasible, but to achieve reasonable accuracy it needs large number of observations. This is not always possible in ICS environments due to the large polling period and hence a different fingerprinting method with fewer samples is a better choice. Another unique approach to passive device fingerprinting relevant to the proposed work concerns the network physical layer communication. Ureten in [46] used amplitude and phase measurements of the signals generated by Wi-Fi radios to identify individual devices. This may have been the first work to use physical measurements to fingerprint devices, but it still is not feasible in ICS networks where Wi-Fi devices are rarely used. The fingerprinting method proposed in this thesis provides higher accuracy than previously proposed techniques and is more suited for ICS networks. It is different from the previous techniques in the notion that it extends the idea of physical layer fingerprinting to identifying ICS field and control devices based on reported timings of their physical operations. The goal of the proposed technique is not to be exclusively used in the ICS environment but rather provide a "defense in breadth" by augmenting existing IDS techniques which have been already researched for ICS networks. Its independent nature in terms of protocol allows it to be utilized in most ICS networks to enable accurate detection of falsified control messages.

CHAPTER IV

PROPOSED RESEARCH

Cyber security has been identified as a critical issue for successful and reliable operation of the power grid. The power grid consists of several critical physical devices which have to be safeguarded. Most of these devices are remotely controlled thus giving rise to many potential vulnerabilities. Cyber attacks on a substation can originate from a malicious intruder outside the substation, an insider who already has access to the substation network or from an operator who inadvertently issues a command. This thesis work discusses the proposed technique to protect electric grid from failure during malicious control message injection but this could be easily extended to several ICS networks.

4.1 Threat Model and Assumptions

One unique feature of ICS network is its distributed nature thus providing a vast attack surface that needs to be secured. For example, the electric utility which provided experimental data to analyze and characterize ICS network for research purposes covers an area of *2800 square miles with 35 substations*, where each point of entry to the network is an attack point. This vast surface makes it almost impossible to protect and thus an attacker attacking the surface can be a disgruntled insider with legitimate access or an outsider who has gained access into the target network as shown in Figure 11.

The attack model for the proposed idea is demonstrated using DNP3 based circuit breaker operation in Figure 12. During normal operation the following sequence of operation is observed.

- The DNP3 master device sends a *CLOSE/OPEN* command to the DNP3 slave device.

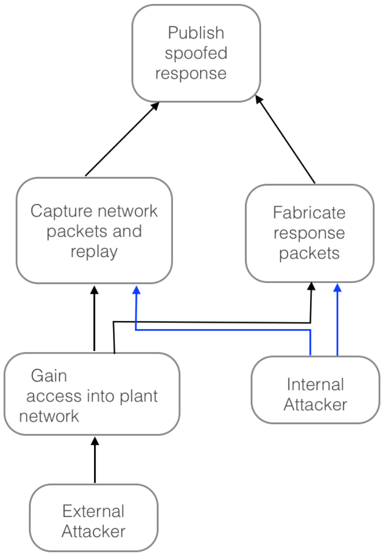

Publish spoofed response
Capture network packets and replay
Fabricate response packets
Gain access into plant network
Internal Attacker
External Attacker

Figure 11: Attack graph to conduct an attack in ICS network

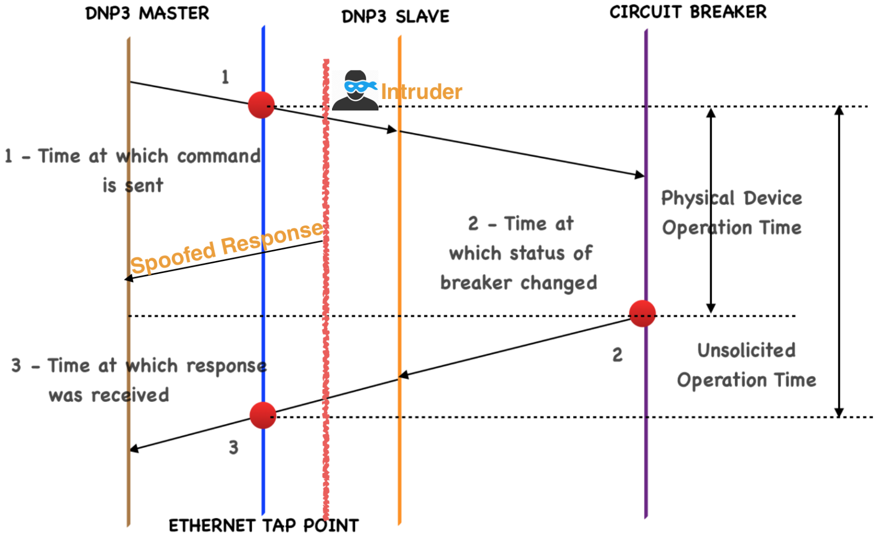
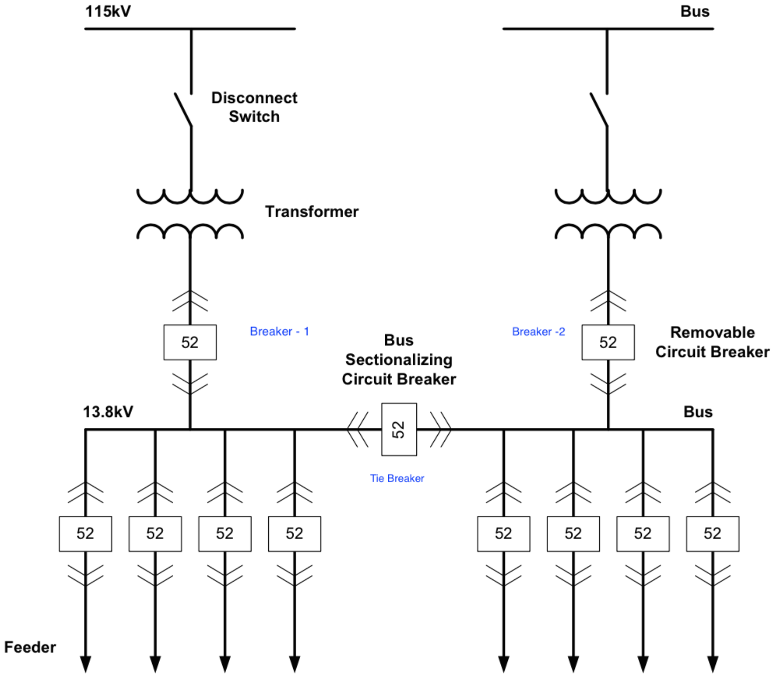

DNP3 MASTER
DNP3 SLAVE
CIRCUIT BREAKER
1
Intruder
1 - Time at which command is sent
Spoofed Response
2 - Time at which status of breaker changed
Physical Device Operation Time
2
Unsolicited Operation Time
3 - Time at which response was received
3
ETHERNET TAP POINT

Figure 12: Timing diagram for attack Model with Breaker Operation

- The slave device in turn sends the hardwired command to the circuit breaker.
- Physical device responds back with the status of the circuit breaker to the DNP3 slave device.
- The DNP3 slave device sends the status information to the DNP3 master.

In the attack scenario assumed in this thesis work, even before the response from DNP3 slave reaches the DNP3 master either due to delay in network or man in the middle attack by the intruder, the intruder hijacks the TCP connection to send a spoofed response to the DNP3 master. Due to lack of any authentication mechanism as of today the master does not have a way to verify the authenticity of the response. With this in mind, the goal of this research is to develop accurate fingerprinting methods to identify from what *type* of device the response is originating from, a legitimate IED, or an adversary with a laptop who has gained access into the network.



Source:[47]

Figure 13: The one line diagram of a substation

A hypothesized scenario is described for better understanding of the importance of this form of network intrusion and the effect of the intrusion on the rest of the system. Figure 13 shows the single line diagram of a substation. A substation like the one shown above is usually equipped with a recloser unit to ensure continuous availability of power to the downstream feeders. During normal operation in the substation two out of three breakers (breaker-1, breaker-2 and tie-breaker) are closed to ensure continuous availability of power to the downstream feeders. On indication of an unhealthy supply on one of the incoming feeders the recloser unit will interfere, closing the tie-breaker and opening the unhealthy supply line. Thus during normal operation of the substation, 2-out-of-3 breaker configuration is maintained. Suppose in such a scenario, assume a *CLOSE* command has been sent by the master to recloser unit to close the tie-breaker and an attacker performs a denial of service (DOS) attack on recloser unit. The attacker then sends a "closed status" back to master but the *CLOSE* command was never sent to the tie-breaker due to a DOS attack. The master assumes that the received response was a legitimate response and issues the next *OPEN* command thus disrupting the power availability to one side of the substation. This is one such scenario which substantiates the need for authenticating the field responses.

To formally state the problem, assume global set of all ICS devices G consists of products $D_{j,k}$ where j identifies the vendor and k signifies the model for each vendor's product. Given a sequence of observations O_i every device i on the network, the goal of the fingerprinting methods will be to identify which subset of G, specifically which $D_{j,k}$ those observations belong to.

4.1.1 Proposed Solution

The main characteristic that differentiate ICS networks from more traditional IT networks is its primary functions of data acquisition through regular polling for measurements and control. This characteristic holds true not only for electric grid but also for several infrastructure networks operating distribution of water, oil and natural gas. As mentioned in Chapter 3 due to unavailability of large number of control samples to create fingerprint, the proposed idea is demonstrated only with lab experiments. Additionally a new method to create a model of the device without observing the network capture is also developed to introduce a new domain of fingerprinting methods.

The proposed fingerprinting method leverages the unique properties of physical devices between vendors in the ICS environment which produces different operation times and then develops a fingerprint for each device based on the distribution of these times. The timing diagram of how this measurement is collected is illustrated in Figure 14 and this time is called as “Breaker Operation Time” (BOT).

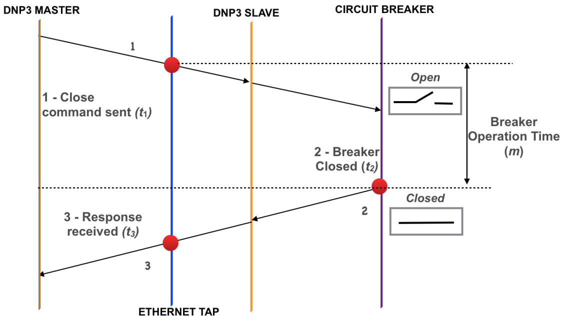


Figure 14: Measurement of device response time

The fingerprint signature is defined by a vector of bin counts from a histogram of BOTs where the final bin includes all values greater than a heuristic threshold. For a formal definition, let M be a set of operation time measurements from a specific device, B define the number of bins in the histogram (and equivalently the number of features in signature vector), and H denote the heuristic threshold chosen to be an estimate of the maximum value an operation should ever take. All the obtained observations by thresholds t_i where $t_i = i\frac{H}{B-1}$, and define each element s_j of the signature vector by the following equation:

$$s_j = \begin{cases} |\{m : t_{j-1} \leq m < t_j, m \in M\}| & 0 < j < B \\ |\{m : m > H, m \in M\}| & j = B \end{cases} \tag{1}$$

4.1.2 Theory

The whole approach of using BOT for fingerprinting is feasible because they rely on physical properties of device which remains the same for a long period of time. They tend to change eventually, for instance, pressure of vacuum in a vacuum circuit breaker reduces around 20,000 operations. Hence these properties stay constant for a long period of time thus defining the operation time by physical and mechanical properties of the device. The proposed work uses this immutable property to create the fingerprint. To understand why this is true for ICS devices, an explanation based on physics behind the operation of the device is explained below.

To demonstrate the implication of mechanical and physical properties on operation time, two latching relays with a solenoid arrangement has been chosen as shown in Figure 15. The electromagnetic force produced while energizing the solenoid coil is directly proportional to current though the solenoid, number of turns in the solenoid, cross sectional area of the solenoid core and the type of the core.

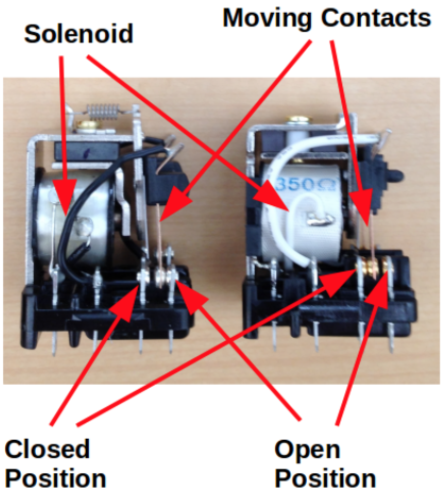


Figure 15: Latching relay constituents

$$F = (N * I)^2 u_0 A/(2g^2) \tag{2}$$

N - Number of turns in the solenoid

I - the current, in amperes(A),running through the solenoid

A - the cross-sectional area, in meters-squared, of the solenoidal magnet

g - the distance in meters, between the magnet and piece of metal

k - 4 x pi x 10^{-7} (a constant)

This electromagnetic force governs the operation time, and modification of any one of these variables due to different vendor implementations results in unique signatures. The electromagnetic force is directly proportional to the operation time because this is the force that is responsible for moving the contact from one position to another. The modification of any one of these components result in a unique signature in the form of varying ranges of operation time for different vendors. This work proposes to use this signature from the network traffic to fingerprint the physical devices in the field.

In addition to proposing a specific distribution in order to differentiate the devices per vendor, individual physical operations like *OPEN* or *CLOSE* will also produce a difference in operation times. This is again attributed to the different force involved in maintaining the position of the contact from the previous operation. This work discusses the difference in operation times between open and close produced by spring force and magnetic force respectively. Thus a combined pattern of *OPEN* and *CLOSE* operations produces an additional fingerprint to distinguish between vendors.

Table 1: Operation Time Dependence Parameters

Characteristic Type	Physical Properties
Mechanical Characteristics	Temperature Control Voltage Stored Energy Level Impact of Idle time Times of Operation
Electrical Characteristics	Rate of Decay of Dielectric Strength

The breaker operation time is observed from the network traffic visible at the tap point. This is because when the breaker responds to the operate command from the master, an event change is observed at the DNP3 slave device. With unsolicited response enabled in the DNP3 slave device, the DNP3 slave asynchronously responds back with a message on an event change. Since the DNP3 protocol supports Sequence of Event Recorder (SER) timestamps as explained in Chapter 2, it is possible to accurately pinpoint the time at which each event occurred. Therefore, operation times can be estimated based on two different methods:

1. Unsolicited Response Timestamps - Calculated by the OS at the tap point by taking the difference between the time at which the command was observed and the time at which the response was observed. $m = t_3 - t_1$
2. SER Response Timestamps - Calculated from the difference between the time at which the command was observed at the tap point and the application layer event timestamp. $m = t_2 - t_1$

Even though operation times are dependent on electromagnetic force which is governed by Equation 2, IEC62271-302 provides its dependence on dynamic instantaneous characteristics in addition to the physical structure's arrangement. Table 1 shows the physical parameters depending upon which the circuit breaker operation time changes. Thus effect of other features provides an additional indeterminism in the operation times which is usually compensated by breaker manufacturer by "Controlled Switching"[48].

CHAPTER V

IMPLEMENTATION AND RESULTS

5.1 Experimental Test Setup

To demonstrate the proposed approach, latching relay operation was chosen. The experimental setup consists of C++ software based DNP3 master from a C++ open source DNP3 implementation (OpenDNP3 version 2.0), an SEL-751A DNP3 slave and two latching relays to demonstrate fingerprinting based on operation time. At the tap point in Figure 16, a C based DNP3 sniffer is used to sniff and parse the DNP3 packets to perform deep packet inspection. At the same tap point, the packets are timestamped by the Linux operating system which is time synchronized by the same time source as that of the DNP3 master and DNP3 slave by SNTP protocol.

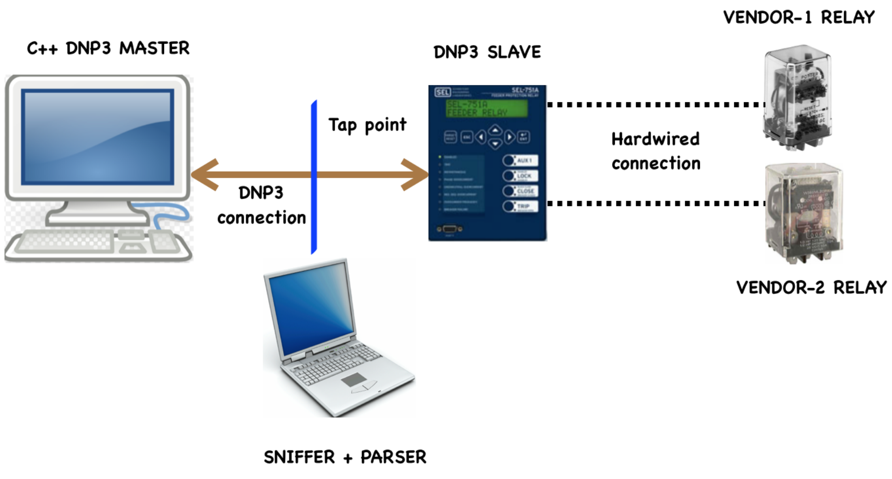


Figure 16: Experimental test setup-fingerprinting breakers

The SEL-751A is a feeder protection relay supporting Modbus, DNP3, IEC61850 protocol, time synchronization based on SNTP protocol and a fast SER protocol which timestamps events with millisecond resolution. The SER buffer settings in the device were enabled to send the response with a delay of 0ms, thus sending the response as soon as the event was observed. The experimental setup for both relays consisted of a latching circuit (Figure 17) and a load circuit (Figure 18). An image of experimental test setup with two latching relays and SEL 751A relay is shown in Figure 19.

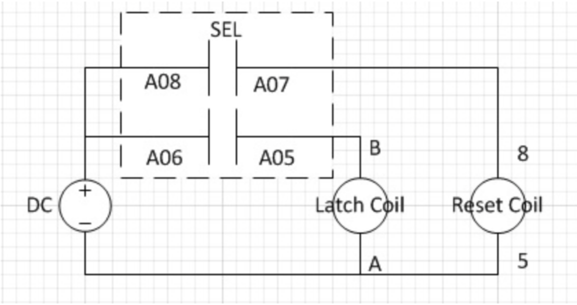


Figure 17: Operation circuit for latching relay

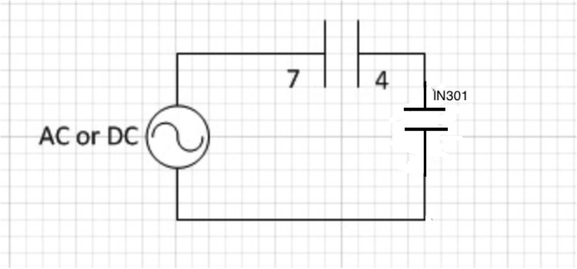


Figure 18: Load circuit for latching relay

Figure 19: An image of the connection test setup

The latching circuit works on an operating voltage of 24VDC needing about 1A to operate and load circuit is based on 110V since the binary input on the IED is rated for that. On a *CLOSE* command from the DNP3 master, the IED activates a binary output energizing the latch coil to close the load circuit. Once the load circuit is energized, the feedback is sent back to activate a binary input in the IED. This event is timestamped and provided back to the relay as activated input. On an *OPEN* command from the DNP3 master, the IED activates the second binary output energizing the reset coil thus opening the load circuit. This deactivates the binary input and is recorded as an event change. For these experiments, 2500 DNP3 *OPEN* and *CLOSE* commands were issued simultaneously to both the latching relays with an idle time of 20ms between operations. The command and responses were recorded at the tap point and operation times were calculated using both the unsolicited response method and SER based method.

5.2 Results

5.2.1 Fingerprinting using Unsolicited Response

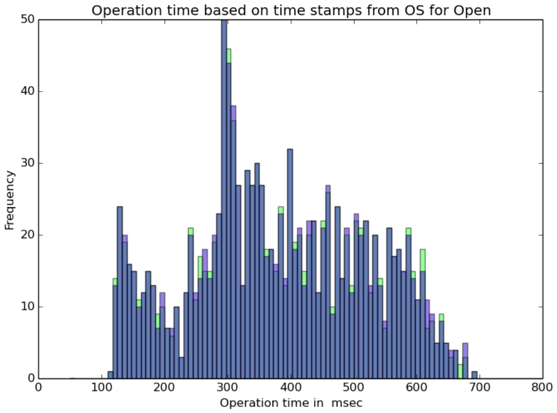


Figure 20: Distribution of open operation times based on unsolicited responses

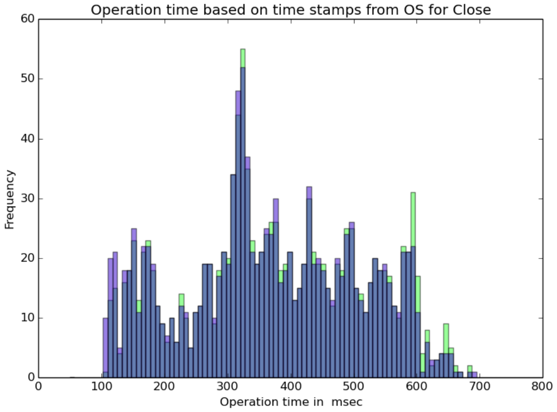


Figure 21: Distribution of Close operation times based on unsolicited responses

The operation time based on unsolicited responses was estimated by measuring the time difference between when the request was sent and when the unsolicited response indicating the event was received. Figure 20 and Figure 21 shows the distribution of open and close operation times respectively based on unsolicited responses. These results are based on unsolicited response observed at the tap point without looking into the application layer of the packet. It is observed that this distribution does not help to fingerprint the device from different vendors. This is because the operation time of the physical device is lesser than the time taken by the DNP3 slave to sense the event, generate the response, and send the packet, thus obscuring the actual operation time of the physical device. After comparing the unsolicited packet capture and the polling based packet capture it was observed that the event buffer was not filled up even after the device had received the latching relay opened/closed feedback. Thus it dominates the actual operation time of the physical device. The components of the unsolicited timestamp are response creation time, transmission time and propagation time. The propagation time is considered to be constant as the experimental setup involves no network delay. The remaining difference in time is produced by time taken by the DNP3 slave to unpack the packet and send the command to the physical device, time taken for the physical device to operate and time taken by the DNP3 slave to create the response packet to be sent back to the master. The time taken to send the response packet overshadows the operation time thus making it unusable for fingerprinting the device. This necessitates the need for deep packet inspection and to refer to the application layer timestamp to accurately determine the operation time.

5.2.2 Fingerprinting based on SER timestamps to differentiate vendors

The distributions of close operation times based on SER timestamps for devices from two different vendors are illustrated in Figure 22. The times range from 26ms to 38ms for the 1st vendor and 14ms to 33ms for the 2nd vendor. Even though both of these devices have similar ratings, the difference in operation is attributed to difference in physical makeup between them. Both of them are made of solenoid coil based magnetic arrangement with one pulse to move their contacts in one direction and another redirected pulse to move them back. The

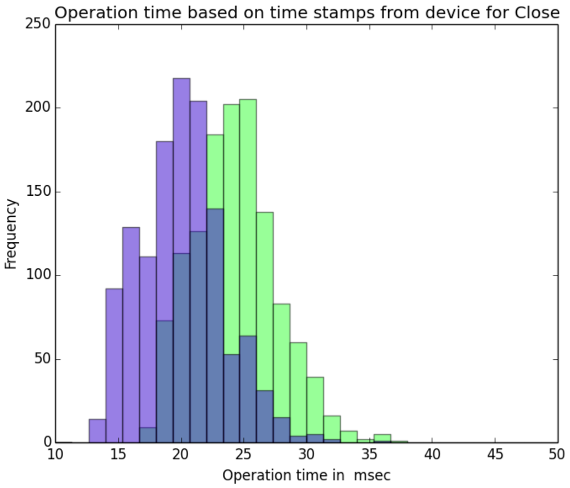


Figure 22: Distribution of close operation times based on SER responses

magnetic force from the solenoid coil arrangement is given by the equation 2. The reason for the 1^{st} vendor's slow operation time is due to the smaller cross-sectional area of the solenoid core in the device. The magnetic force is responsible for moving the contact and reduced cross-sectional area results in reduced magnetic force since it is directly proportional to force. Thus reduced force resulted in increased operation time. This variation in operation time provides a unique fingerprint based on physical arrangement of the device. The physical characteristics of the field device and its effect on the mechanical operation of the device are directly related thus making the responses dependent on the mechanical characteristics which are difficult to forge.

The machine learning algorithm used in these experiments to classify the labeled data was a feed forward artificial neural network (FF ANN) with one hidden layer trained using the back propagation algorithm. The bin counts of the histograms, as defined in Equation 1, were used as the feature vector for each sample and the time slice they were taken over was varied. The samples were randomly divided using 75% as training data and 25% as testing data. This technique when applied were able to classify the latches based on SER timestamped operations, the accuracy leveled off around 88%. The average accuracy, precision, and recall for these experiments are shown in Figure 24, and suggests that even with time slices as small as 30 minutes, very high accuracy, precision, and recall can be

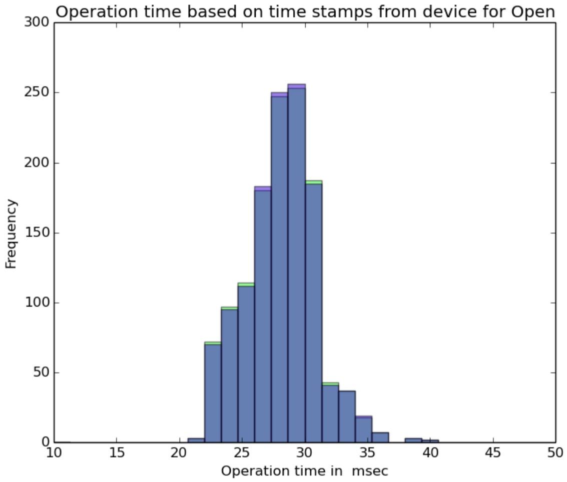


Figure 23: Distribution of open operation times based on SER responses

achieved.

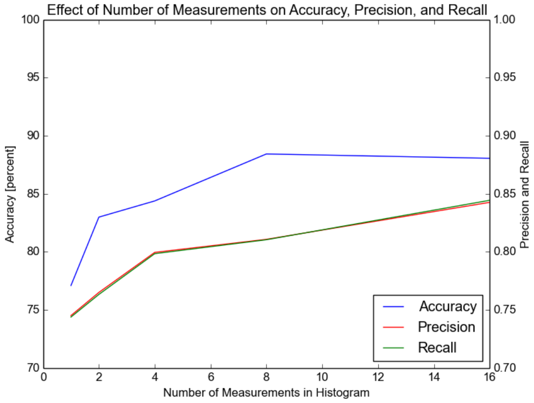


Figure 24: Classification performance based on timestamped close operations

Figure 23 shows the distribution of open operation times for devices from two different vendors. The time range varies from 22ms to 35ms for both the devices and shows that there is no variation between them. The interruption or opening time of the relay is provided in the data sheet of the relay and it is taken as the point of reference for choosing the relay. Thus the observation that two devices has the same opening time is validated. This is counter-productive for fingerprinting and thus the close operation must be used to fingerprint the devices among vendors.

5.2.3 Fingerprinting based on SER timestamps to differentiate between Operations

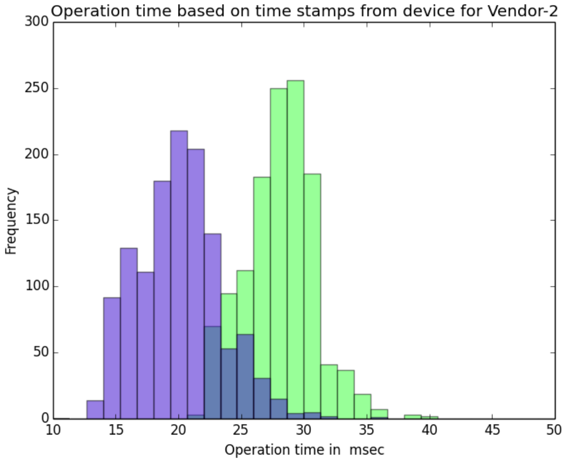


Figure 25: Distribution of open and close operation times based on SER responses for vendor-2

Figure 25 shows the distribution of open and close operations from 1st vendor. The reason for difference in operation times in the same device is attributed to the permanent magnet arrangement to hold the position of the contacts. The magnet is 'H' shaped, one end of which is connected to the plate attached to the moving contact. This arrangement magnetizes the plate and helps in providing the torque to move the moving contact. The torque to move the contacts is higher in one direction than in the other direction due to the distance involved in the movement represented by the equation 3.

$$Torque = r * F \tag{3}$$

r - perpendicular distance from pivot to point where force is applied

F - applied force

For the same amount of magnetic force, the torque is directly proportional to the distance relative to the pivot. Thus for one position, the distance is less thus having less torque and for the second position the torque is higher due to longer distance. This clearly produces distinct operation time ranges for the vendor device.

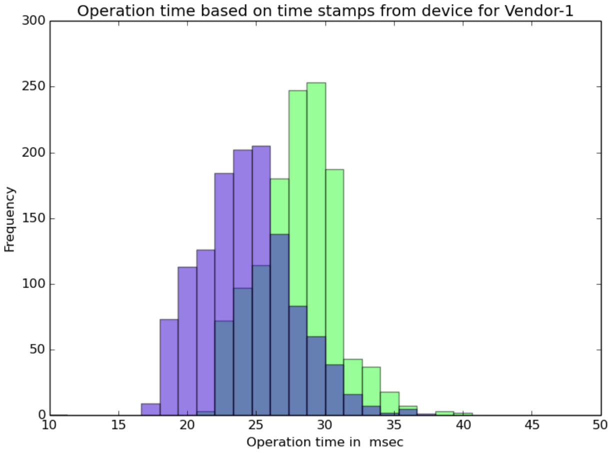


Figure 26: Distribution of open and close operation times based on SER responses for vendor-1

On repeating the experiments on the second vendor device, the distribution of open and close operation times (Figure 26) were very different from the 1st vendor. This was attributed to the force used to hold the last operated position until a second pulse resets the relay back to its original state. The device from this vendor uses spring arrangement for holding the position in one direction and magnetic force (equation 2) from a permanent magnet in the other direction. The force of the spring arrangement is represented by the equation 4.

$$F = -k * X \tag{4}$$

k - spring constant

X - amount by which the free end of the spring was displaced from its relaxed position

This difference in arrangement provides a unique fingerprint when open and close operation pattern are considered together to differentiate devices between vendors.

5.3 Difference between single device and n-device operation

The purpose of this set of experiments was to determine if a there were any significant differences between one physical device operating behind an IED or n such devices. To test this, two devices were simultaneously operated and the operation times were compared with experiments where only one device was operated in Figure 27.

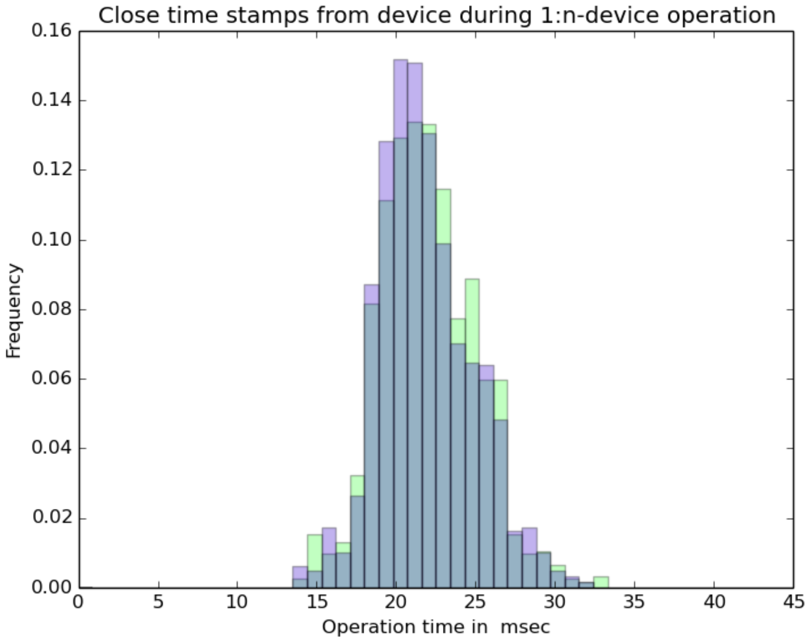


Figure 27: Distribution of open and close operation times based on SER responses for vendor-1

While the two experiments look too similar to draw any firm conclusions, there are some small differences that suggest a possible trend and could be investigated further. The distribution of operation times with only one device appears to have more “fast” operation times less than 20ms. This could be caused by the time stamping of the DNP3 slave device varying since it has to perform more work when it has to monitor two devices than when it has to monitor single device.

5.4 Does protocol matter?

During the initial phase of this research work, it was assumed that the protocol through which the breaker operation used was irrelevant, as the main objective was to identify the breaker operation time. But experiments proved that the packet timing with DNP3 unsolicited response will not serve much in providing unique signatures. Additionally, frequent polling for measurements every 1ms using Modbus also did not yield distinguishable results as shown in Figure 29 and Figure 28. Therefore, in order for fingerprinting technique to work, the protocol being used should support event based time stamping with at least millisecond resolution, which is needed to accurately determine the signature of a particular physical device. This work used DNP3 as an example protocol but other protocols such as Synchrophasor and IEC61850 would also suffice.

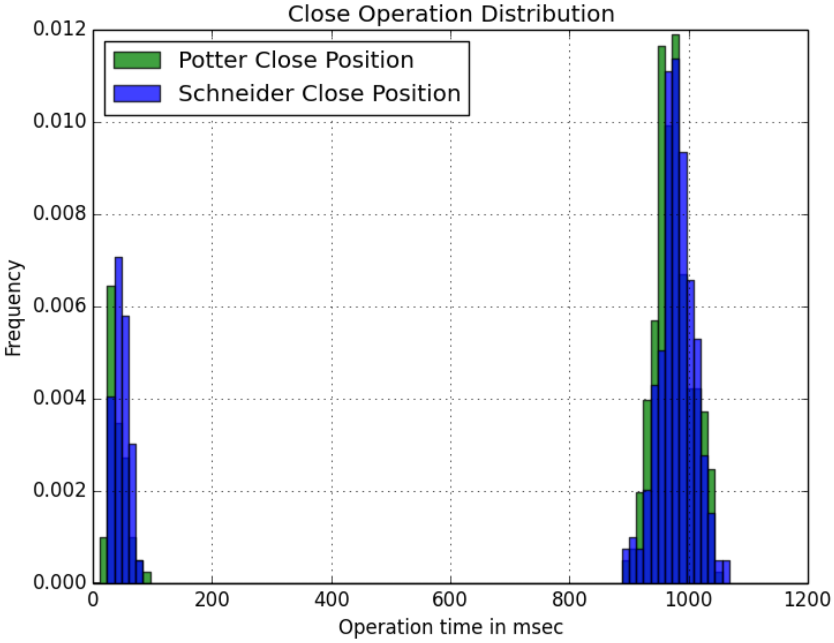


Figure 28: Distribution of close operation times based on Modbus protocol

Moreover IEC61850 GOOSE protocol, which by standard is faster than DNP3 could be a more ideal choice. One more observation regarding protocol from this work is that while using DNP3, no information about the physical device was found to be directly obtainable from the network traffic itself. Therefore, it is necessary to perform a deep

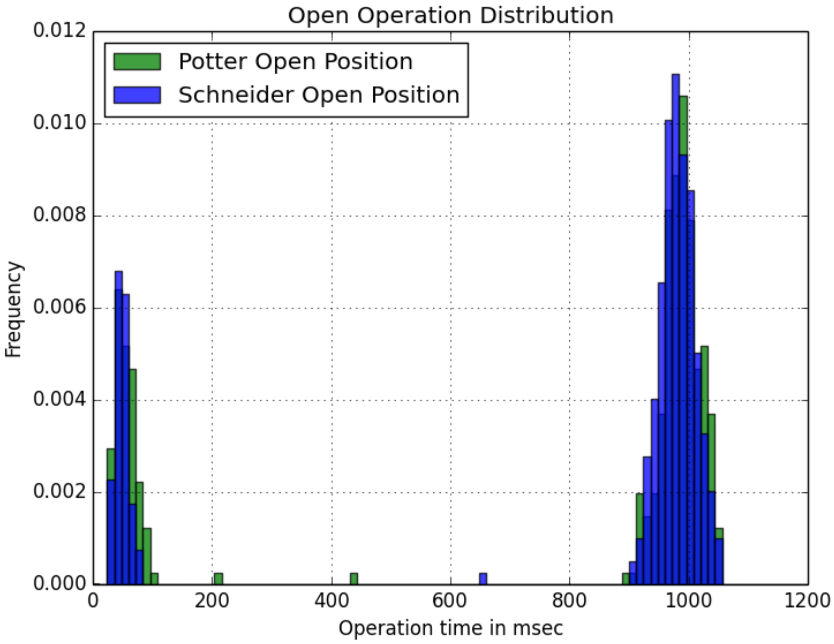


Figure 29: Distribution of open operation times based on Modbus protocol

packet inspection to get a unique signature since the timestamps are available only at the application layer. This suggests that implementing security at the Transport layer to encrypt the application layer payload should prevent information leakage from the physical device connected to the DNP3 slave.

5.5 Discussion

5.5.1 Performance

In order for a fingerprinting method to be useful for any situation, whether it is for intrusion detection, surveillance, or network management, the techniques should be relatively accurate and scalable.

Accuracy: While this method was able to obtain the acceptable classification accuracy needed for an effective stand-alone intrusion detection system, it achieved high enough accuracy to prove useful in a defense-in-breadth strategy as a supplement to traditional IDS approaches. The physical fingerprinting method was able to accurately classify measurements from two nearly identical devices around 88% of the time. For reference, all of the previous passive fingerprinting methods described in Chapter 3 achieved classification accuracies ranging from 86% to 100%, so these performances are quite comparable.

Scalability: The FF-ANN algorithms used in training the fingerprinting technique only had one hidden layer and 200 input features, resulting in reasonable scalability for computational complexity. Furthermore, our results suggest that the accuracy for the methods scales as well. Although the physical fingerprinting method only achieved an accuracy of 88% for two similarly rated devices, it would be expected to achieve even higher accuracy as more diverse types of devices are added to the test set, resulting in more clear differences in distributions.

5.5.2 Robustness Against Forgery

When using device fingerprinting to augment traditional IDS methods, it is also desired that the fingerprints be difficult to forge. To evaluate the proposed method against forgery, it is assumed that an adversary has gained access to an ICS network, has monitored it to generate a black box signature for a target device, and is masquerading as that device while attempting to recreate the signature. The physical fingerprinting method was attacked by modifying an open source implementation of DNP3 (OpenDNP3 version 2.0) and running it on the same machine described above. A DNP3 master was configured to send operate commands every second, and the adversary machine programmed to send responses with timestamps calculated from the machine's current time, added with the known distribution of operation times. The resulting forgery attempt, illustrated in Figure 30, is similar to the original, but has noticeable differences that could be explained by randomness added by the adversary's machine and a faster processor than the original IED. Using the same FF-ANN methods as above to distinguish between these two resulted in an accuracy of 71.4%, an average precision of 0.587, and recall of 0.578.

Even though the fingerprinting techniques exhibit resistance to these naïve forgery attacks, we admit it is still possible that an attacker could more intelligently shape his response times to more closely match the true fingerprint. However, this would require a significantly more knowledgeable and skilled adversary to successfully accomplish, suggesting that these methods are robust enough to be used as part of a defense-in-breadth IDS strategy.

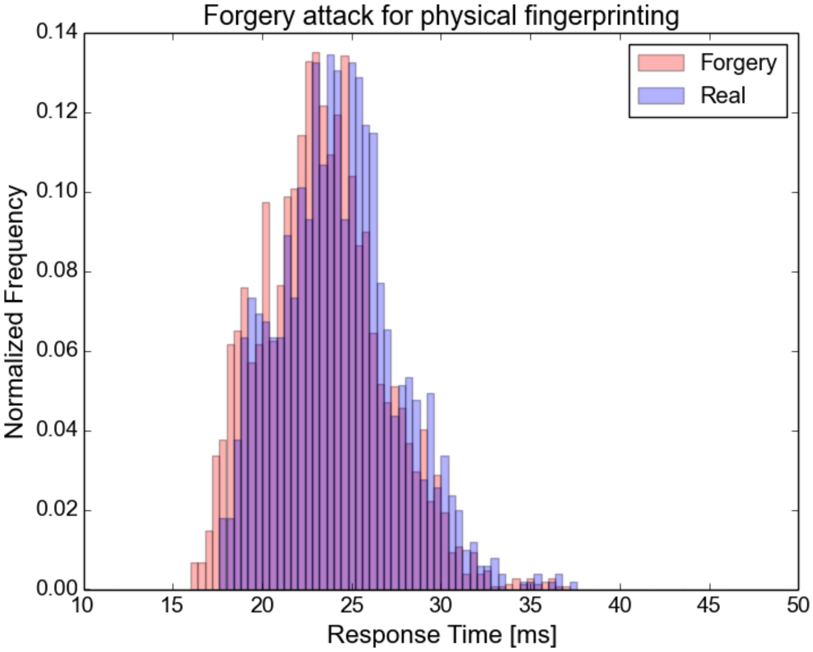


Figure 30: Forgery attempt for physical fingerprinting

5.5.3 Limitations

The physical fingerprinting method requires high resolution timing of when operations take place, so it must be used with protocols that include operation timestamps in their responses. Not all SCADA protocol support this functionality, but the ones used in time-critical environments, such as the power grid, do include such timestamps. Requiring timestamps in the network traffic is a limitation in the sense that it can make it easier for an adversary to generate and forge the device fingerprints, but it can also be a defensive strength in another. If the network traffic is encrypted, an adversary would have to resort to white box modeling to attempt to generate any fingerprints, which is non-trivial and becomes more difficult as the devices modeled become more complex (explained in detail in [9]) .

CHAPTER VI

CONCLUSION AND FUTURE WORK

In this thesis, a novel method to passively fingerprint the physical field device in a power grid environment has been introduced and a proof of concept for such an implementation has also been provided. All the experiments demonstrated in this work is done with respect to the electric grid only but can be easily extended to more ICS networks in general. After evaluating the method with controlled lab experiments, fingerprint classification accuracies as high as 88% was achieved. The technique showed resistance to simple forgery attacks and could be practically implemented alongside traditional IDS system solutions to augment security of critical networks. Even though there are several legacy protocols in ICS network, the experiments conducted proved that the fingerprinting technique needs high resolution timestamps in the response which is supported by several ICS networks.

For the future work, we plan to extend this technique towards the fast growing "Internet Of Things" (IoT) domain. IoT has been pervasive recently and predominantly used in "Home Automation" (HA) systems where security of the control and response messages are very important to ensure user's safety. An example scenario is one where the user sends the command to lock the apartment but was interrupted by the adversary to fake the response to the user. Such an attack is capable of causing both the loss of life and property. A simple solution to tackle this problem is to develop a way to fingerprint and authenticate the response received from the device. So this technique can be extended to fingerprint the devices in the IoT system to identify the type of device from which the response was received. But IoT networks are more complex than ICS network due to their inherent encryption algorithms similar to traditional IT networks. There is communication between the mobile application and IoT server first and then the command is sent from the IoT server to the local IoT controller (e.g., Wink Hub). Usually the communication between server and the local IoT controller uses the Zigbee protocol and the physical device fingerprinting technique can be extended to the IoT space.

REFERENCES

[1] Jian-Wei Wang and Li-Li Rong. Cascade-based attack vulnerability on the {US} power grid. *Safety Science*, 47(10):1332 – 1336, 2009.

[2] Marshall Abrams and Joe Weiss. Malicious control system cyber security attack case studymaroochy water services, australia.

[3] Advisory (icsa-15-169-01). `https://ics-cert.us-cert.gov/advisories/ICSA-15-169-01/`, 2015. [Online; accessed 10-March-2015].

[4] Wikipedia electric grid layout. `https://en.wikipedia.org/wiki/Electrical_grid`, 2015. [Online; accessed 07-July-2015].

[5] Scada architecture. `http://www.ooshutup.com/wp-content/uploads/2014/11/scada.jpg`, 2015. [Online; accessed 07-July-2015].

[6] Latching relay circuit. `http://www.selfhelpandmore.com`, 2015. [Online; accessed 07-July-2015].

[7] Dnp3. `http://www.dnp3.org`, 2015. [Online; accessed 07-July-2015].

[8] Kepware. `https://www.kepware.com/products/kepserverex/drivers/dnp3-master-ethernet/documents/dnp-master-ethernet-manual/`, 2015. [Online; accessed 07-July-2015].

[9] Raheem Beyah David J Formby, Preethi Srinivasan and Jonathan Rogers. Device fingerprinting methods for industrial control system networks. Submission in process to ACM CCS 2015, 2015.

[10] Nicolas Falliere, Liam O Murchu, and Eric Chien. W32. stuxnet dossier. *White paper, Symantec Corp., Security Response*, 2011.

[11] David Kushner. The real story of stuxnet. *Spectrum, IEEE*, 50(3):48–53, 2013.

[12] Todd Baumeister. Literature review on smart grid cyber security. *University of Hawaii at Manoa, Tech. Rep*, 2010.

[13] Per Erik Nordbø. Cyber security in smart grid stations. 2013.

[14] Tony Flick and Justin Morehouse. *Securing the smart grid: next generation power grid security.* Elsevier, 2010.

[15] PAS Ralston, JH Graham, and JL Hieb. Cyber security risk assessment for scada and dcs networks. *ISA transactions*, 46(4):583–594, 2007.

[16] Terry Fleury, Himanshu Khurana, and Von Welch. Towards a taxonomy of attacks against energy control systems. In *Critical Infrastructure Protection II*, pages 71–85. Springer, 2009.

[17] Vinay M Igure, Sean A Laughter, and Ronald D Williams. Security issues in scada networks. *Computers & Security*, 25(7):498–506, 2006.

[18] Bonnie Zhu, Anthony Joseph, and Shankar Sastry. A taxonomy of cyber attacks on scada systems. In *Internet of Things (iThings/CPSCom), 2011 International Conference on and 4th International Conference on Cyber, Physical and Social Computing*, pages 380–388. IEEE, 2011.

[19] Wenye Wang and Zhuo Lu. Cyber security in the smart grid: Survey and challenges. *Computer Networks*, 57(5):1344–1371, 2013.

[20] Alvaro A Cardenas, Tanya Roosta, and Shankar Sastry. Rethinking security properties, threat models, and the design space in sensor networks: A case study in scada systems. *Ad Hoc Networks*, 7(8):1434–1447, 2009.

[21] Jared Verba and Michael Milvich. Idaho national laboratory supervisory control and data acquisition intrusion detection system (scada ids). In *Technologies for Homeland Security, 2008 IEEE Conference on*, pages 469–473. IEEE, 2008.

[22] Steven Cheung, Bruno Dutertre, Martin Fong, Ulf Lindqvist, Keith Skinner, and Alfonso Valdes. Using model-based intrusion detection for scada networks. In *Proceedings of the SCADA Security Scientific Symposium*, volume 46, pages 1–12, 2007.

[23] R Sekar, Ajay Gupta, James Frullo, Tushar Shanbhag, Abhishek Tiwari, Henglin Yang, and Sheng Zhou. Specification-based anomaly detection: a new approach for detecting network intrusions. In *Proceedings of the 9th ACM conference on Computer and communications security*, pages 265–274. ACM, 2002.

[24] Hui Lin, Adam Slagell, Catello Di Martino, Zbigniew Kalbarczyk, and Ravishankar K. Iyer. Adapting bro into scada: Building a specification-based intrusion detection system for the dnp3 protocol. In *Proceedings of the Eighth Annual Cyber Security and Information Intelligence Research Workshop*, CSIIRW '13, pages 5:1–5:4, New York, NY, USA, 2013. ACM.

[25] Ondrej Linda, Todd Vollmer, and Milos Manic. Neural network based intrusion detection system for critical infrastructures. In *Neural Networks, 2009. IJCNN 2009. International Joint Conference on*, pages 1827–1834. IEEE, 2009.

[26] Kyung Choi, Xinyi Chen, Shi Li, Mihui Kim, Kijoon Chae, and JungChan Na. Intrusion detection of nsm based dos attacks using data mining in smart grid. *Energies*, 5(10):4091–4109, 2012.

[27] Ieee standard for electric power systems communications-distributed network protocol (dnp3). *IEEE Std 1815-2012 (Revision of IEEE Std 1815-2010)*, pages 1–821, Oct 2012.

[28] Samuel East, Jonathan Butts, Mauricio Papa, and Sujeet Shenoi. A taxonomy of attacks on the dnp3 protocol. In *Critical Infrastructure Protection III*, pages 67–81. Springer, 2009.

[29] Dongsoo Lee, HakJu Kim, Kwangjo Kim, and Paul D Yoo. Simulated attack on dnp3 protocol in scada system. 2014.

[30] Dong Jin, D.M. Nicol, and Guanhua Yan. An event buffer flooding attack in dnp3 controlled scada systems. In *Simulation Conference (WSC), Proceedings of the 2011 Winter*, pages 2614–2626, Dec 2011.

[31] Rakesh B Bobba, Katherine M Rogers, Qiyan Wang, Himanshu Khurana, Klara Nahrstedt, and Thomas J Overbye. Detecting false data injection attacks on dc state estimation. In *Preprints of the First Workshop on Secure Control Systems, CPSWEEK*, volume 2010, 2010.

[32] Suzhi Bi and Ying Jun Angela Zhang. Defending mechanisms against false-data injection attacks in the power system state estimation. In *GLOBECOM Workshops (GC Wkshps), 2011 IEEE*, pages 1162–1167. IEEE, 2011.

[33] Oliver Kosut, Liyan Jia, Robert J Thomas, and Lang Tong. Malicious data attacks on smart grid state estimation: Attack strategies and countermeasures. In *Smart Grid Communications (SmartGridComm), 2010 First IEEE International Conference on*, pages 220–225. IEEE, 2010.

[34] Alvaro A Cardenas, Saurabh Amin, Zong-Syun Lin, Yu-Lun Huang, Chi-Yen Huang, and Shankar Sastry. Attacks against process control systems: risk assessment, detection, and response. In *Proceedings of the 6th ACM symposium on information, computer and communications security*, pages 355–366. ACM, 2011.

[35] Hui Lin, Adam Slagell, Zbigniew Kalbarczyk, Peter W Sauer, and Ravishankar K Iyer. Semantic security analysis of scada networks to detect malicious control commands in power grids. In *Proceedings of the first ACM workshop on Smart energy grid security*, pages 29–34. ACM, 2013.

[36] Masood Parvania, Georgia Koutsandria, Vishak Muthukumary, Sean Peisert, Chuck McParland, and Anna Scaglione. Hybrid control network intrusion detection systems for automated power distribution systems. In *Dependable Systems and Networks (DSN), 2014 44th Annual IEEE/IFIP International Conference on*, pages 774–779. IEEE, 2014.

[37] Robert Mitchell and I-R Chen. Behavior rule specification-based intrusion detection for safety critical smart grid applications. 2012.

[38] Maarten Hoeve. Detecting intrusions in encrypted control traffic. In *Proceedings of the first ACM workshop on Smart energy grid security*, pages 23–28. ACM, 2013.

[39] Nmap - free security scanner for network exploration & security audits. `https://nmap.org`, 2015. [Online; accessed 25-March-2015].

[40] p0f v3: passive fingerprinter. `https://github.com/p0f/p0f`, 2014. [Online; accessed 21-May-2014].

[41] Guoqiang Shu and D. Lee. Network protocol system fingerprinting - a formal approach. In *INFOCOM 2006. 25th IEEE International Conference on Computer Communications. Proceedings*, pages 1–12, April 2006.

[42] Tadayoshi Kohno, Andre Broido, and K. C. Claffy. Remote physical device fingerprinting. *IEEE Trans. Dependable Secur. Comput.*, 2(2):93–108, April 2005.

[43] Ke Gao, C. Corbett, and R. Beyah. A passive approach to wireless device fingerprinting. In *Dependable Systems and Networks (DSN), 2010 IEEE/IFIP International Conference on*, pages 383–392, June 2010.

[44] J. Francois, H. Abdelnur, R. State, and O. Festor. Ptf: Passive temporal fingerprinting. In *Integrated Network Management (IM), 2011 IFIP/IEEE International Symposium on*, pages 289–296, May 2011.

[45] S.V. Radhakrishnan, A.S. Uluagac, and R. Beyah. Gtid: A technique for physical device and device type fingerprinting. *Dependable and Secure Computing, IEEE Transactions on*, PP(99):1–1, 2014.

[46] O. Ureten and N. Serinken. Wireless security through rf fingerprinting. *Electrical and Computer Engineering, Canadian Journal of*, 32(1):27–33, Winter 2007.

[47] Single line diagram of a substation. `http://www.electricalknowhow.com`, 2015. [Online; accessed 07-July-2015].

[48] Kohyama Yamamoto Wilson Billings Todd Ito, Tsutada. Factory and field verification tests of controlled switching system. *Mitsubishi Tech Rep.*, 2003.