Spring 2018

Multiple security domain non deducibility in the FREEDM smart grid infrastructure

Manish Jaisinghani

Department:

MULTIPLE SECURITY DOMAIN NON DEDUCIBILITY IN THE FREEDM SMART GRID INFRASTRUCTURE

by

MANISH JAISINGHANI

A THESIS

Presented to the Graduate Faculty of the

MISSOURI UNIVERSITY OF SCIENCE AND TECHNOLOGY

In Partial Fulfillment of the Requirements for the Degree

MASTER OF SCIENCE

in

COMPUTER SCIENCE

2018

Approved by

Dr. Bruce McMillin, Advisor
Dr. Jonathan Kimball
Dr. Wei Jiang

ABSTRACT

The building block of today's world are not materials, but, computers and algorithms with communication networks between physical entities. A cyber physical system (CPS) is a system in which the cyber and physical entities of the system work together towards a common goal, for example a water treatment facility or an electricity distribution system. These cyber physical infrastructures affect day to day lives of people and hence become target point for the attackers to disrupt normal daily life. Owing to the complexity of a cyber physical system, the attacks have themselves become sophisticated and harder to detect. These sophisticated attacks no longer attempt to steal information, however, intend to corrupt it inside the system in order to affect the normal functioning of the system.

To identify such attacks in a CPS, this thesis uses the *multiple security domain non-deducibility model*. The MSDND model divides the system into security domains and reduces the notion of trust into the system by replacing it with invariant based valuation functions. This work concentrates on the *Future Renewable Electric Energy Distribution Management System* (FREEDM) as a smart grid infrastructure. This thesis will attempt to identify potential ways in which smart grid infrastructure FREEDM can be attacked and suggest measures to identify the attacker using the *MSDND* model. While doing so this thesis concentrates on building blocks of the FREEDM system i.e. the state collection protocol and its distributed nature.

ACKNOWLEDGMENTS

To start with i would want to quote below from "Bob Proctor":

"A mentor is someone who sees more talent and ability within you,
than you see in yourself, and helps bring it out of you"

This quote truly expresses my mentor or advisor Dr. Bruce McMillin. Words are not enough to thank him for all his knowledge, guidance and motivation that he has bestowed upon me. His experience and perspective towards research problems has always been an inspiration. My experience with Dr. McMillin is a treasure that i would cherish all life.

I would also like to express my gratitude towards my thesis committee: Dr. Jonathan Kimball for his thoughtful comments and motivation and and Dr. Wei Jiang for his support in extending the much needed knowledge of Distributed Systems. I would also like to extend gratitude towards my fellow graduate students: Vamsi Krishna Chokkapu, Sai Sidharth Patlolla and Prashanth Palaniswamy and undergraduate student: Julius Ceasar Aguma for their constructive queries and intuitive thoughts towards my work.

Last but not the least I am indebted to the endless support of my family members, my parents and my brother for showing trust in me and supporting me to pursue my dream towards higher education at a place too far from home. Thank and gratitude is a small return for the experience and knowledge i have gained.

TABLE OF CONTENTS

Page

ABSTRACT iii

ACKNOWLEDGMENTS iv

LIST OF ILLUSTRATIONS vii

LIST OF TABLES ix

NOMENCLATURE x

SECTION

1. INTRODUCTION 1

2. LITERATURE REVIEW 2
   - 2.1. MODAL LOGIC 2
   - 2.2. MSDND 2
   - 2.3. INVARIANTS 3
   - 2.4. UNDERSTANDING MSDND AND HOW A PROOF IS CONSTRUCTED 3
   - 2.5. THE FREEDM SYSTEM 5
     - 2.5.1. DGI 5
     - 2.5.2. IEM 7
     - 2.5.3. IFM 7
   - 2.6. ENERGY INTERNET 7
   - 2.7. THE BYZANTINE GENERALS PROBLEM 8
   - 2.8. PHYSICAL ATTESTATION OF CYBER PROCESSES IN A SMART GRID 8

3. PROBLEM STATEMENT 10

4. SECURITY ANALYSIS OF THE FREEDM SYSTEM 13

4.1. STATE COLLECTION PROTOCOL 13

4.1.1. MSDND Analysis State Collection Protocol - Step 1 14

4.1.2. MSDND Analysis State Collection protocol - Step 2 18

4.2. INTRODUCING DEDUCIBILITY IN CONSENSUS BASED STATE COLLECTION PROTOCOL USING BYZANTINE AGREEMENT 28

4.3. PHYSICAL ATTESTATION 43

4.3.1. Physical Attestation of Cyber Process in a 3 Node FREEDM System 43

4.3.2. Physical Attestation of Cyber Process in a 7 Node FREEDM System 59

5. CONCLUSIONS 72

5.1. DISTRIBUTED CYBER PHYSICAL SYSTEMS 72

5.2. MSDND 72

5.3. STATE COLLECTION PROTOCOL IN THE FREEDM SYSTEM 72

5.4. MSDND ANALYSIS OF THE PHYSICAL ATTESTATION PROTOCOL . 73

5.5. SUMMARY 73

REFERENCES 75

VITA 77

LIST OF ILLUSTRATIONS

Figure Page

2.1. Basic MSDND 4
2.2. The FREEDM system architecture 6
2.3. 3 Node System Depicting Power Flows 9
3.1. 3 Node FREEDM System architecture 11
3.2. 3 Node FREEDM System affected by the STUXNET-like virus 12
4.1. DGI device interaction 15
4.2. DGI device interaction under virus attack 17
4.3. DGI DGI interaction under normal operations 19
4.4. DGI DGI interaction under STUXNET-like virus attack 22
4.5. Initiator node marker message communication under STUXNET-like virus attack 24
4.6. Peer node marker message communication under STUXNET-like virus attack .. 26
4.7. 4 Node FREEDM system 30
4.8. Message flow in a 4 node system 30
4.9. Device signal status message flow in a 4 node system 31
4.10. Round 0 message exchange 32
4.11. 4 node FREEDM system under STUXNET-like virus attack 34
4.12. Failed interactive consistency and MSDND - BIT logic view Byzantine Agreement 35
4.13. Interactive consistency and MSDND - BIT logic view Byzantine Agreement.... 40
4.14. Node 1 acting as malicious node in a 3 Node system 45
4.15. Node 2 acting as malicious node in a 3 Node system 49
4.16. Node 3 acting as malicious node in a 3 Node system 54

4.17. 7 Node System depicting power flows 60

4.18. Node 1 acting as malicious node in a 7 Node system 63

4.19. Node 4 acting as malicious node in a 7 Node system 66

LIST OF TABLES

Table Page

2.1. Security Domains - Understanding MSDND 4

3.1. Attack Model: Details of Security Domains 12

4.1. Devices and signal types 13

4.2. 3 Node System - Invariant Violations 59

4.3. 7 Node System - Invariant Violations 62

5.1. MSDND analysis results 74

NOMENCLATURE

Symbols

$\oplus$	Exclusive OR (xor)
$Device$	Set of devices in FREEDM system
DS	Set of device signals in FREEDM system
S_x	A boolean state variable, x is true or false
W	Set of all possible worlds
w	A world of interest
$B_i\phi$	Modal BELIEF operator
$I_{i,j}\phi$	Modal INFORMATION TRANSFER operator
SD^i	Security domain of entity i
$T_{i,j}\phi$	Modal TRUST operator
${v_x}^i(\phi)$	Valuation function of boolean x in domain i

Acronyms

CPS	Cyber Physical System
$DESD$	Distributed Energy Storage Device
DGI	Distributed Grid Intelligence
$DRER$	Distributed Renewable Energy Resource

FID	Fault Isolation Device
$FREEDM$	Future Renewable Electric Energy Delivery and Management
MM	Marker Message
MS	Message Passing Module
PE	Power Electronics
SST	Solid State Transformer

1. INTRODUCTION

A coordination between computers, algorithms, communication networks and underlying physical components forms the core concept of a CPS. A wide variety of attacks are possible on all the CPS by affecting any of the above components of the system. An important point to observe here is that this work does not talk about identity theft or access theft, the problem at hand is corrupting the information flow paths among distributed components of a CPS to affect normal operations of a system. This work considers the FREEDM system as our cyber physical infrastructure. The FREEDM smart grid is a proposed energy internet or electric power distribution system that is suitable for plug and play of distributed energy resources and energy storage devices (Huang *et al.*, 2011). A smart grid is susceptible to different types of attacks such as data integrity attacks (Duan and Chow, 2017) and fake supply attacks (Roth and McMillin, 2013). These attacks have been demonstrated over the FREEDM system and the paper proposes a common approach based over the MSDND framework and belief, information transfer and trust(BIT) logic, (Howser and McMillin, 2014) to identify the malicious nodes in the system. The power distribution and consumption system is heavily dependent over three modules in the FREEDM system: Group Management, state collection protocol and energy management protocol. The task of the state collection protocol is to collect states of all the devices in the energy internet (Crow *et al.*, 2010). A malicious node (distributed renewable energy device(DRER) / distributed energy storage device(DESD) / solid state transformer (SST)) can lie about its state to the distributed grid intelligence (DGI) corrupting all the power computations of the DGI which may result into a potential blackout for the sub-grid or issues such as power migration contacts not being fulfilled.

2. LITERATURE REVIEW

In a CPS attacks that corrupt the information flow are difficult to identify as the attacker becomes part of the system and is not an external entity aiming for theft of information. This thesis also discusses, solutions proposed to identify failed components (specifically a component that sends conflicting or false messages to peer components) in a distributed system.

2.1. MODAL LOGIC

The modal logic (Liau, 2003) (Liau, 2005) or belief, information acquisition, and trust(BIT) logic is a well formulated method to analyse information flow between two entities. BIT logic is important to determine security for a cyber physical system, as it helps us to determine belief and trust as a logic rather than a propositional boolean entity. It also helps us to represent a formal definition of MSDND in the form of modal logic. Sutherland's Nondeducibility (Sutherland, 1986), BIT logic (Liau, 2003) and MSDND (Howser and McMillin, 2013) are the three main pillars of this work.

2.2. MSDND

In order to analyse complex cyber physical systems multiple security domain non deducibility is introduced by (Howser and McMillin, 2013). MSDND is based on modal logic where in a complex infrastructure is divided into multiple security domains as compared to two in Sutherlands' Nondeducibility model (Sutherland, 1986). A security domain is a partition or world which may overlap / coincide with other partitions or worlds. An action invisible outside its security domain is said to be MSDND secure. For an action

or event to be visible outside its security domain a valuation function $v_x^y(\phi)$ is defined. A valuation function v_y^i is a boolean function which outputs true if the value of entity of variable x can be seen from domain y and false otherwise.

$$MSDND(ES) = \exists\, w \ni W \vdash \left[(S_x \oplus S_y)\right] \wedge \left[w \vDash (\nexists\, v_x^i\,(w) \wedge \nexists\, v_y^i\,(w))\right]$$

2.3. INVARIANTS

A property or characteristic of system that remains unaffected or can be evaluated to determine specify system semantics or functioning can be termed as an invariant. (Owicki and Gries, 1976) proposed an axiomatic basis for the truth of invariants on cyber systems. Recent developments show the use of invariants in physical power systems (Paul *et al.*, 2014) and water treatment systems (Adepu and Mathur, 2016).

2.4. UNDERSTANDING MSDND AND HOW A PROOF IS CONSTRUCTED

This section aims at giving a high level view of MSDND and how MSDND proofs are constructed. MSDND model has two important components, 1. Dividing the underlying infrastructure into security domains and 2. Capturing information flow paths within these security domains. To understand this better, consider architecture in Figure 2.1

The Figure 2.1 captures two individuals sitting in a room divided through a wall. Alice and Bob can only communicate through the communication channel. The wall does not allow alice or bob to see each other or pass messages without using the communication channel. As there is only one information flow path between alice and bob, Table 2.1 displays details of security domains for the system.

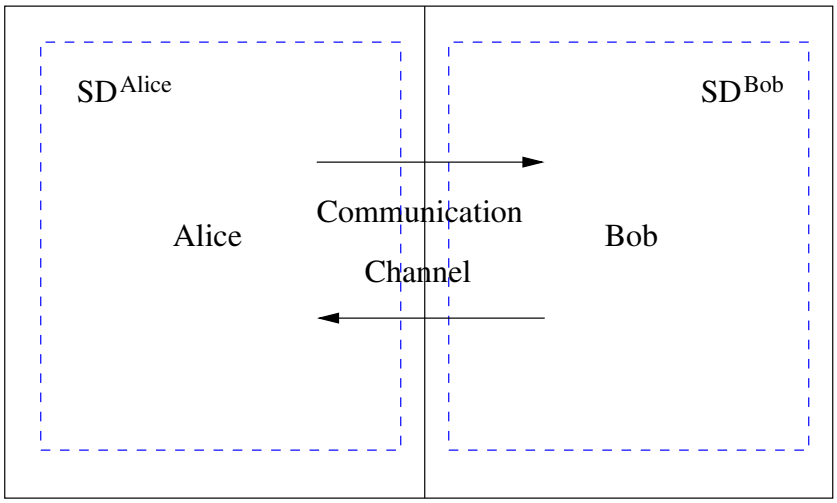

Figure 2.1. Basic MSDND

Table 2.1. Security Domains - Understanding MSDND

Security Domain	System Entity
SD^{Alice}	Alice's domain
SD^{Bob}	Bob's domain

Considering the system architecture in the Figure 2.1, imagine below line of questions:

Alice: Bob, are you working on the thesis?

Bob: Yes Alice, of-course I am.

Alice: Amazing, i am also working on the thesis.

In the above conversation, there is no way in which both Alice or Bob can verify if the other was speaking the truth. They have to trust the responses from each other. In such a case MSDND says that there is no valuation function that exists in either domains which can verify the truth or the system is MSDND secure. As discussed above MSDND secure system is good for the attacker and bad for the system. MSDND captures validity of working over thesis by Alice and Bob as represented as below:

$$MSDND(ES) = \exists\, w \ni W \vdash [(S_{thesis} \oplus S_{\sim thesis})] \wedge \left[w \vDash (\nexists\, v^{Alice}_{thesis}(w) \wedge \nexists\, v^{Alice}_{\sim thesis}(w))\right]$$

$$MSDND(ES) = \exists\, w \ni W \vdash [(S_{thesis} \oplus S_{\sim thesis})] \wedge \left[w \vDash (\nexists\, v^{Bob}_{thesis}(w) \wedge \nexists\, v^{Bob}_{\sim thesis}(w))\right]$$

An intuitive way to make this system deducible is to introduce a window in the wall between Alice and Bob. This window will allow both Alice and Bob to see through the wall and hence verify the validity or truth of the responses, there by giving a valuation function to both of them. As the window is based over the system properties and cannot be masked or falsified, it is called as an invariant. Once the system becomes deducible and one domain can verify other, MSDND is represented as below:

$$MSDND(ES) \neq \exists\, w \ni W \vdash [(S_{thesis} \oplus S_{\sim thesis})] \wedge \left[w \vDash (\exists\, v^{Alice}_{thesis}(w) \wedge \exists\, v^{Alice}_{\sim thesis}(w))\right]$$

$$MSDND(ES) \neq \exists\, w \ni W \vdash [(S_{thesis} \oplus S_{\sim thesis})] \wedge \left[w \vDash (\exists\, v^{Bob}_{thesis}(w) \wedge \exists\, v^{Bob}_{\sim thesis}(w))\right]$$

2.5. THE FREEDM SYSTEM

The future renewable electric energy management system (Crow *et al.*, 2010) is a highly distributed system, intended to serve as collection of distributed energy generation and storage devices along with existing power infrastructure. A general purpose architecture of FREEDM system is shown in Figure 2.2:

2.5.1. DGI. The distributed grid intelligence or DGI is the software component or brain behind controlling the FREEDM system. The DGI is responsible to implement various energy management algorithms and implement decisions such as the power migration contracts.

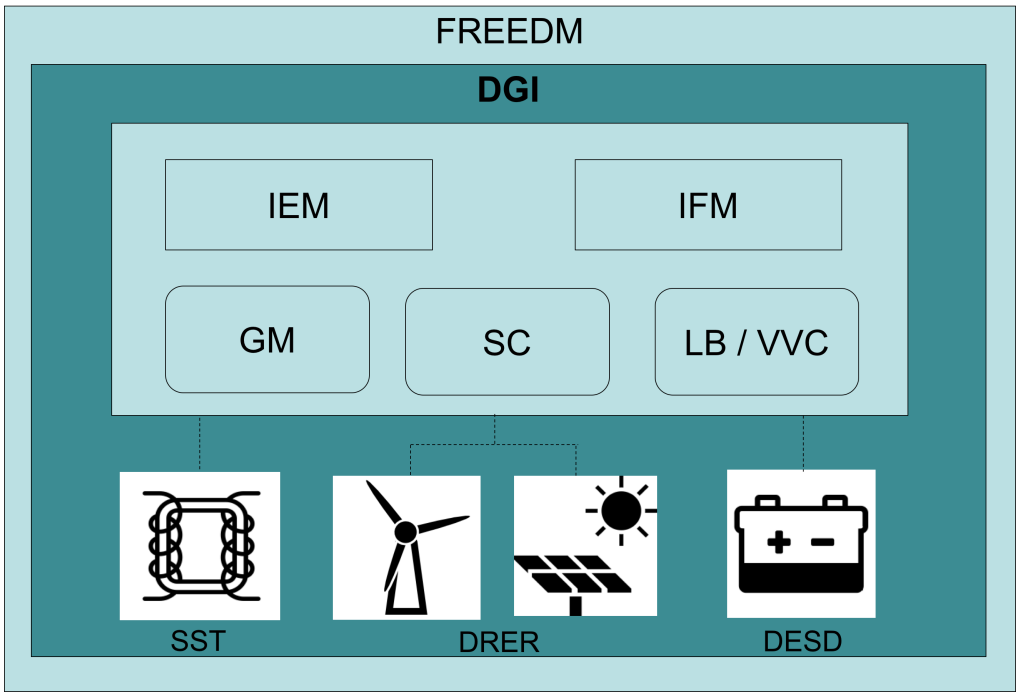

Figure 2.2. The FREEDM system architecture

- **Power Migration Contracts** A Power migration contract is an atomic set of instructions among the supply (with excess power availability) and demand (in need for more power) node that helps to buy and sell power. Power migration in the FREEDM system happens through a power migration contract. A power migration contract comprises of below steps:
  - 1. Supply house advertises excess generation.
  - 2. Demand house requests power from supply house.
  - 3. Supply and demand house start a migration.
  - 4a. Supply house increases its local generation.
  - 4b. Demand house increases its local load.

A power migration contract is considered successful if all of the above steps are executed as stated.

2.5.2. IEM. The intelligent energy management (IEM) comprises both hardware as well as the software components. The component being referred to here is a solid state transformer (SST). A SST behaves essentially as an energy router, facilitating exchange of power to and from the grid and individual house nodes.

2.5.3. IFM. The intelligent fault management (IFM) comes into play to handle known unknowns in the FREEDM system. It refers to the ability to handle and recover from unlikely situations of power disruptions.

2.6. ENERGY INTERNET

The distributed nature of the FREEDM system has SST and DGI as its core.The cyber components of the grid are heavily dependent on two algorithms the state collection protocol (Chandy and Lamport, 1985) and the energy management algorithm. The task of state collection protocol is to keep the DGI updated of current status of all the power devices managed by the it. The communication happens with a status message. The status message packet contains the device type along with a floating point value which represents status of the device. This work does not concentrate on stealing any information flowing in the system, rather, concentrates on corrupting the information in a way where in the cyber components of cyber physical system are unaware of the issues in the system. This work uses a STUXNET-like (Howser and McMillin, 2014) virus to corrupt the information flowing through status messages and demonstrate how MSDND can be helpful to detect such attacks. Similar attacks are possible on the distributed nature of the FREEDM system, where in message flow inside the system through different protocols can be corrupted to disrupt the normal functioning of the system. This work makes use of MSDND and formulates invariant dependent on the physical properties of the system (Roth and McMillin, 2013) to help us detect such attacks in the FREEDM system.

2.7. THE BYZANTINE GENERALS PROBLEM

The Byzantine Generals Problem (Lamport *et al.*, 1982) provides solution to a scenario when a failed component of the distributed system tries to mislead the system semantics by sending conflicting messages to its peers. These conflicting messages can lead to decisions causing system failures in many scenarios. (Lamport *et al.*, 1982) proposes a solution based on message communication which can prevent such failures that can also be implemented in the FREEDM system.

2.8. PHYSICAL ATTESTATION OF CYBER PROCESSES IN A SMART GRID

The physical attestation protocol proposed by (Roth and McMillin, 2013) is a distributed algorithm based on the physical properties of the system to validate the cyber process truth. The protocol is a general purpose solution for smart grids to validate the cyber component behaviour using the physical properties of the system. Physical attestation of the cyber process primarily helps in identifying the fake power injection attacks. To understand physical attestation, we have to first understand the system below:

Conservation of energy. To determine if reported readings by a node are true or false law of conservation of energy can be used. Law of conservation of energy can provide us with an invariant based over physical properties of the system. An invariant is based over the physical properties of the system and cannot be falsified by the cyber components in a cyber physical system.

To understand the invariant based over the law of conservation of energy, please consider the Figure 2.3

The law of conservation of energy states that at points a, b and c or the point of common coupling the total energy entering the point should be equal to the total energy leaving the point. Therefore, the invariants at points of common coupling are given as below:

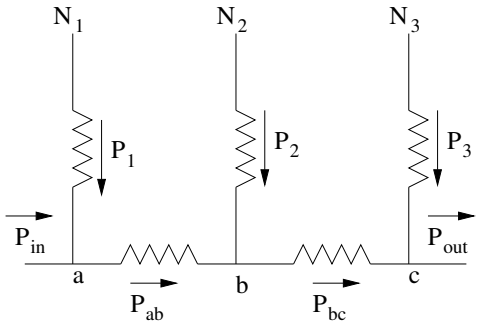

Figure 2.3. 3 Node System Depicting Power Flows

$$I_a : P_{in} + P_1 - P_{ab} = 0$$

$$I_b : P_{ab} + P_2 - P_{bc} = 0$$

$$I_c : P_{bc} + P_3 - P_{out} = 0$$

The above three equations originate from the physical properties of the system and cannot be falsified or masked. In the Figure 2.3 let us consider node 2 being the target of physical attestation protocol. To verify the reported value P_2 the power values from adjacent nodes can be used. The below equation can be used to calculate the power values at the junction or point of common coupling b.

$$P_{ab} = \frac{V_a V_b}{X_{ab}} \sin(\theta_b - \theta_a)$$

3. PROBLEM STATEMENT

An intrinsic property of a CPS is its distributed nature. The distributed nature of a CPS makes it more vulnerable to attacks from attackers who have partial or complete information of the distributed components. The work demonstrates STUXNET-like (Howser and McMillin, 2014) attacks on distributed systems working over the FREEDM (Huang *et al.*, 2011) system as an example model. It uses MSDND and BIT logic to model the attacks and address the non-deducible nature of these attacks. The STUXNET-like attacks are an unconventional type of attacks where in, the motive of an attacker is not to steal the information, however, to corrupt the information inside the system in order to destabilise the system (Chen, 2010). The behavior of corrupting rather than stealing the information is the primary reason why such attacks go un-noticed and harm the system. This work considers a 3 node 3.1 and a 7 node FREEDM system, that are scalable to much larger systems, to demonstrate an attack scenario. Under the MSDND model, an attack is successful if the information in one security domain is not visible to another security domain. Such a system is called MSDND secure. MSDND secure system is not ideal for the system, however, good for an attacker, as the attack remains hidden inside the security domain and is not visible to other domains.

Attack Model

The FREEDM system, due to its distributed nature, is heavily dependent on the message flow among peer nodes. Message or information flow among the peer nodes is taken care by the state collection protocol. Corrupting this message flow among peer nodes will disrupt the normal functioning of the system. Let us assume a 3 node system to demonstrate effect of a STUXNET-like (Howser and McMillin, 2014) virus.

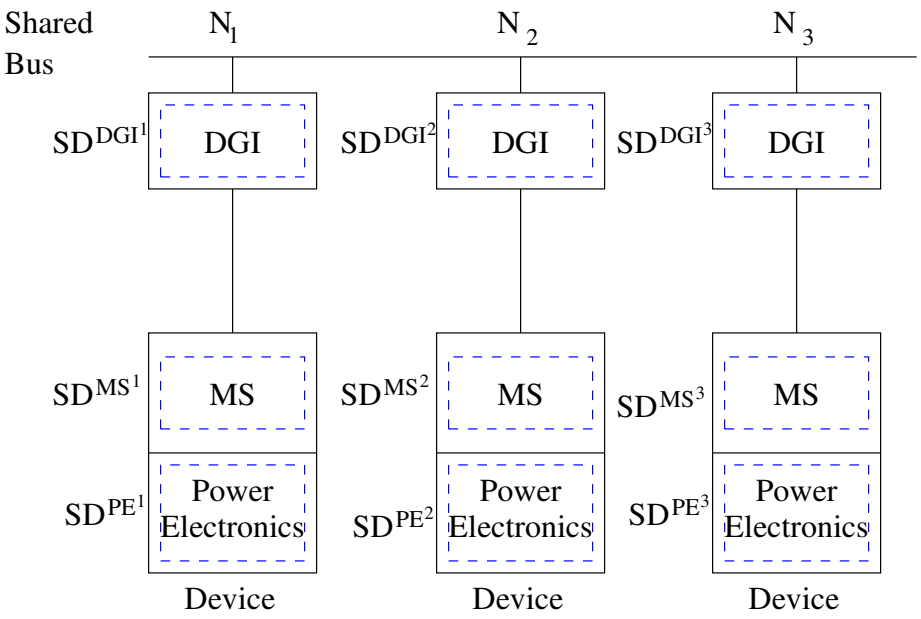

Figure 3.1. 3 Node FREEDM System architecture

In the system architecture displayed in Figure 3.2, the information path in between the power electronics module and message passing module is corrupted due to the the presence of a STUXNET-like virus. To analyze the effect of such an attack this work has divided the system into various security domains based over the information flow paths. Table 3.1 shows the security domain partitions and the associated system entity comprised within it.

The system architecture in Figure 3.2 is a basic architecture, that will demonstrate some modifications based over the number of nodes in the architecture or the position of the virus over the information flow paths in later detailed sections.

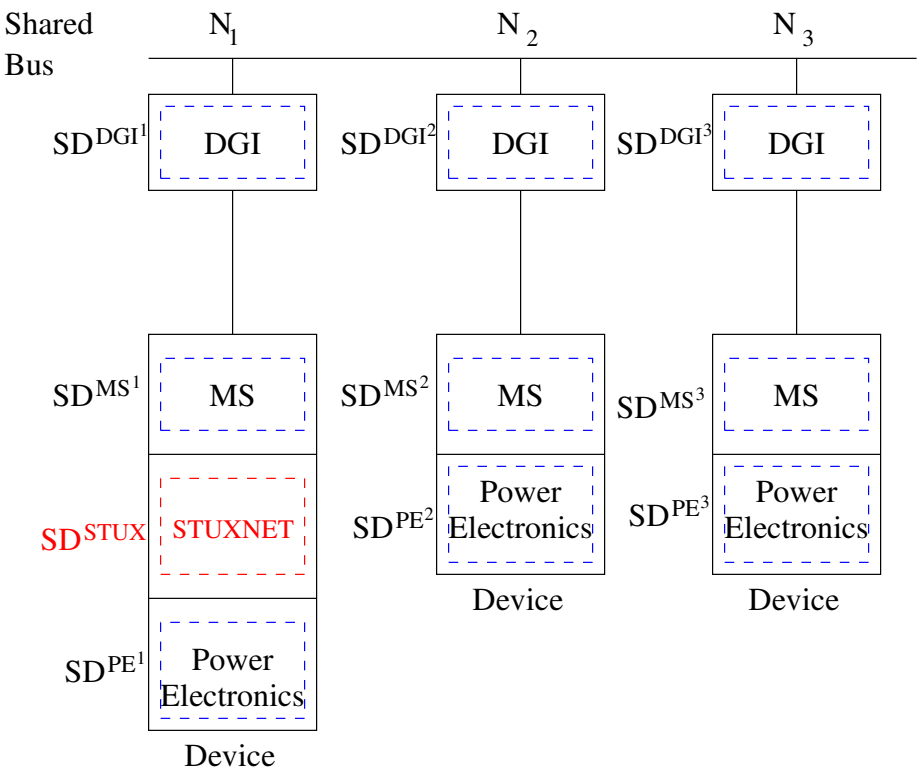

Figure 3.2. 3 Node FREEDM System affected by the STUXNET-like virus

Table 3.1. Attack Model: Details of Security Domains

Security Domain	System Entity
SD^{PE^1}	Power Electronics (Node 1)
SD^{MS^1}	Message Passing Module (Node 1)
SD^{DGI^1}	DGI (Node 1)
SD^{DGI^2}	DGI (Node 2)
SD^{MS^2}	Message Passing Module (Node 2)
SD^{PE^2}	Power Electronics (Node 2)
SD^{DGI^3}	DGI (Node 3)
SD^{MS^3}	Message Passing Module (Node 3)
SD^{PE^3}	Power Electronics (Node 3)
SD^{STUX}	STUXNET-like firus

4. SECURITY ANALYSIS OF THE FREEDM SYSTEM

4.1. STATE COLLECTION PROTOCOL

The task of state collection protocol is to collect the state of each of the devices in FREEDM system and update the same to the DGI. A status message has below parameters or signal types from different devices:

Table 4.1. Devices and signal types

Device Type($Device$)	Device Signal(DS)
SST	gateway
DRER	generation
DESD	storage
LOAD	drain
FID	state

The state collection protocol is based over the distributed snapshot algorithm from Chandy Lamport (Chandy and Lamport, 1985). The protocol works in 2 steps:

1. The initiator node records its own state and broadcasts a marker out to the peers. It also starts recording the messages from other peers until it receives the marker back.

2. A peer node, upon receiving the marker for the first time, records its own state and forwards the marker to the next peer. After recording its own state it also records messages from other peers, until it receives the marker back.

Based over the two stage process this work will perform a security analysis based over multiple security domain nondeducibility in the FREEDM system. The thesis targets the information path available among different devices and analyzes the effect of STUXNET-like virus over the information flowing over the paths.

4.1.1. MSDND Analysis State Collection Protocol - Step 1.

- *DGI - device interaction.* DGI Device interaction is when the state collection protocol takes a local snapshot at the device level. The device here refers to $\{Device \mid device \in SST, DESD, DRER\}$. Each device has a status message or status signal as given in Table 4.1 The set of device signals is given as $\{DS \mid DS \in gateway, storage, generation\}$

  Theorem 4.1.1.1. Under normal conditions device signal status message from a device to DGI is not MSDND secure

  Proof: Under normal conditions status message received by DGI from the devices is correct and the normal functioning of the system is not affected. The depiction of security domains is as shown in Figure 4.1

  Information Flow Path:

  - Power electronics sends the device signal to message passing module
  - Message passing module sends device signal values to DGI

Security Domain	Valuation Function	Correctness
SD^{DGI}	v_{DS}^{DGI}	$True$
SD^{MS}	v_{DS}^{MS}	$True$
SD^{PE}	v_{DS}^{PE}	$True$

  - $DS = True$; device signal status message exchange is normal
  - $I_{MS,PE}(DS)$; PE reports device signal value to Message passing module
  - $B_{MS}I_{MS,PE}(DS)$; MS module believes report from PE
  - $T_{MS,PE}(DS)$; MS module trusts the report from PE

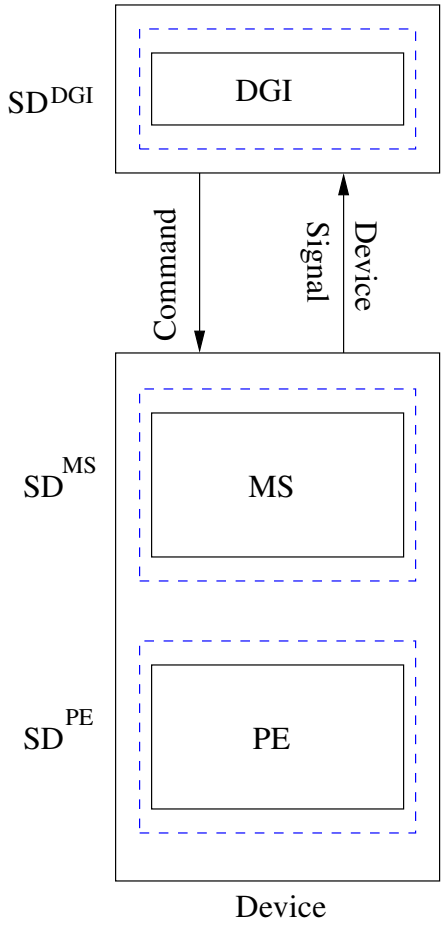

Figure 4.1. DGI device interaction

- $B_{MS}I_{MS,PE}(DS) \wedge T_{MS,PE}(DS) \rightarrow B_{MS}(DS)$; MS believes the reading
- $I_{DGI,MS}(DS)$; MS reports device signal value to DGI
- $B_{DGI}I_{DGI,MS}(DS)$; DGI believes report from MS
- $T_{DGI,MS}(DS)$; DGI module trusts the report from MS
- $B_{DGI}I_{DGI,MS}(DS) \wedge T_{DGI,MS}(DS) \rightarrow B_{DGI}(DS)$; DGI believes the reading
- $w \vDash v_{DS}^{DGI} = True$; There exists valuation function in security domain for DGI

$$MSDND(ES) \neq \exists\, w \in W \vdash [(S_{DS} \oplus S_{\sim DS})] \wedge \left[w \vDash (\exists\, v_{DS}^{DGI}(w) \wedge \exists\, v_{\sim DS}^{DGI}(w))\right]$$

Theorem 4.1.1.2. DGI device communication is MSDND secure in presence of STUXNET-like virus

Proof: Under STUXNET-like virus attack, status message received by DGI from the device is falsified and the normal functioning of the system is affected. The depiction of security domains is as shown in Figure 4.2

Information Flow Path:

- Power electronics sends the device signal value to STUXNET-like virus
- STUXNET-like virus sends device signal values to Message passing module
- Message passing module sends device signal values to DGI

- $\sim DS = True$; Device signal status message exchange is not normal
- $w \vDash V_{DS}^{DGI} = False$; No valuation function in DGI security domain for storage values
- $I_{STUX,PE}(\sim DS)$; PE reports device signal value to STUXNET-like virus
- $B_{STUX}I_{STUX,PE}(\sim DS)$; STUXNET-like virus believes report from PE
- $T_{STUX,PE}(\sim DS)$; STUXNET-like virus trusts the report from PE

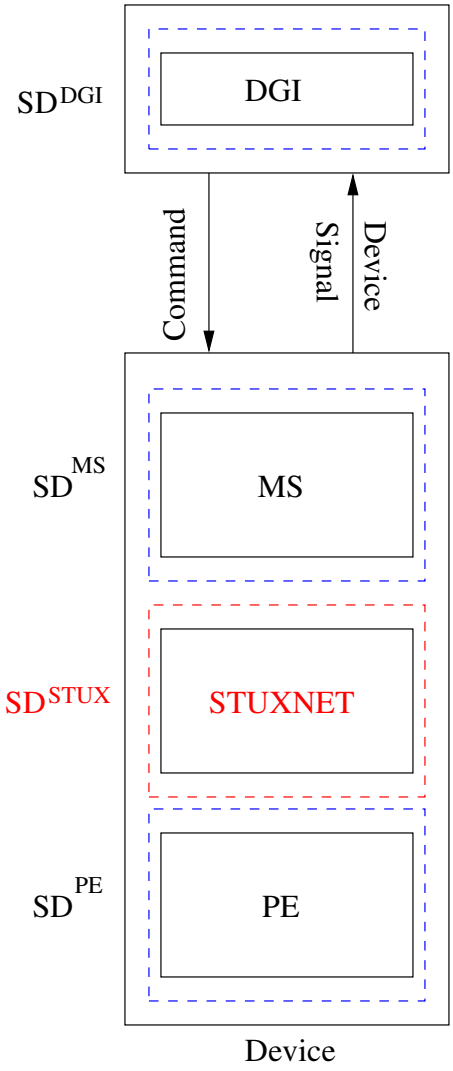

Figure 4.2. DGI device interaction under virus attack

- $B_{STUX} I_{STUX,PE}(\sim DS) \wedge T_{STUX,PE}(\sim DS) \rightarrow B_{STUX}(\sim DS)$; STUXNET-like virus believes the reading
- $I_{MS,STUX}(DS)$; STUXNET-like virus reports modified device signal value to MS
- $B_{MS} I_{MS,STUX}(DS)$; MS module believes report from STUXNET-like virus
- $T_{MS,STUX}(DS)$; MS module trusts the report from STUXNET-like virus
- $B_{MS} I_{MS,STUX}(DS) \wedge T_{MS,STUX}(DS) \rightarrow B_{MS}(DS)$; MS module believes the reading
- $I_{DGI,MS}(DS)$; MS reports device signal value to DGI
- $B_{DGI} I_{DGI,MS}(DS)$; DGI believes report from MS
- $T_{DGI,MS}(DS)$; DGI module trusts the report from MS
- $B_{DGI} I_{DGI,MS}(DS) \wedge T_{DGI,MS}(DS) \rightarrow B_{DGI}(DS)$; DGI believes the reading
- $w \vDash v_{DS}^{DGI} = False$; No valuation function exists in security domain for DGI

$$MSDND(ES) = \exists w \in W \vdash [(S_{DS} \oplus S_{\sim DS})] \wedge \left[w \vDash (\nexists v_{DS}^{DGI}(w) \wedge \nexists v_{\sim DS}^{DGI}(w)) \right]$$

4.1.2. MSDND Analysis State Collection protocol - Step 2. State collection protocol, in its first step asks a DGI node to collect a local snapshot of the system state and send a marker to all its peer nodes. Once the marker is sent, the DGI listens to all the communication from peer nodes until it receives the marker back. This marks the second step of the state collection protocol. The protocol targets all the different device types and status message types associated with them. This work considers each of the device types and messages below in detail.

- *DGI - DGI Interaction* Device types in the FREEDM system report their signal status value to DGI. The details of device types and their associated signal values are given in Table 4.1. The status signal message is shared with the DGI which in turn shares it with peer DGI nodes as part of step 2 of the state collection protocol.

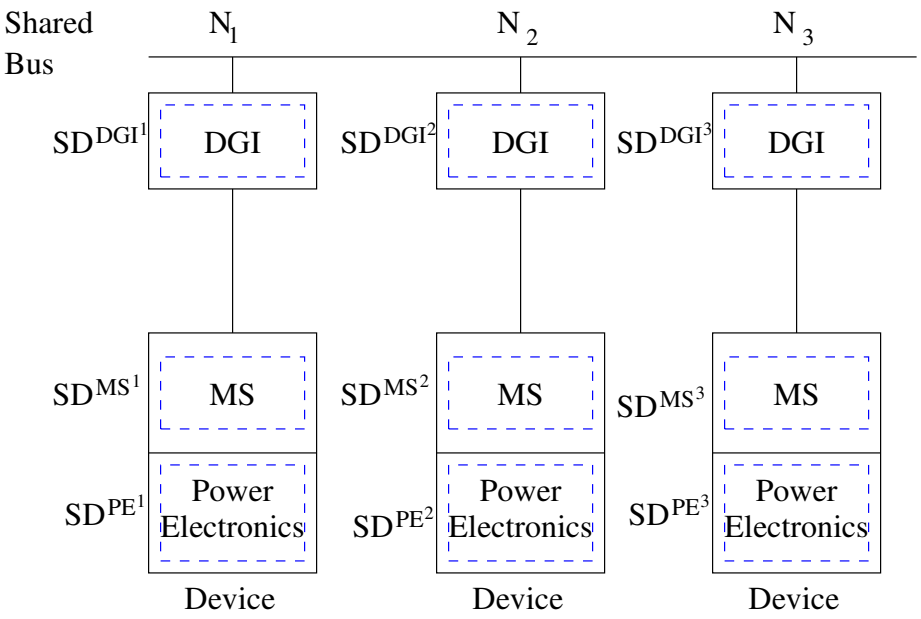

Figure 4.3. DGI DGI interaction under normal operations

Theorem 4.1.2.1. Under normal conditions the state collection protocol communication between two DGI nodes is not MSDND secure

Proof: Under normal conditions status message received by peer nodes from any other node is correct and the normal functioning of the system is not affected. The depiction of security domains is as shown in Figure 4.3

Information Flow Path:

- Node 1 Power electronics sends the device signal value to node 1 message passing module
- Node 1 message passing module sends device signal values to node 1 DGI
- Node 1 DGI sends the status message to Node 2 DGI and Node 3 DGI

Security Domain	Valuation Function	Correctness
SD^{PE^1}	$v_{DS}^{PE^1}$	$True$
SD^{MS^1}	$v_{DS}^{MS^1}$	$True$
SD^{DGI^1}	$V_{DS}^{DGI^1}$	$True$
SD^{DGI^2}	$V_{DS}^{DGI^2}$	$True$
SD^{DGI^3}	$V_{DS}^{DGI^3}$	$True$

- $DS = True$; Device signal status message exchange is normal
- $I_{MS^1,PE^1}(DS)$; Node 1 PE reports device signal value to node 1 message passing module
- $B_{MS^1} I_{MS^1,PE^1}(DS)$; Node 1 MS module believes report from node 1 PE
- $T_{MS^1,PE^1}(DS)$; Node 1 MS module trusts the report from node 1 PE
- $B_{MS^1} I_{MS^1,PE^1}(DS) \wedge T_{MS^1,PE^1}(DS) \rightarrow B_{MS^1}(DS)$; Node 1 MS believes the reading
- $I_{DGI^1,MS^1}(DS)$; Node 1 MS reports device signal value to node 1 DGI
- $B_{DGI^1} I_{DGI^1,MS^1}(DS)$; Node 1 DGI believes report from node 1 MS
- $T_{DGI^1,MS^1}(DS)$; node 1 DGI module trusts the report from MS
- $B_{DGI^1} I_{DGI^1,MS^1}(DS) \wedge T_{DGI^1,MS^1}(DS) \rightarrow B_{DGI^1}(DS)$; Node 1 DGI believes the reading
- $I_{DGI^2,DGI^1}(DS)$; Node 1 DGI reports device signal value to node 2 DGI
- $B_{DGI^2} I_{DGI^2,DGI^1}(DS)$; node 2 DGI believes report from node 1 DGI
- $T_{DGI^2,DGI^1}(DS)$; node 2 DGI module trusts the report from node 1 DGI
- $B_{DGI^2} I_{DGI^2,DGI^1}(DS) \wedge T_{DGI^2,DGI^1}(DS) \rightarrow B_{DGI^2}(DS)$; Node 2 DGI believes the reading
- $I_{DGI^3,DGI^1}(DS)$; Node 1 DGI reports device signal value to node 3 DGI
- $B_{DGI^3} I_{DGI^3,DGI^1}(DS)$; node 3 DGI believes report from node 1 DGI
- $T_{DGI^3,DGI^1}(DS)$; node 3 DGI module trusts the report from node 1 DGI
- $B_{DGI^3} I_{DGI^3,DGI^1}(DS) \wedge T_{DGI^3,DGI^1}(DS) \rightarrow B_{DGI^3}(DS)$; Node 3 DGI believes the reading

- $w \vDash v_{DS}^{DGI^2} = True$; There exists valuation function in security domain for node 2 DGI
- $w \vDash v_{DS}^{DGI^3} = True$; There exists valuation function in security domain for node 3 DGI

$$MSDND(ES) \neq \exists w \in W \vdash [(S_{DS} \oplus S_{\sim DS})] \wedge \left[w \vDash (\exists v_{DS}^{DGI^2}(w) \wedge \exists V_{\sim DS}^{DGI^2}(w))\right]$$
$$MSDND(ES) \neq \exists w \in W \vdash [(S_{DS} \oplus S_{\sim DS})] \wedge \left[w \vDash (\exists v_{DS}^{DGI^3}(w) \wedge \exists v_{\sim DS}^{DGI^3}(w))\right]$$

Theorem 4.1.2.2. State collection communication between two DGI nodes is MSDND secure in presence of STUXNET-like virus

Proof: Under STUXNET-like virus attack, status message exchange between two DGI nodes is not normal and the functioning of the system is affected. The depiction of security domains is as shown in Figure 4.4

Information Flow Path:

- Node 1 power electronics sends the device signal value to STUXNET-like virus
- STUXNET-like virus sends device signal values to node 1 message passing module
- Node 1 message passing module sends device signal values to node 1 DGI
- Node 1 DGI sends device signal values to node 2 DGI and node 3 DGI

- $\sim DS = True$; Device signal status message exchange is not normal
- $w \vDash V_{DS}^{DGI^2} = False$; No valuation function in security domain for node 2 DGI
- $I_{STUX,PE^1}(\sim DS)$; Node 1 PE reports device signal status message value to STUXNET-like virus
- $B_{STUX} I_{STUX,PE^1}(\sim DS)$; STUXNET-like virus believes report from node 1 PE
- $T_{STUX,PE^1}(\sim DS)$; STUXNET-like virus trusts the report from node 1 PE
- $B_{STUX} I_{STUX,PE^1}(\sim DS) \wedge T_{STUX,PE^1}(\sim DS) \rightarrow B_{STUX}(\sim DS)$; STUXNET-like virus believes the reading

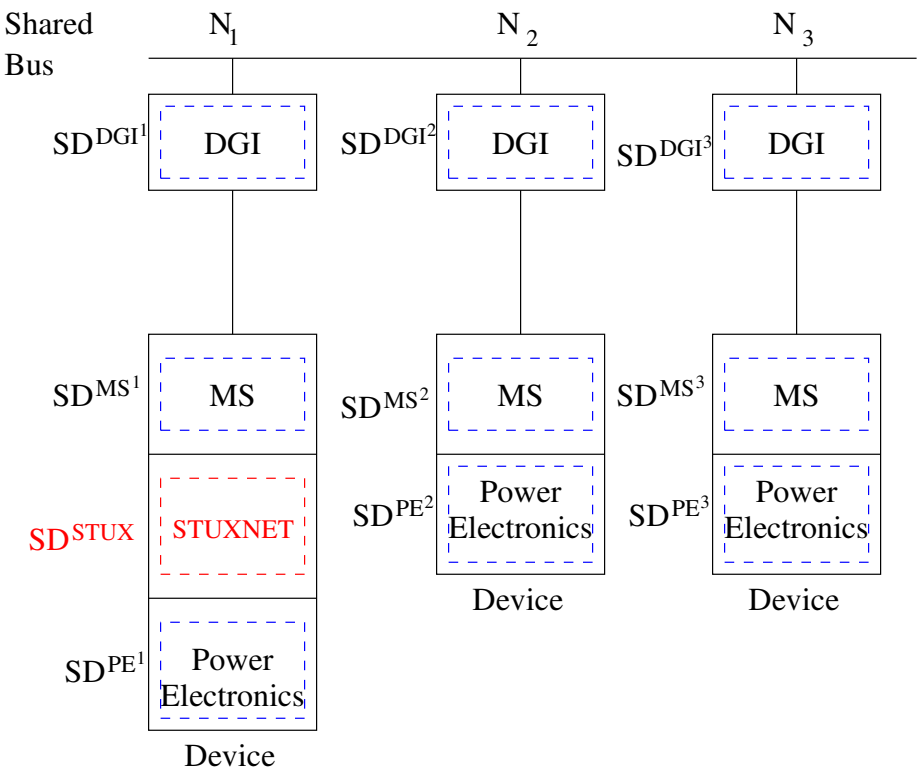

Figure 4.4. DGI DGI interaction under STUXNET-like virus attack

– $I_{MS^1,STUX}(stor)$; STUXNET-like virus reports modified device signal value to node 1 MS
– $B_{MS^1} I_{MS^1,STUX}(DS)$; Node 1 MS module believes report from STUXNET-like virus.
– $T_{MS^1,STUX}(DS)$; Node 1 MS module trusts the report from STUXNET-like virus
– $B_{MS^1} I_{MS^1,STUX}(DS) \wedge T_{MS^1,STUX}(DS) \rightarrow B_{MS^1}(DS)$; Node 1 MS module believes the reading
– $I_{DGI^1,MS^1}(DS)$; Node 1 MS reports device signal value to node 1 DGI
– $B_{DGI^1} I_{DGI^1,MS^1}(DS)$; Node 1 DGI believes report from node 1 MS
– $T_{DGI^1,MS^1}(DS)$; Node 1 DGI module trusts the report from node 1 MS
– $B_{DGI^1} I_{DGI^1,MS^1}(MS) \wedge T_{DGI^1,MS^1}(DS) \rightarrow B_{DGI^1}(DS)$; Node 1 DGI believes the reading
– $I_{DGI^2,DGI^1}(DS)$; Node 1 DGI reports device signal value to node 2 DGI

- $B_{DGI^2} I_{DGI^2,DGI^1}(DS)$; node 2 DGI believes report from node 1 DGI
- $T_{DGI^2,DGI^1}(DS)$; node 2 DGI module trusts the report from node 1 DGI
- $B_{DGI^2} I_{DGI^2,DGI^1}(DS) \wedge T_{DGI^2,DGI^1}(DS) \rightarrow B_{DGI^2}(DS)$; Node 2 DGI believes the reading
- $I_{DGI^3,DGI^2}(DS)$; Node 1 DGI reports device signal value to node 3 DGI
- $B_{DGI^3} I_{DGI^3,DGI^2}(DS)$; node 3 DGI believes report from node 1 DGI
- $T_{DGI^3,DGI^2}(DS)$; node 3 DGI module trusts the report from node 1 DGI
- $B_{DGI^3} I_{DGI^3,DGI^2}(DS) \wedge T_{DGI^3,DGI^2}(DS) \rightarrow B_{DGI^3}(DS)$; Node 3 DGI believes the reading
- $w \vDash v_{DS}^{DGI^2} = False$; No valuation function exists in security domain for Node 2 DGI
- $w \vDash v_{DS}^{DGI^3} = False$; No valuation function exists in security domain for Node 3 DGI

$$MSDND(ES) = \exists\, w \in W \vdash [(S_{DS} \oplus S_{\sim DS})] \wedge \left[w \vDash (\nexists\, v_{DS}^{DGI^2}(w) \wedge \nexists\, v_{\sim DS}^{DGI^2}(w))\right]$$

$$MSDND(ES) = \exists\, w \in W \vdash [(S_{DS} \oplus S_{\sim DS})] \wedge \left[w \vDash (\nexists\, v_{DS}^{DGI^3}(w) \wedge \nexists\, v_{\sim DS}^{DGI^3}(w))\right]$$

Theorem 4.1.2.3. State collection marker message communication between two DGI nodes is MSDND secure in presence of STUXNET-like virus

Proof: Under STUXNET-like virus attack on the DGI, the marker message exchange between two DGI nodes is not normal and the functioning of the system is affected. It is worth noting here that the impact of such an attack will be concentrated to the affected DGI and its peer nodes. Marker message here is represented as MM

Case a. Considering node 1 as the initiator of state collection protocol as well as the malicious node The depiction of security domains is as shown in Figure 4.5

Information Flow Path:

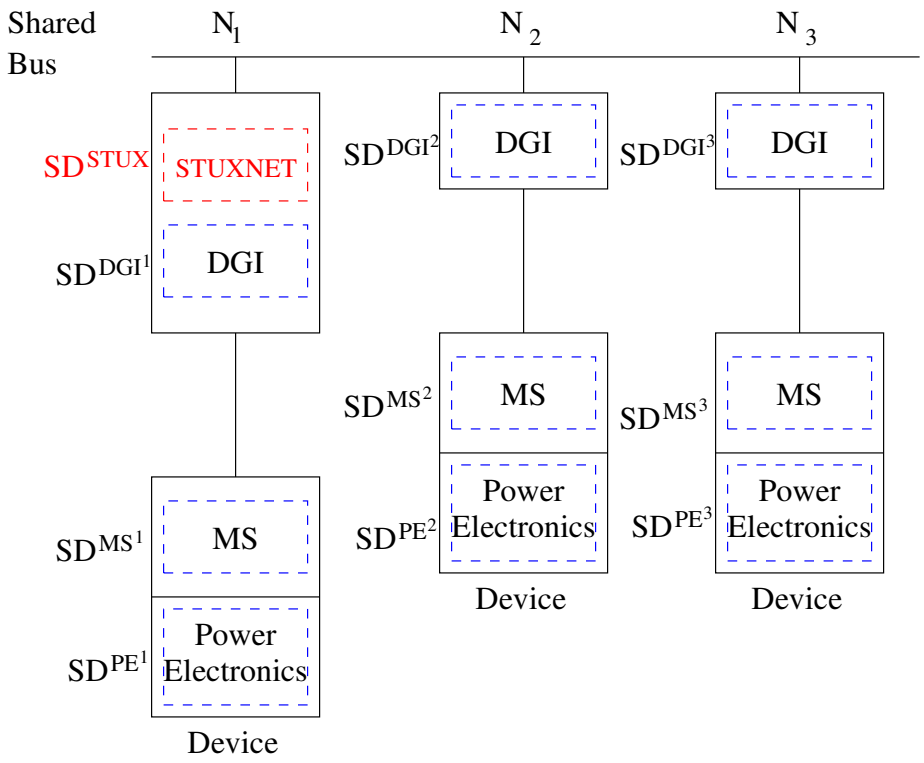

Figure 4.5. Initiator node marker message communication under STUXNET-like virus attack

- Node 1 is the initiator of state collection, and initiates a local system snapshot
- Node 1 power electronics sends the device signal value to node 1 message passing virus
- Node 1 message passing module sends the device signal value to node 1 DGI virus
- Node 1 DGI sends the device signal value to stuxnet-like virus
- STUXNET-like virus receives the local parameters, however does not send a marker to peer nodes to collect global states.

- $DS = True$; Device signal status message exchange is not normal
- $w \vDash V_{DS}^{DGI^1} = True$;Valuation function exists in security domain for node 1 DGI
- $I_{MS^1,PE^1}(DS)$; Node 1 PE reports device signal status message value to node 1 message passing module

- $B_{MS^1} I_{MS^1,PE^1}(DS)$; Node 1 message passing module believes report from node 1 PE
- $T_{MS^1,PE^1}(DS)$; Node 1 message passing module trusts the report from node 1 PE
- $B_{MS^1} I_{MS^1,PE^1}(DS) \wedge T_{MS^1,PE^1}(DS) \rightarrow B_{MS^1}(DS)$; Node 1 message passing module believes the reading
- $I_{DGI^1,MS^1}(DS)$; Node 1 MS reports device signal value to node 1 DGI
- $B_{DGI^1} I_{DGI^1,MS^1}(DS)$; Node 1 DGI believes report from node 1 MS
- $T_{DGI^1,MS^1}(DS)$; Node 1 DGI module trusts the report from node 1 MS
- $B_{DGI^1} I_{DGI^1,MS^1}(MS) \wedge T_{DGI^1,MS^1}(DS) \rightarrow B_{DGI^1}(DS)$; Node 1 DGI believes the reading
- Step 2 of the state collection protocol is initiated, i.e., sending the marker node to peer nodes for global state collection.
- The STUXNET-like virus observes this request and stops the global state collection by not forwarding the marker message to peer nodes.
- Since node N_1 is the initiator node for state collection protocol and no marker message is sent to peer nodes, step 2 of the state collection protocol does not take place.
- Peer nodes are not aware of the existence of node N_1
- $w \vDash v_{DS}^{DGI^1} = True$; Valuation function exists in security domain for Node 1 DGI
- $w \vDash v_{DS}^{DGI^2} = False$; No valuation function exists in security domain for Node 2 DGI
- $w \vDash v_{DS}^{DGI^3} = False$; No valuation function exists in security domain for Node 3 DGI

$$MSDND(ES) = \exists w \in W \vdash [(S_{DS} \oplus S_{\sim DS})] \wedge \left[w \vDash (\nexists v_{DS}^{DGI^2}(w) \wedge \nexists v_{\sim DS}^{DGI^2}(w))\right]$$

$$MSDND(ES) = \exists w \in W \vdash [(S_{DS} \oplus S_{\sim DS})] \wedge \left[w \vDash (\nexists v_{DS}^{DGI^3}(w) \wedge \nexists v_{\sim DS}^{DGI^3}(w))\right]$$

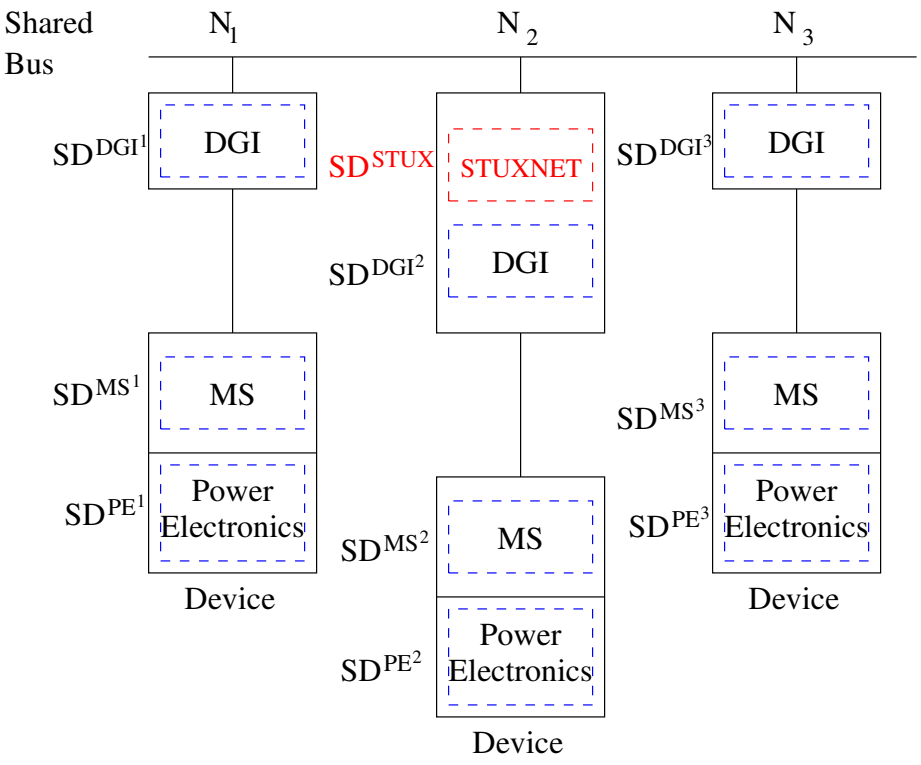

Figure 4.6. Peer node marker message communication under STUXNET-like virus attack

Case b. Considering node N_1 as the initiator of state collection protocol and Node N_2 as the malicious node The depiction of security domains is as shown in Figure 4.6

Information Flow Path:

- Node 1 is the initiator of state collection, and initiates a local system snapshot
- Node 1 power electronics sends the device signal value to node 1 message passing virus
- Node 1 message passing module sends the device signal value to node 1 DGI virus
- Node 1 DGI sends the device signal value and marker message to its peer nodes
- The STUXNET-like virus in node 2 receives the parameters and marker message, however chooses not to send a marker to peer nodes to collect global states and returns the marker back to Node 1 DGI.

- $DS = True$; Device signal status message exchange is normal
- $w \vDash V_{DS}^{DGI^1} = True$;Valuation function exists in security domain for node 1 DGI
- $I_{MS^1,PE^1}(DS)$; Node 1 PE reports device signal status message value to node 1 message passing module
- $B_{MS^1} I_{MS^1,PE^1}(DS)$; Node 1 message passing module believes report from node 1 PE
- $T_{MS^1,PE^1}(DS)$; Node 1 message passing module trusts the report from node 1 PE
- $B_{MS^1} I_{MS^1,PE^1}(DS) \wedge T_{MS^1,PE^1}(DS) \rightarrow B_{MS^1}(DS)$; Node 1 message passing module believes the reading
- $I_{DGI^1,MS^1}(DS)$; Node 1 MS reports device signal value to node 1 DGI
- $B_{DGI^1} I_{DGI^1,MS^1}(DS)$; Node 1 DGI believes report from node 1 MS
- $T_{DGI^1,MS^1}(DS)$; Node 1 DGI module trusts the report from node 1 MS
- $B_{DGI^1} I_{DGI^1,MS^1}(MS) \wedge T_{DGI^1,MS^1}(DS) \rightarrow B_{DGI^1}(DS)$; Node 1 DGI believes the reading
- $I_{STUX,DGI^1}(DS)$; Node 1 DGI reports device signal value to STUXNET-like virus
- $B_{STUX} I_{STUX,DGI^1}(DS)$; SYUXNET-like virus believes report from node 1 DGI
- $T_{STUX,DGI^1}(DS)$; STUXNET-like virus trusts the report from node 1 DGI
- $B_{STUX} I_{STUX,DGI^1}(DS) \wedge T_{STUX,DGI^1}(DS) \rightarrow B_{STUX}(DS)$; STUXNET-like virus believes the reading
- $I_{STUX,DGI^1}(MM)$; Node 1 DGI reports marker message to STUXNET-like virus
- $B_{STUX} I_{STUX,DGI^1}(MM)$; SYUXNET-like virus believes report from node 1 DGI
- $T_{STUX,DGI^1}(MM)$; STUXNET-like virus trusts the report from node 1 DGI
- $B_{STUX} I_{STUX,DGI^1}(MM) \wedge T_{STUX,DGI^1}(MM) \rightarrow B_{STUX}(MM)$; STUXNET-like virus believes the reading and receives the marker message from node 1 DGI
- The STUXNET-like virus observes this request and stops the global state collection by not forwarding the marker message to peer nodes.
- Node N_1 is the initiator node for state collection protocol and receives the marker message back from node N_2

- The marker message received from node N_2 marks the completion of global state collection for node N_1
- Node N_1 is not aware of the global state, which could lead to inconsistency in the system.
- $w \vDash v_{DS}^{DGI^1} = False$; No valuation function exists in security domain for Node 1 DGI
- $w \vDash v_{DS}^{DGI^3} = False$; No valuation function exists in security domain for Node 3 DGI

$$MSDND(ES) = \exists\, w \in W \vdash [(S_{DS} \oplus S_{\sim DS})] \wedge \left[w \vDash (\nexists\, v_{DS}^{DGI^1}(w) \wedge \nexists\, v_{\sim DS}^{DGI^1}(w))\right]$$

$$MSDND(ES) = \exists\, w \in W \vdash [(S_{MM} \oplus S_{\sim MM})] \wedge \left[w \vDash (\nexists\, v_{MM}^{DGI^1}(w) \wedge \nexists\, v_{\sim MM}^{DGI^1}(w))\right]$$

$$MSDND(ES) = \exists\, w \in W \vdash [(S_{DS} \oplus S_{\sim DS})] \wedge \left[w \vDash (\nexists\, v_{DS}^{DGI^3}(w) \wedge \nexists\, v_{\sim DS}^{DGI^3}(w))\right]$$

$$MSDND(ES) = \exists\, w \in W \vdash [(S_{MM} \oplus S_{\sim MM})] \wedge \left[w \vDash (\nexists\, v_{MM}^{DGI^3}(w) \wedge \nexists\, v_{\sim MM}^{DGI^3}(w))\right]$$

4.2. INTRODUCING DEDUCIBILITY IN CONSENSUS BASED STATE COLLECTION PROTOCOL USING BYZANTINE AGREEMENT

In the previous sections this work demonstrated different ways in which the FREEDM system is exposed to STUXNET-like attacks making the system as MSDND secure. For a cyber physical system such as the FREEDM system an MSDND secure system is good for an attacker. In further sections this work will try to break the MSDND secure information flow paths with the help of Byzantine agreement. Our motive is to use the cyber properties of the system in order to verify the information flowing through the paths, thus, changing the state of system from MSDND secure to not MSDND secure.

- *Modelling Byzantine Agreement Problem as Part of the FREEDM System*

Byzantine agreement problem is the classic representation of a distributed system in which one or more components lie about their states to all the other components. This may lead to incorrect decisions or system instability due to incorrect information flowing among the system. As for the FREEDM system, one or more nodes can lie about their local states to the global state collection, hence a possibility of system instability or incorrect decisions.

An important condition based over the solution to the Byzantine agreement problem by Leslie Lamport (Lamport *et al.*, 1982) is the relation between total number of nodes and faulty nodes in the system. The relation is given as below:

$$n > 3m$$

Where, n = total number of nodes and m = faulty nodes in the system. From the above relation we have below:

m (faulty nodes)	relation	nodes
0	$n > 3(0)$	NA
1	$n > 3(1)$	4
2	$n > 3(2)$	7

Therefore, with one faulty node, a minimum of 4 nodes in the FREEDM system is required. Expanding upon the condition this work analyzes the state collection protocol for a 4 node FREEDM system. For the state collection protocol an initiator node initiates the protocol. A depiction of the 4 node system is shown in Figure 4.7

- *Analyzing Byzantine agreement as part of consensus based state collection protocol*

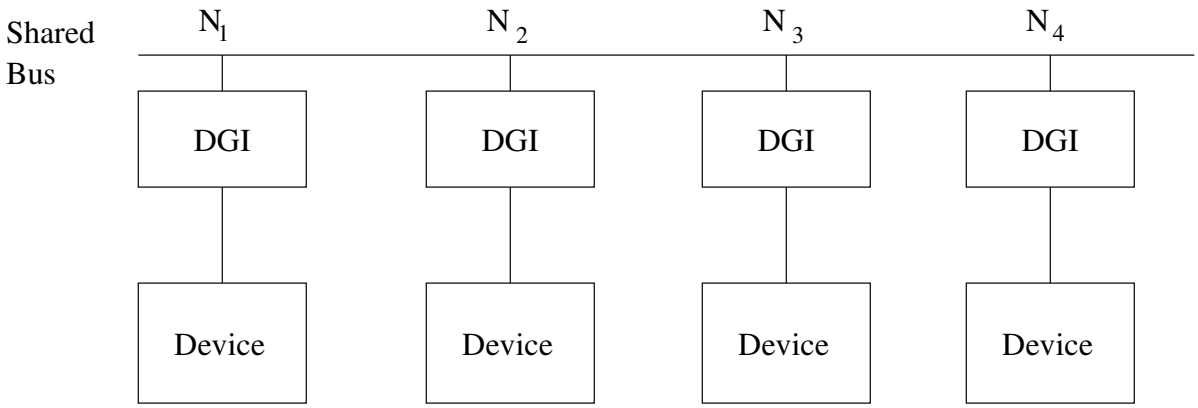

Figure 4.7. 4 Node FREEDM system

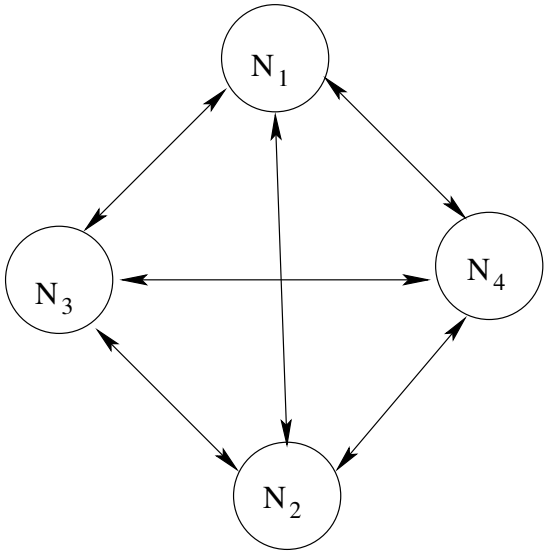

Figure 4.8. Message flow in a 4 node system

The message flow in consensus based state collection protocol is such that all the nodes can read messages from all the other nodes, hence, forming a completely connected graph as in Figure 4.8:

Each node as shown in 4.8 will send the device signal values to every other node as in Figure 4.9:

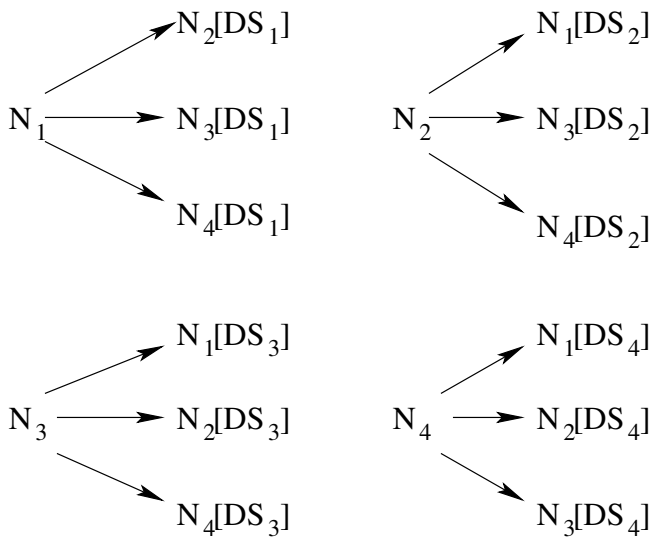

Figure 4.9. Device signal status message flow in a 4 node system

The above shows that each node will send its device signal value to every other node. A parallel execution of consensus based state collection protocol will take place at every node. Owing to a basic constraint given by the Byzantine Agreement problem $n > 3m$ where, n is the total number of nodes and m is the number of malicious nodes, this work assumes node N_1 or node 1 is the malicious node.

This work considers node N_1 is the initiator of state collection protocol and is the malicious node in the 4 node system.

Assumptions:

- Only Node N_1 is the malicious node
- Node N_1 is the initiator of the consensus based state collection protocol

- Node N_1 tries to falsify device signal status message by sending different values to different nodes (the motive of the Node is to destabilize the system)
- Identity of message sender can be authenticated

Since there is only 1 faulty node there will be $m + 1$ rounds of message exchange.

Round 0: In this round node N_1 shares device signal values to all the other nodes i.e. nodes N_2, N_3 and N_4. Figure 4.10 diplays the representation of round 0 when Node N_1 is the initiator for consensus based state collection protocol

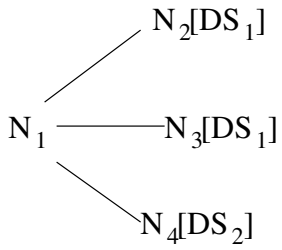

Figure 4.10. Round 0 message exchange

Clearly, in Figure 4.10 Node N_1 sends different generation values to nodes N_2, N_3 and N_4.

Round 1: Now the nodes N_2, N_3 and N_4 will share the messages with each other. Below are the details:

Sender = N_2		Sender = N_3		Sender = N_4	
Dest	Msg	Dest	Msg	Dest	Msg
N_2	$\{DS_1, 12\}$	N_2	$\{DS_1, 13\}$	N_2	$\{DS_2, 14\}$
N_3	$\{DS_1, 12\}$	N_3	$\{DS_1, 13\}$	N_3	$\{DS_2, 14\}$
N_4	$\{DS_1, 12\}$	N_4	$\{DS_1, 13\}$	N_4	$\{DS_2, 14\}$

From the above message details it can be identified that Node N_1 is the malicious node as it is trying to send different device signal values to different nodes. For example:

After round 1 the message details with node N_2 will be:

$\{DS_1, 12\}, \{DS_1, 13\}, \{DS_2, 14\}, \{DS_1, 1\}$

Clearly, from the above it can be established either node N_1 or node N_4 is malicious. Hence in such a case a legitimate migration contract should restrict participation of node N_1 and node N_4. A similar consensus based comparison will take place at node N_3 and node N_4. This will improve the formulation of migration contracts among processes that are not lying about their states to other nodes.

Theorem 4.2.1. The system is not MSDND secure in a 4 node system (Figure 4.11) with Byzantine consensus formulation when the malicious node tries to share different status messages to different nodes. *Proof:* Since the initiator node is malicious node sharing a different status message to different nodes leads to a failure to comply with *interactive consistency 2*, which implies that if the commander or initiator is loyal, every other node in the system should receive similar status message. Figure 4.12 depicts the BIT logic flow. The MSDND proof below corroborates the same:

Information Flow Path:

- Node 1 Power electronics sends the device signal value to STUXNET
- STUXNET sends those values to Node 1 Message passing module
- Node 1 Message passing module sends those messages to node 1 DGI
- Node 1 DGI sends message to node 2 DGI, node 3 DGI and node 4 DGI
- Now all nodes except the initiator node 1 send their messages to all the peer nodes

- $\sim DS = True$; Device signal status message exchange is not normal
- $I_{STUX,PE^1}(\sim DS)$; Node 1 PE reports generation value to STUXNET-like virus
- $B_{STUX} I_{STUX,PE^1}(\sim gen)$; STUXNET-like virus believes report from Node 1 PE
- $T_{STUX,PE^1}(\sim DS)$; STUXNET-like virus trusts the report from Node 1 PE
- $B_{STUX} I_{STUX,PE^1}(\sim DS) \wedge T_{STUX,PE^1}(\sim DS) \rightarrow B_{STUX}(\sim DS)$; STUXNET-like virus believes the reading

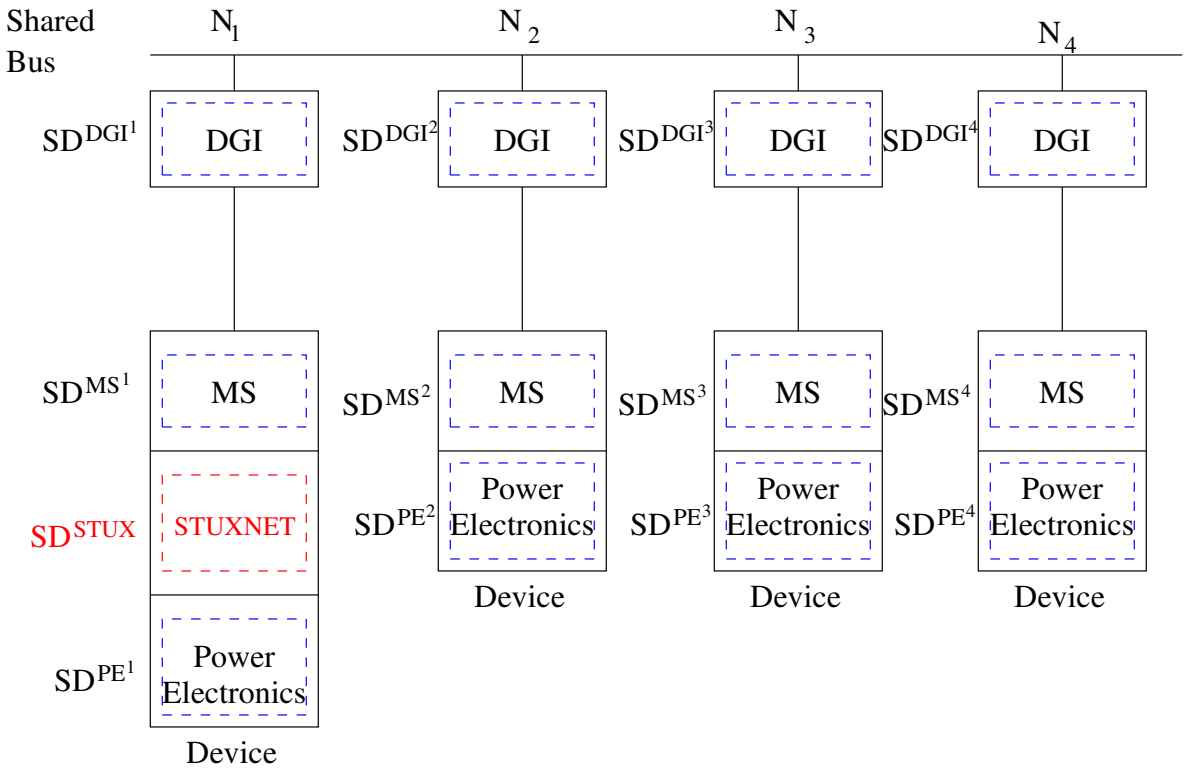

Figure 4.11. 4 node FREEDM system under STUXNET-like virus attack

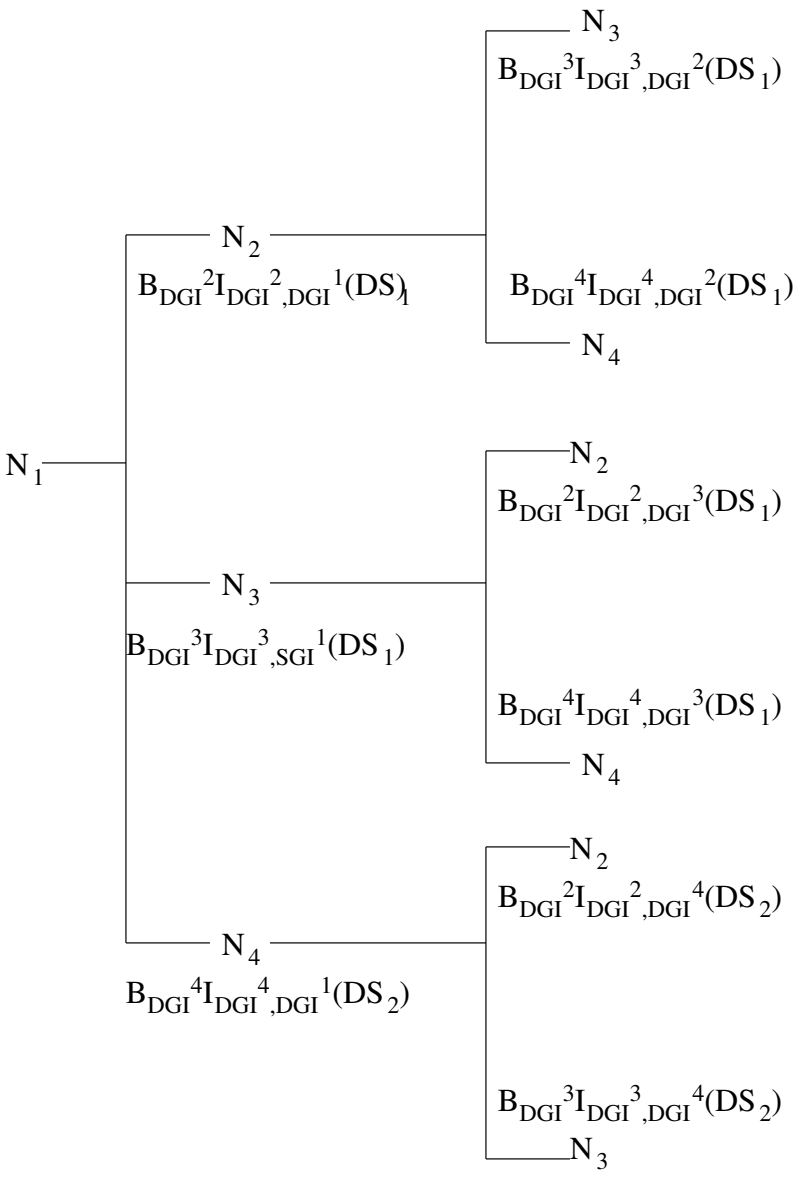

Figure 4.12. Failed interactive consistency and MSDND - BIT logic view Byzantine Agreement

Now the STUXNET-like virus overwrites the true device signal value and sends different values to different nodes. Without loss of generality the message transfer takes place as recorded below:

- Node 1 DGI will send DS_1 as device signal value to Node 2 DGI
- Node 1 DGI will send DS_1 as device signal value to Node 3 DGI
- Node 1 DGI will send DS_2 as device signal value to Node 4 DGI

All message transformation or masking is performed by the STUXNET-like virus and the same is sent to different nodes. The further analysis of MSDND takes place at the DGI security domains. BIT logic formulation of round 0:

- $I_{DGI^2,DGI^1}(DS_1)$; Node 1 DGI reports device signal value to Node 2 DGI
- $B_{DGI^2}I_{DGI^2,DGI^1}(DS_1)$; Node 2 DGI believes report from Node 1 DGI
- $T_{DGI^2,DGI^1}(DS_1)$; Node 2 DGI trusts the report from Node 1 DGI
- $I_{DGI^3,DGI^1}(DS_1)$; Node 1 DGI reports device signal value to Node 3 DGI
- $B_{DGI^3}I_{DGI^3,DGI^1}(DS_1)$; Node 3 DGI believes report from Node 1 DGI
- $T_{DGI^3,DGI^1}(DS_1)$; Node 3 DGI trusts the report from Node 1 DGI
- $I_{DGI^4,DGI^1}(DS_2)$; Node 1 DGI reports a different device signal value to Node 4 DGI
- $B_{DGI^4}I_{DGI^4,DGI^1}(DS_2)$; Node 4 DGI believes report from Node 1 DGI
- $T_{DGI^4,DGI^1}(DS_2)$; Node 4 DGI trusts the report from Node 1 DGI

BIT logic formulation of round 1:

- $I_{DGI^3,DGI^2}(DS_1)$; Node 2 DGI reports device signal value to Node 3 DGI that it received from Node 1 DGI
- $B_{DGI^3}I_{DGI^3,DGI^2}(DS_1)$; Node 3 DGI believes report from Node 2 DGI
- $T_{DGI^3,DGI^2}(DS_1)$; Node 3 DGI trusts the report from Node 2 DGI

- $I_{DGI^4,DGI^2}(DS_1)$; Node 2 DGI reports device signal value to Node 4 DGI that it received from Node 1 DGI
- $B_{DGI^4} I_{DGI^4,DGI^2}(DS_1)$; Node 4 DGI believes report from Node 2 DGI
- $T_{DGI^4,DGI^2}(DS_1)$; Node 4 DGI trusts the report from Node 2 DGI
- $I_{DGI^2,DGI^3}(DS_1)$; Node 3 DGI reports device signal value to Node 2 DGI that it received from Node 1 DGI
- $B_{DGI^2} I_{DGI^2,DGI^3}(DS_1)$; Node 2 DGI believes report from Node 3 DGI
- $T_{DGI^2,DGI^3}(DS_1)$; Node 2 DGI trusts the report from Node 3 DGI
- $I_{DGI^4,DGI^3}(DS_1)$; Node 3 DGI reports device signal value to Node 4 DGI that it received from Node 1 DGI
- $B_{DGI^4} I_{DGI^4,DGI^3}(DS_1)$; Node 4 DGI believes report from Node 3 DGI
- $T_{DGI^4,DGI^3}(DS_1)$; Node 4 DGI trusts the report from Node 3 DGI
- $I_{DGI^2,DGI^4}(DS_2)$; Node 4 DGI reports device signal value to Node 2 DGI that it received from Node 1 DGI
- $B_{DGI^2} I_{DGI^2,DGI^4}(DS_2)$; Node 2 DGI believes report from Node 4 DGI
- $T_{DGI^2,DGI^4}(DS_2)$; Node 2 DGI trusts the report from Node 4 DGI
- $I_{DGI^3,DGI^4}(DS_2)$; Node 4 DGI reports device signal value to Node 3 DGI that it received from Node 1 DGI
- $B_{DGI^3} I_{DGI^3,DGI^4}(DS_2)$; Node 3 DGI believes report from Node 4 DGI
- $T_{DGI^3,DGI^4}(DS_2)$; Node 3 DGI trusts the report from Node 4 DGI

Now combining all the BIT logic formulated until now to force deducibility:

- At Node 2:

  $[B_{DGI^2} I_{DGI^2,DGI^3}(DS_1) \wedge T_{DGI^2,DGI^3}(DS_1)]$

  $\wedge [B_{DGI^2} I_{DGI^2,DGI^4}(DS_2) \wedge T_{DGI^2,DGI^4}(DS_2)]$

$\wedge [B_{DGI^2} I_{DGI^2,DGI^1}(DS_1 \wedge T_{DGI^2,DGI^1}(DS_1))] \rightarrow\sim B_{DGI^2}(DS_1)$;Node 2 DGI does not believe the reading. Clearly either one of node 1 or node 4 are lying about the device signal values to node 2

- At Node 3:

  $[B_{DGI^3} I_{DGI^3,DGI^1}(DS_1) \wedge T_{DGI^3,DGI^1}(DS_1)]$

  $\wedge [B_{DGI^3} I_{DGI^3,DGI^2}(DS_1) \wedge T_{DGI^3,DGI^2}(DS_1)]$

  $\wedge [B_{DGI^3} I_{DGI^3,DGI^4}(DS_2) \wedge T_{DGI^3,DGI^4}(DS_2)] \rightarrow\sim B_{DGI^3}(DS_1)$;Node 3 DGI does not believe the reading. Clearly either one of node 1 or node 4 are lying about the device signal values to node 3

- At Node 4:

  $[B_{DGI^4} I_{DGI^4,DGI^3}(DS_2) \wedge T_{DGI^4,DGI^1}(DS_2)]$

  $\wedge [B_{DGI^4} I_{DGI^4,DGI^2}(DS_1) \wedge T_{DGI^4,DGI^2}(DS_1)]$

  $\wedge [B_{DGI^4} I_{DGI^4,DGI^3}(DS_1) \wedge T_{DGI^4,DGI^3}(DS_1)] \rightarrow\sim B_{DGI^4}(DS_2)$;Node 4 DGI does not believe the reading. Clearly node 1 is lying about device signal values to different nodes

- $w \vDash v_{DS}^{DGI^2} = True$; Valuation function exists in security domain for Node 2 DGI
- $w \vDash v_{DS}^{DGI^3} = True$; Valuation function exists in security domain for Node 3 DGI
- $w \vDash v_{DS}^{DGI^4} = True$; Valuation function exists in security domain for Node 4 DGI

$$MSDND(ES) \neq \exists w \in W \vdash [(S_{DS} \oplus S_{\sim DS})] \wedge \left[w \vDash (\exists V_{DS}^{DGI^2}(w) \wedge \exists V_{\sim DS}^{DGI^2}(w))\right]$$

$$MSDND(ES) \neq \exists w \in W \vdash [(S_{DS} \oplus S_{\sim DS})] \wedge \left[w \vDash (\exists V_{DS}^{DGI^3}(w) \wedge \exists V_{\sim DS}^{DGI^3}(w))\right]$$

$$MSDND(ES) \neq \exists w \in W \vdash [(S_{DS} \oplus S_{\sim DS})] \wedge \left[w \vDash (\exists V_{DS}^{DGI^4}(w) \wedge \exists V_{\sim DS}^{DGI^4}(w))\right]$$

Theorem 4.2.2. The system is MSDND secure in a 4 node system with Byzantine consensus formulation when the malicious node tries to share similar falsified status messages to different nodes.

Proof: Since the initiator node is a malicious node and sophisticated enough to share similar falsified status message to different nodes*interactive consistency 2* property is preserved. Figure 4.13 depicts the BIT logic interaction among the nodes. The MSDND proof below corroborates the same:

Information Flow Path:

- Node 1 Power electronics sends the device signal value to STUXNET
- STUXNET sends those values to Node 1 Message passing module
- Node 1 Message passing module sends those messages to Node 1 DGI
- Node 1 DGI Send message to Node 2 DGI, Node 3 DGI and Node 4 DGI
- Now all nodes except the initiator node 1 send their messages to all the peer nodes

- $\sim DS = True$; Device signal status message exchange is not normal
- $I_{STUX,PE^1}(\sim DS)$; Node 1 PE reports device signal value to STUXNET-like virus
- $B_{STUX} I_{STUX,PE^1}(\sim DS)$; STUXNET-like virus believes report from Node 1 PE
- $T_{STUX,PE^1}(\sim DS)$; STUXNET-like virus trusts the report from Node 1 PE
- $B_{STUX} I_{STUX,PE^1}(\sim DS) \wedge T_{STUX,PE^1}(\sim DS) \rightarrow B_{STUX}(\sim DS)$; STUXNET-like virus believes the reading

Now the STUXNET-like virus overwrites the true device signal values and sends similar falsified values to different nodes. Further analysis will assume message transfer as below:

- Node 1 DGI will send DS_1 as device signal value to Node 2 DGI
- Node 1 DGI will send DS_1 as device signal value to Node 3 DGI
- Node 1 DGI will send DS_1 as device signal value to Node 4 DGI

All message transformation or masking is performed by the STUXNET-like virus and the same is sent to different nodes. The further analysis of MSDND takes place at the DGI security domains. BIT logic formulation of round 0:

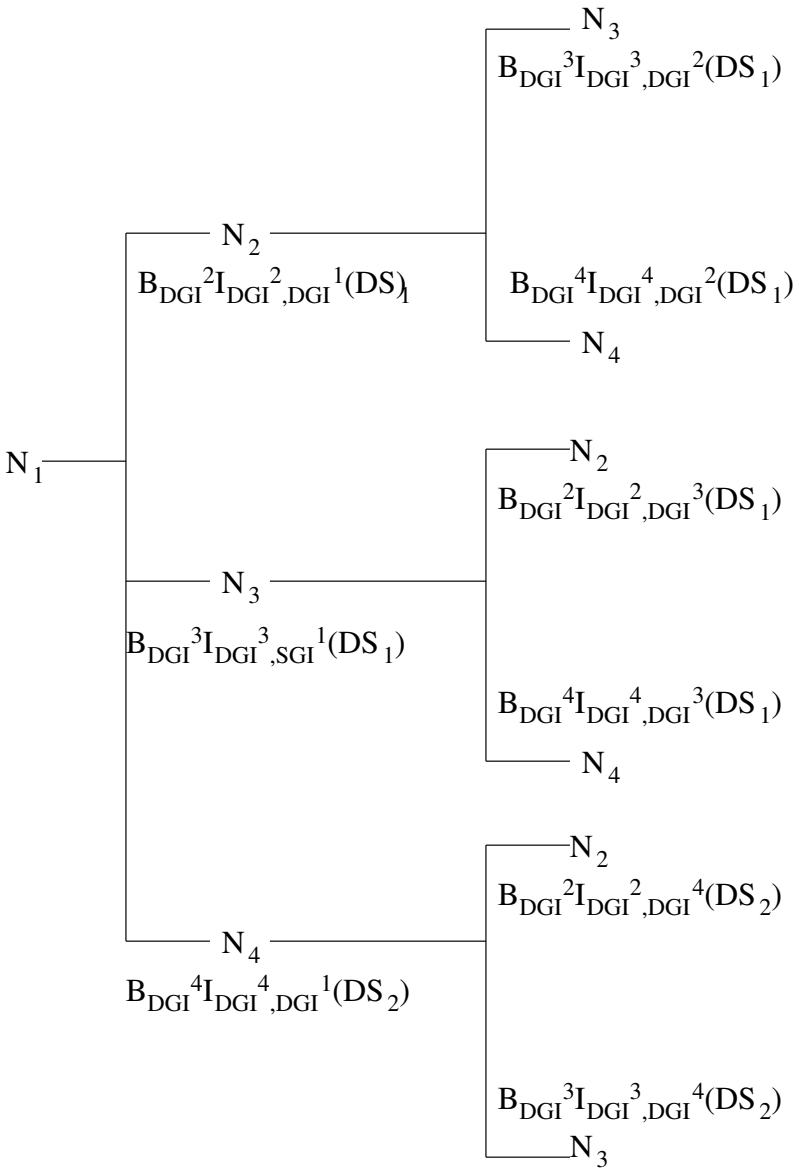

Figure 4.13. Interactive consistency and MSDND - BIT logic view Byzantine Agreement

- $I_{DGI^1,DGI^1}(DS_1)$; Node 1 DGI reports device signal value to Node 2 DGI
- $B_{DGI^2}I_{DGI^2,DGI^1}(DS_1)$; Node 2 DGI believes report from Node 1 DGI
- $T_{DGI^2,DGI^1}(DS_1)$; Node 2 DGI trusts the report from Node 1 DGI
- $I_{DGI^3,DGI^1}(DS_1)$; Node 1 DGI reports device signal value to Node 3 DGI
- $B_{DGI^3}I_{DGI^3,DGI^1}(DS_1)$; Node 3 DGI believes report from Node 1 DGI
- $T_{DGI^3,DGI^1}(DS_1)$; Node 3 DGI trusts the report from Node 1 DGI
- $I_{DGI^4,DGI^1}(DS_1)$; Node 1 DGI reports device signal value to Node 4 DGI
- $B_{DGI^4}I_{DGI^4,DGI^1}(DS_1)$; Node 3 DGI believes report from Node 1 DGI
- $T_{DGI^4,DGI^1}(DS_1)$; Node 3 DGI trusts the report from Node 1 DGI

BIT logic formulation of round 1:

- $I_{DGI^3,DGI^2}(DS_1)$; Node 2 DGI reports device singal value to Node 3 DGI that it received from Node 1 DGI
- $B_{DGI^3}I_{DGI^3,DGI^2}(DS_1)$; Node 3 DGI believes report from Node 2 DGI
- $T_{DGI^3,DGI^2}(DS_1)$; Node 3 DGI trusts the report from Node 2 DGI
- $I_{DGI^4,DGI^2}(DS_1)$; Node 2 DGI reports device singal value to Node 4 DGI that it received from Node 1 DGI
- $B_{DGI^4}I_{DGI^4,DGI^2}(DS_1)$; Node 4 DGI believes report from Node 2 DGI
- $T_{DGI^4,DGI^2}(DS_1)$; Node 4 DGI trusts the report from Node 2 DGI
- $I_{DGI^2,DGI^3}(DS_1)$; Node 3 DGI reports device signal value to Node 2 DGI that it received from Node 1 DGI
- $B_{DGI^2}I_{DGI^2,DGI^3}(DS_1)$; Node 2 DGI believes report from Node 3 DGI
- $T_{DGI^2,DGI^3}(DS_1)$; Node 2 DGI trusts the report from Node 3 DGI
- $I_{DGI^4,DGI^3}(DS_1)$; Node 3 DGI reports device signal value to Node 4 DGI that it received from Node 1 DGI

- $B_{DGI^4} I_{DGI^4,DGI^3}(DS_1)$; Node 4 DGI believes report from Node 3 DGI
- $T_{DGI^4,DGI^3}(DS_1)$; Node 4 DGI trusts the report from Node 3 DGI
- $I_{DGI^2,DGI^4}(DS_1)$; Node 4 DGI reports device signal value to Node 2 DGI that it received from Node 1 DGI
- $B_{DGI^2} I_{DGI^2,DGI^4}(DS_1)$; Node 2 DGI believes report from Node 4 DGI
- $T_{DGI^2,DGI^4}(DS_1)$; Node 2 DGI trusts the report from Node 4 DGI
- $I_{DGI^3,DGI^4}(DS_1)$; Node 4 DGI reports device signal value to Node 3 DGI that it received from Node 1 DGI
- $B_{DGI^3} I_{DGI^3,DGI^4}(DS_1)$; Node 3 DGI believes report from Node 4 DGI
- $T_{DGI^3,DGI^4}(DS_1)$; Node 3 DGI trusts the report from Node 4 DGI

Now combining all the BIT logic formulated until now to force deducibility:

- At Node 2: $[B_{DGI^2} I_{DGI^2,DGI^3}(DS_1) \wedge T_{DGI^2,DGI^3}(DS_1)] \wedge [B_{DGI^2} I_{DGI^2,DGI^4}(DS_1) \wedge T_{DGI^2,DGI^4}(DS_1)] \wedge [B_{DGI^2} I_{DGI^2,DGI^1}(DS_1 \wedge T_{DGI^2,DGI^1}(DS_1))] \rightarrow B_{DGI^2}(DS_1)$;Node 2 DGI believes the reading. Clearly, a similar falsified device signal value induces non deducibility into the system
- At Node 3: $[B_{DGI^3} I_{DGI^3,DGI^1}(DS_1) \wedge T_{DGI^3,DGI^1}(DS_1)] \wedge [B_{DGI^3} I_{DGI^3,DGI^2}(DS_1) \wedge T_{DGI^3,DGI^2}(DS_1)] \wedge [B_{DGI^3} I_{DGI^3,DGI^4}(DS_1) \wedge T_{DGI^3,DGI^4}(DS_1)] \rightarrow B_{DGI^3}(DS_1)$;Node 3 DGI believes the reading. Clearly, a similar falsified device signal value induces non deducibility into the system
- At Node 4: $[B_{DGI^4} I_{DGI^4,DGI^1}(DS_1) \wedge T_{DGI^4,DGI^1}(DS_1)] \wedge [B_{DGI^4} I_{DGI^4,DGI^2}(DS_1) \wedge T_{DGI^4,DGI^2}(DS_1)] \wedge [B_{DGI^4} I_{DGI^4,DGI^3}(DS_1) \wedge T_{DGI^4,DGI^3}(DS_1)] \rightarrow B_{DGI^4}(DS_1)$;Node 4 DGI does not believe the reading. Clearly, a similar falsified device signal value induces non deducibility into the system
- $w \vDash v_{DS}^{DGI^2} = False$; No valuation function exists in security domain for Node 2 DGI

- $w \vDash v_{DS}^{DGI^3} = False$; No valuation function exists in security domain for Node 3 DGI
- $w \vDash v_{DS}^{DGI^4} = False$; No valuation function exists in security domain for Node 4 DGI

$$MSDND(ES) = \exists\, w \in W \vdash [(S_{DS} \oplus S_{\sim DS})] \wedge \left[w \vDash (\nexists\, v_{DS}^{DGI^2}(w) \wedge \nexists\, v_{\sim DS}^{DGI^2}(w))\right]$$

$$MSDND(ES) = \exists\, w \in W \vdash [(S_{DS} \oplus S_{\sim DS})] \wedge \left[w \vDash (\nexists\, v_{DS}^{DGI^3}(w) \wedge \nexists\, v_{\sim DS}^{DGI^3}(w))\right]$$

$$MSDND(ES) = \exists\, w \in W \vdash [(S_{DS} \oplus S_{\sim DS})] \wedge \left[w \vDash (\nexists\, V_{DS}^{DGI^4}(w) \wedge \nexists\, v_{\sim DS}^{DGI^4}(w))\right]$$

4.3. PHYSICAL ATTESTATION

In the previous section during analysis of state collection protocol this work observed that an attacker node or malicious node can send similar falsified values to other nodes and make the system MSDND secure. In such a scenario the Byzantine consensus algorithm fails to identify the problem and the attacker is able to make the system MSDND secure there by hiding the attack over the system. Moving forward this work will break the MSDND security in system by using the physical properties of the system. The argument behind using the physical properties to verify the cyber components is that they cannot be changed. Cyber components of the system have no control over the physical properties of the system. To identify such scenarios and narrow down to a definitive number of components responsible for system malfunction this work uses physical attestation of the cyber process proposed by (Roth and McMillin, 2013).

4.3.1. Physical Attestation of Cyber Process in a 3 Node FREEDM System. Physical attestation of the cyber process primarily helps in identifying the fake power injection attack. It uses the law of conservation of energy to generate invariants based over the system architecture. The generated invariants are based over physical properties of the

system and should hold irrespective of the cyber process reporting of status messages. The basis of a power migration contact is the cyber communication between peer nodes. Owing to this cyber communication, a malicious node can mask its true parameters and lead to unpleasant scenarios such as the fake power injection attack.

Assumption: The physical attestation protocol assumes that each node on the smart grid has the ability to measure voltage and phase angle on the public side of its connection. This thesis introduces a small change over here. This thesis assumes that the public side of the connection has smart devices that can report the voltage and phase angle from public side of connection to the nearest point of common coupling. The point of common coupling calculates the invariant and sends it to all the nodes in the architecture. This change helps us to preserve the privacy of the nodes as well as does not give them an undue control over the public side of the connection, which ideally should remain with the utility. The change can also be considered as a proposal to the future smart grid infrastructure which will help increase the resilience and reliability of smart grids.

- *MSDND analysis of physical attestation protocol over a 3 node FREEDM system* To verify if the system is MSDND secure in a three node system this work will consider one node at a time and the parameter values they could falsify to affect the system. Below is the list of parameters that could be falsified along with a 3 node system architecture:

Node	Can Falsify
1	P_1, V_1, θ_1
2	P_2, V_2, θ_2
3	P_3, V_3, θ_3

  - *Considering node 1 as the malicious node* This thesis assumes node 1 tries to falsify its values and see what all invariants will be violated. A list of impacts over the invariants as below:

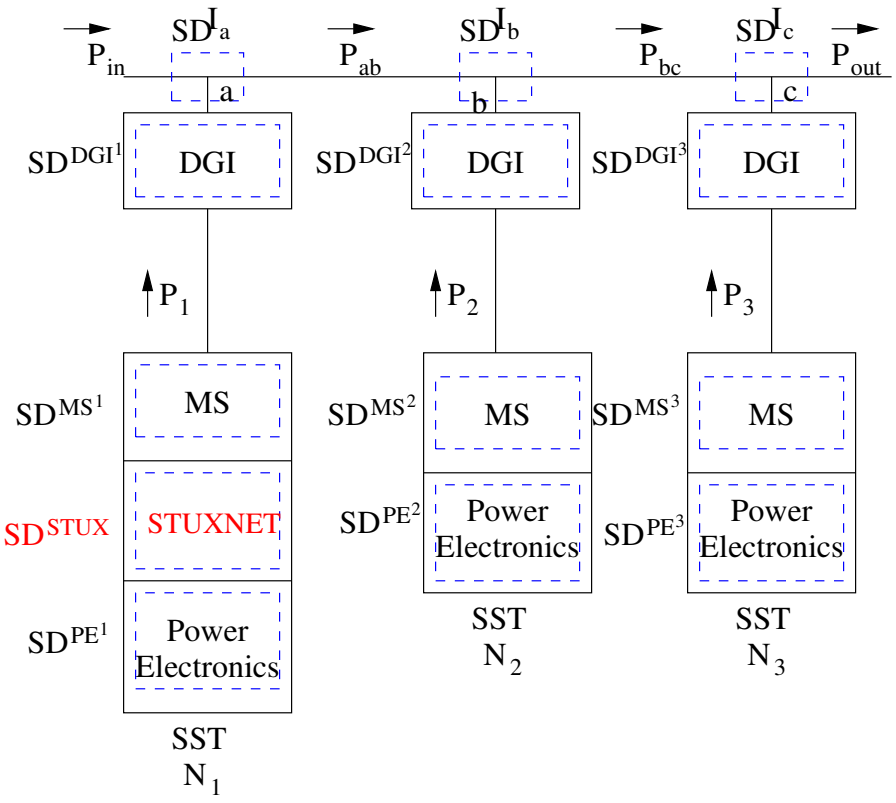

Figure 4.14. Node 1 acting as malicious node in a 3 Node system

* Falsifying P_1 will lead to an invariant I_a violation at point of common coupling a.
* Falsifying V_1 and θ_1 will lead to an invariant I_a, I_b violation at point of common coupling a and b respectively.
* Falsifying P_1, V_1 and θ_1 will lead to an invariant I_a violation at points of common coupling a and b.

Theorem 4.3.1.1. The system is not MSDND secure when Node 1 tries to falsify V_1 and θ_1

Proof: Let us assume Node 1 tried to falsify V_1 and θ_1. To represent the corrupt values, this work will consider P as the entity of exchange.

* $\sim P = True$; Generation reading reported is not normal
* $I_{DGI^2,DGI^1}(P)$; Node 2 gets generation values from node 1
* $B_{DGI^2} I_{DGI^2,DGI^1}(P)$; Node 2 believes reading from node 1

* $T_{DGI^2,DGI^1}(P)$; Node 2 trusts Node 1
* Considering Node 1 tries to falsify V_1 and θ_1
* $I_{DGI^2,I_b}(Invariant_b)$; Node 2 gets the invariant I_b from SD^{I_b}
* $B_{DGI^2}I_{DGI^2,I_b}(Invariant_b)$; Node 2 believes the reading from SD^{I_b}
* $T_{DGI^2,I_b}(Invariant_b)$; Node 2 trusts the reading from SD^{I_b}
* $I_{DGI^2,I_a}(Invariant_a)$; Node 2 gets the invariant I_a from SD^{I_a}
* $B_{DGI^2}I_{DGI^2,I_a}(Invariant_a)$; Node 2 believes the reading from SD^{I_a}
* $T_{DGI^2,I_a}(Invariant_a)$; Node 2 trusts the reading from SD^{I_a}
* $[B_{DGI^2}I_{DGI^2,DGI^1}(P) \wedge T_{DGI^2,DGI^1}(P)]$
  $\wedge [B_{DGI^2}I_{DGI^2,I_b}(Invariant_b) \wedge T_{DGI^2,I_b}(Invariant_b)]$
  $\wedge [B_{DGI^2}I_{DGI^2,I_a}(Invariant_a) \wedge T_{DGI^2,I_a}(Invariant_a)] \rightarrow\sim B_{DGI^2}(P)$; Node 2 does not believe the reading based over the invariant violations
* $w \vDash v_P^{DGI^2} = True$; Valuation function exists in security domain for node 2 DGI

$$MSDND(ES) \neq \exists\, w \in W \vdash [(S_P \oplus S_{\sim P})] \wedge \left[w \vDash (\exists\, v_P^{DGI^2}(w) \wedge \exists\, v_{\sim P}^{DGI^2}(w))\right]$$

Theorem 4.3.1.2. The system is MSDND secure when Node 1 tries to falsify P_1, V_1 and θ_1

Proof: Let us assume Node 1 tried to falsify P_1, V_1 and θ_1. To represent the corrupt values, this work will consider P as the entity of exchange.

* $\sim P = True$; Generation reading reported is not normal
* $I_{DGI^2,DGI^1}(P)$; Node 2 gets generation values from node 1
* $B_{DGI^2}I_{DGI^2,DGI^1}(P)$; Node 2 believes reading from node 1
* $T_{DGI^2,DGI^1}(P)$; Node 2 trusts Node 1
* Considering Node 1 tries to falsify P_1, V_1 and θ_1
* The invariant $I_b = P_{ab} + P_2 - P_{bc} = 0$ should be violated and, falsifying P_1, V_1 and θ_1 violates the invariant.
* $I_{DGI^2,I_b}(Invariant_b)$; Node 2 gets the invariant I_b from SD^{I_b}

* $B_{DGI^2} I_{DGI^2,I_b}(Invariant_b)$; Node 2 believes the reading from SD^{I_b}
* $T_{DGI^2,I_b}(Invariant_b)$; Node 2 trusts the reading from SD^{I_b}
* $[B_{DGI^2} I_{DGI^2,DGI^1}(P) \wedge T_{DGI^2,DGI^1}(P)]$
  $\wedge\ [B_{DGI^2} I_{DGI^2,I_b}(Invariant_b) \wedge T_{DGI^2,I_b}(Invariant_b)] \rightarrow\sim B_{DGI^2}(P)$; Node 2 does not believe the reading based over the invariant violations
* $w \vDash v_P^{DGI^2} = True$; Valuation function exists in security domain for node 2 DGI to identify that generation values reported are corrupt.
* $w \vDash v_{N_i}^{DGI^2} = False$; Valuation function does not exist in security domain for node 2 DGI to identify which node reported corrupt generation values.

$$MSDND(ES) = \exists\, w \in W \vdash [(S_P \oplus S_{\sim P})] \wedge \left[w \vDash (\exists\, v_P^{DGI^2}(w) \wedge \exists\, v_{\sim P}^{DGI^2}(w))\right] \wedge \left[w \vDash (\nexists\, v_{N_i}^{DGI^2}(w) \wedge \nexists\, v_{\sim N_i}^{DGI^2}(w))\right]$$

Remark: Here, the above case of invariant violation leads to MSDND secure system. From the above equation it can be clearly demonstrated that the security domain 4 has a valuation function to identify if something wrong is going on in the system, however, it is not possible to identify the origin of the attack. The invariant I_b can be affected by falsifying either of the P_1, V_1 and θ_1 by node 1 or P_2 by node 2. Hence, in a 3 node system it is impossible to identify which of the two nodes falsified values for invariant to report the problem in system.

Theorem 4.3.1.3. The system is not MSDND secure when Node 1 tries to falsify P_1

Proof: Let us assume Node 1 tried to falsify P_1. To represent the corrupt values, this work will consider P as the entity of exchange.

* $\sim P = True$; Generation reading reported is not normal
* $I_{DGI^2,DGI^1}(P)$; Node 2 gets generation values from node 1
* $B_{DGI^2} I_{DGI^2,DGI^1}(P)$; Node 2 believes reading from node 1
* $T_{DGI^2,DGI^1}(P)$; Node 2 trusts Node 1

* Considering Node 1 tries to falsify P_1
* The invariant $I_a = P_{in} + P_1 - P_{ab} = 0$ should be violated and, falsifying P_1 violates the invariant.
* $I_{DGI^2,I_a}(Invariant_a)$; Node 2 gets the invariant I_a from SD^{I_a}
* $B_{DGI^2} I_{DGI^2,I_a}(Invariant_a)$; Node 2 believes the reading from SD^{I_a}
* $T_{DGI^2,I_a}(Invariant_a)$; Node 2 trusts the reading from SD^{I_a}
* $[B_{DGI^2} I_{DGI^2,DGI^1}(P) \wedge T_{DGI^2,DGI^1}(P)]$
  $\wedge\ [B_{DGI^2} I_{DGI^2,I_a}(Invariant_a) \wedge T_{DGI^2,I_a}(Invariant_a)] \rightarrow\sim B_{DGI^2}(P)$; Node 2 does not believe the reading based over the invariant violations
* $w \vDash v_P^{DGI^2} = True$; Valuation function exists in security domain for node 2 DGI

$$MSDND(ES) \neq \exists\, w \in W \vdash [(S_P \oplus S_{\sim P})] \wedge \left[w \vDash (\exists\, v_P^{DGI^2}(w) \wedge \exists\, v_{\sim P}^{DGI^2}(w))\right]$$

– *Considering node 2 as the malicious node 4.15.* This work will assume that node 2 tries to falsify its values and see what all invariants will be violated. A list of impacts over the invariants is as below:

* Falsifying P_2 will lead to an invariant I_b violation at point of common coupling b.
* Falsifying V_2 and θ_2 will lead to an invariant I_a, I_b and I_c violation at point of common coupling a, b and c respectively.
* Falsifying P_2, V_2 and θ_2 will lead to invariant I_a and I_c violation at points of common coupling a and c.

Theorem 4.3.1.4. The system is not MSDND secure when Node 2 tries to falsify V_2 and θ_2

Proof: Let us assume Node 2 tried to falsify V_2 and θ_2. To represent the corrupt values, this work will consider P as the entity of exchange.

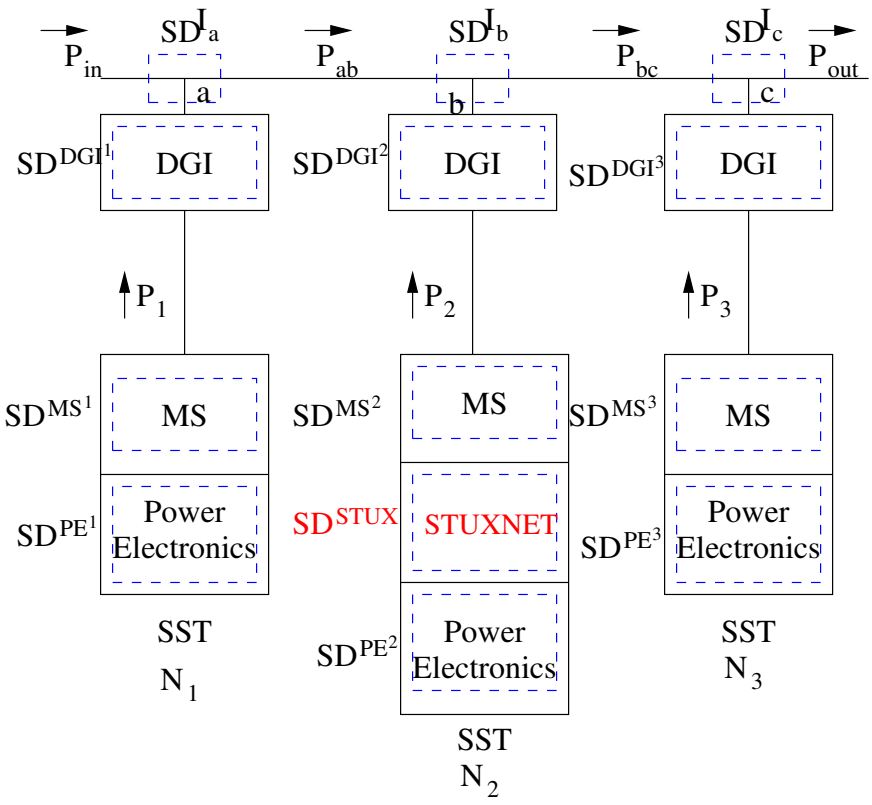

Figure 4.15. Node 2 acting as malicious node in a 3 Node system

* $\sim P = True$; Generation reading reported is not normal
* $I_{DGI^1,DGI^2}(P)$; Node 1 gets generation values from node 2
* $B_{DGI^1} I_{DGI^1,DGI^2}(P)$; Node 1 believes reading from Node 2
* $T_{DGI^1,DGI^2}(P)$; Node 1 trusts Node 2
* $I_{DGI^3,DGI^2}(P)$; Node 3 gets generation values from Node 2
* $B_{DGI^3} I_{DGI^3,DGI^2}(P)$; Node 3 believes reading from Node 2
* $T_{DGI^3,DGI^2}(P)$; Node 3 trusts Node 2
* Considering Node 2 tries to falsify V_2 and θ_2 all three invariants will be violated
* $I_{DGI^1,I_b}(Invariant_b)$; Node 1 gets the invariant I_b from SD^{I_b}
* $B_{DGI^1} I_{DGI^1,I_b}(Invariant_b)$; Node 1 believes the reading from SD^{I_b}
* $T_{DGI^1,I_b}(Invariant_b)$; Node 1 trusts the reading from SD^{I_b}
* $I_{DGI^1,I_a}(Invariant_a)$; Node 1 gets the invariant I_a from SD^{I_a}
* $B_{DGI^1} I_{DGI^1,I_a}(Invariant_a)$; Node 1 believes the reading from SD^{I_a}
* $T_{DGI^1,I_a}(Invariant_a)$; Node 1 trusts the reading from SD^{I_a}
* $I_{DGI^1,I_c}(Invariant_c)$; Node 1 gets the invariant I_c from SD^{I_c}
* $B_{DGI^1} I_{DGI^1,I_c}(Invariant_c)$; Node 1 believes the reading from SD^{I_c}
* $T_{DGI^1,I_c}(Invariant_c)$; Node 1 trusts the reading from SD^{I_c}
* $[B_{DGI^1} I_{DGI^1,DGI^2}(P) \wedge T_{DGI^1,DGI^2}(P)]$
  $\wedge [B_{DGI^1} I_{DGI^1,I_a}(Invariant_a) \wedge T_{DGI^1,I_a}(Invariant_a)]$
  $\wedge [B_{DGI^1} I_{DGI^1,I_b}(Invariant_b) \wedge T_{DGI^1,I_b}(Invariant_b)]$
  $\wedge [B_{DGI^1} I_{DGI^1,I_c}(Invariant_c) \wedge T_{DGI^1,I_c}(Invariant_c)] \rightarrow\sim B_{DGI^1}(P)$; Node 1 does not believe the reading based over the invariant violations
* $w \vDash v_P^{DGI^1} = True$; Valuation function exists in security domain for node 1 DGI
* $I_{DGI^3,I_b}(Invariant_b)$; Node 3 gets the invariant I_b from SD^{I_b}
* $B_{DGI^3} I_{DGI^3,I_b}(Invariant_b)$; Node 3 believes the reading from SD^{I_b}
* $T_{DGI^3,I_b}(Invariant_b)$; Node 3 trusts the reading from SD^{I_b}
* $I_{DGI^3,I_a}(Invariant_a)$; Node 3 gets the invariant I_a from SD^{I_a}
* $B_{DGI^3} I_{DGI^3,I_a}(Invariant_a)$; Node 3 believes the reading from SD^{I_a}
* $T_{DGI^3,I_c}(Invariant_a)$; Node 3 trusts the reading from SD^{I_a}
* $I_{DGI^3,I_c}(Invariant_c)$; Node 3 gets the invariant I_c from SD^{I_c}

* $B_{DGI^3} I_{DGI^3,I_c}(Invariant_c)$; Node 3 believes the reading from SD^{I_c}
* $T_{DGI^3,I_c}(Invariant_c)$; Node 3 trusts the reading from SD^{I_c}
* $[B_{DGI^3} I_{DGI^3,DGI^2}(P) \wedge T_{DGI^3,DGI^2}(P)]$
  $\wedge [B_{DGI^3} I_{DGI^3,I_a}(Invariant_a) \wedge T_{DGI^3,I_a}(Invariant_a)]$
  $\wedge [B_{DGI^3} I_{DGI^3,I_b}(Invariant_b) \wedge T_{DGI^3,I_b}(Invariant_b)]$
  $\wedge [B_{DGI^3} I_{DGI^3,I_c}(Invariant_c) \wedge T_{DGI^3,I_c}(Invariant_c)] \rightarrow\sim B_{DGI^3}(P)$; Node 3 does not believe the reading based over the invariant violations
* $w \vDash v_P^{DGI^3} = True$; Valuation function exists in security domain for node 3 DGI

$$MSDND(ES) \neq \exists\, w \in W \vdash [(S_P \oplus S_{\sim P})] \wedge \left[w \vDash (\exists\, v_P^{DGI^1}(w) \wedge \exists\, v_{\sim P}^{DGI^1}(w))\right]$$
$$MSDND(ES) \neq \exists\, w \in W \vdash [(S_P \oplus S_{\sim P})] \wedge \left[w \vDash (\exists\, v_P^{DGI^3}(w) \wedge \exists\, v_{\sim P}^{DGI^3}(w))\right]$$

Theorem 4.3.1.5. The system is not MSDND secure when Node 2 tries to falsify P_2, V_2 and θ_2

Proof: Let us assume Node 2 tried to falsify P_2, V_2 and θ_2. To represent the corrupt values, this work will consider P as the entity of exchange.

* $\sim P = True$; Generation reading reported is not normal
* $I_{DGI^1,DGI^2}(P)$; Node 1 gets generation values from node 2
* $B_{DGI^1} I_{DGI^1,DGI^2}(P)$; Node 1 believes reading from Node 2
* $T_{DGI^1,DGI^2}(P)$; Node 1 trusts Node 2
* $I_{DGI^3,DGI^2}(P)$; Node 3 gets generation values from Node 2
* $B_{DGI^3} I_{DGI^3,DGI^2}(P)$; Node 3 believes reading from Node 2
* $T_{DGI^3,DGI^1}(P)$; Node 3 trusts Node 2
* Considering Node 2 tries to falsify P_2, V_2 and θ_2 invariants I_a and I_c will be violated
* $I_{DGI^1,I_a}(Invariant_a)$; Node 1 gets the invariant I_a from SD^{I_a}
* $B_{DGI^1} I_{DGI^1,I_a}(Invariant_a)$; Node 1 believes the reading from SD^{I_a}
* $T_{DGI^1,I_a}(Invariant_a)$; Node 1 trusts the reading from SD^{I_a}

* $I_{DGI^1,I_c}(Invariant_c)$; Node 1 gets the invariant I_c from SD^{I_c}
* $B_{DGI^1}I_{DGI^1,I_c}(Invariant_c)$; Node 1 believes the reading from SD^{I_c}
* $T_{DGI^1,I_c}(Invariant_c)$; Node 1 trusts the reading from SD^{I_c}
* $[B_{DGI^1}I_{DGI^1,DGI^2}(P) \wedge T_{DGI^1,DGI^2}(P)]$
  $\wedge [B_{DGI^1}I_{DGI^1,I_a}(Invariant_a) \wedge T_{DGI^1,I_a}(Invariant_a)]$
  $\wedge [B_{DGI^1}I_{DGI^1,I_c}(Invariant_c) \wedge T_{DGI^1,I_c}(Invariant_c)] \rightarrow\sim B_{DGI^1}(P)$; Node 1 does not believe the reading based over the invariant violations
* $w \vDash v_P^{DGI^1} = True$; Valuation function exists in security domain for node 1 DGI
* $I_{DGI^3,I_a}(Invariant_a)$; Node 3 gets the invariant I_a from SD^{I_a}
* $B_{DGI^3}I_{DGI^3,I_a}(Invariant_a)$; Node 3 believes the reading from SD^{I_a}
* $T_{DGI^3,I_a}(Invariant_a)$; Node 3 trusts the reading from SD^{I_a}
* $I_{DGI^3,I_c}(Invariant_c)$; Node 3 gets the invariant I_c from SD^{I_c}
* $B_{DGI^3}I_{DGI^3,I_c}(Invariant_c)$; Node 3 believes the reading from SD^{I_c}
* $T_{DGI^3,I_c}(Invariant_c)$; Node 3 trusts the reading from SD^{I_c}
* $[B_{DGI^3}I_{DGI^3,DGI^2}(P) \wedge T_{DGI^3,DGI^2}(P)]$
  $\wedge [B_{DGI^3}I_{DGI^3,I_a}(Invariant_a) \wedge T_{DGI^3,I_a}(Invariant_a)]$
  $\wedge [B_{DGI^3}I_{DGI^3,I_c}(Invariant_c) \wedge T_{DGI^3,I_c}(Invariant_c)] \rightarrow\sim B_{DGI^3}(P)$; Node 3 does not believe the reading based over the invariant violations
* $w \vDash v_P^{DGI^3} = True$; Valuation function exists in security domain for node 3 DGI

$$MSDND(ES) \neq \exists\, w \in W \vdash [(S_P \oplus S_{\sim P})] \wedge \left[w \vDash (\exists\, v_P^{DGI^1}(w) \wedge \exists\, v_{\sim P}^{DGI^1}(w))\right]$$
$$MSDND(ES) \neq \exists\, w \in W \vdash [(S_P \oplus S_{\sim P})] \wedge \left[w \vDash (\exists\, v_P^{DGI^3}(w) \wedge \exists\, v_{\sim P}^{DGI^3}(w))\right]$$

Theorem 4.3.1.6. The system is MSDND secure when Node 2 tries to falsify P_2

Proof: Let us assume Node 2 tries to falsify P_2. To represent the corrupt values, this work will consider P as the entity of exchange.

* $\sim P = True$; Generation reading reported is not normal
* $I_{DGI^1,DGI^2}(P)$; Node 1 gets generation values from node 2

* $B_{DGI^1} I_{DGI^1,DGI^2}(P)$; Node 1 believes reading from Node 2
* $T_{DGI^1,DGI^2}(P)$; Node 1 trusts Node 2
* $I_{DGI^3,DGI^2}(P)$; Node 3 gets generation values from Node 2
* $B_{DGI^3} I_{DGI^3,DGI^2}(P)$; Node 3 believes reading from Node 2
* $T_{DGI^3,DGI^2}(P)$; Node 3 trusts Node 2
* Considering Node 2 tries to falsify P_2 invariant I_b will be violated
* $I_{DGI^1,I_b}(Invariant_b)$; Node 1 gets the invariant I_b from SD^{I_b}
* $B_{DGI^1} I_{DGI^1,I_b}(Invariant_b)$; Node 1 believes the reading from SD^{I_b}
* $T_{DGI^1,I_b}(Invariant_b)$; Node 1 trusts the reading from SD^{I_b}
* $[B_{DGI^1} I_{DGI^1,DGI^2}(P) \wedge T_{DGI^1,DGI^2}(P)]$
  $\wedge\ [B_{DGI^1} I_{DGI^1,I_b}(Invariant_b) \wedge T_{DGI^1,I_b}(Invariant_b)] \rightarrow\sim B_{DGI^1}(P)$; Node 1 does not believe the reading based over the invariant violations
* $w \vDash v_P^{DGI^1} = True$; Valuation function exists in security domain for node 1 DGI
* $I_{DGI^3,I_b}(Invariant_b)$; Node 3 gets the invariant I_b from SD^{I_b}
* $B_{DGI^3} I_{DGI^3,I_b}(Invariant_b)$; Node 3 believes the reading from SD^{I_b}
* $T_{DGI^3,I_b}(Invariant_b)$; Node 3 trusts the reading from SD^{I_b}
* $[B_{DGI^3} I_{DGI^3,DGI^2}(P) \wedge T_{DGI^3,DGI^2}(P)]$
  $\wedge\ [B_{DGI^3} I_{DGI^3,I_b}(Invariant_b) \wedge T_{DGI^3,I_b}(Invariant_b)] \rightarrow\sim B_{DGI^3}(P)$; Node 3 does not believe the reading based over the invariant violations
* $w \vDash v_P^{DGI^3} = True$; Valuation function exists in security domain for node 3 DGI

$$MSDND(ES) = \exists\, w \in W \vdash [(S_P \oplus S_{\sim P})] \wedge \left[w \vDash (\exists\, v_P^{DGI^1}(w) \wedge \exists\, v_{\sim P}^{DGI^1}(w))\right] \wedge \left[w \vDash (\nexists\, v_{N_i}^{DGI^1}(w) \wedge \nexists\, v_{\sim N_i}^{DGI^1}(w))\right]$$

$$MSDND(ES) = \exists\, w \in W \vdash [(S_P \oplus S_{\sim P})] \wedge \left[w \vDash (\exists\, v_P^{DGI^3}(w) \wedge \exists\, v_{\sim P}^{DGI^3}(w))\right] \wedge \left[w \vDash (\nexists\, v_{N_i}^{DGI^3}(w) \wedge \nexists\, v_{\sim N_i}^{DGI^3}(w))\right]$$

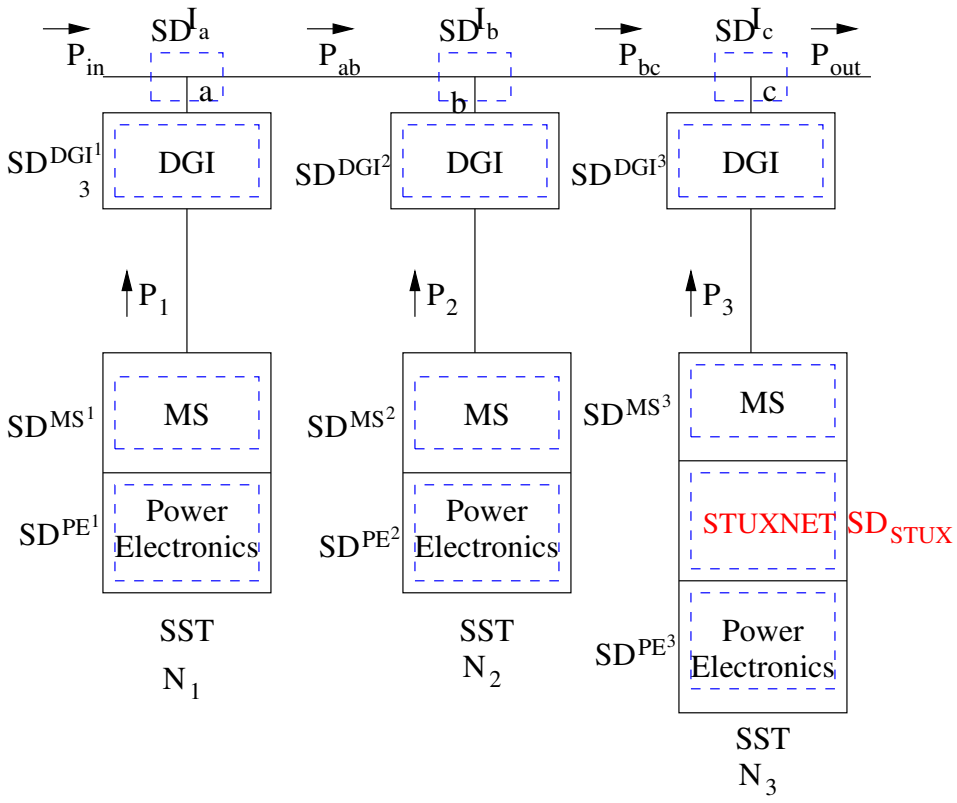

Figure 4.16. Node 3 acting as malicious node in a 3 Node system

Remark: Here it is worth noting that though security domains 10 and security domains 4 do have a valuation function to identify that there is something wrong with the system, it is not possible to identify the origin of attack. The invariant I_b can be affected both by falsifying P_1, V_1 and θ_1 by Node 1 or by falsifying P_2 by Node 2. Hence, in a 3 node system it is impossible to identify which of the two nodes falsified values for invariant to report the problem in system.

– *Considering Node 3 as the malicious node Figure 4.16:* Assuming node 3 tries to falsify its values, a list of impacted invariants is as below:

  * Falsifying P_3 will lead to an invariant I_c violation at point of common coupling c.
  * Falsifying V_3 and θ_3 will lead to an invariant I_b and I_c violation at point of common coupling b and c respectively.

* Falsifying P_3, V_3 and θ_3 will lead to invariant I_b violation at point of common coupling b.

Theorem 4.3.1.7. The system is not MSDND secure when Node 3 tries to falsify V_3 and θ_3

Proof: Let us assume Node 3 tried to falsify V_3 and θ_3. To represent the corrupt values, this work will consider P as the entity of exchange.

* $\sim P = True$; Generation reading reported is not normal
* $I_{DGI^1,DGI^3}(P)$; Node 1 gets generation values from node 3
* $B_{DGI^1} I_{DGI^1,DGI^3}(P)$; Node 1 believes reading from Node 3
* $T_{DGI^1,DGI^3}(P)$; Node 1 trusts node 3
* $I_{DGI^2,DGI^3}(P)$; Node 2 gets generation values from node 3
* $B_{DGI^3} I_{DGI^2,DGI^3}(P)$; Node 2 believes reading from node 3
* $T_{DGI^2,DGI^3}(P)$; Node 2 trusts Node 3
* Considering Node 3 tries to falsify V_3 and θ_3 invariants I_b and I_c will be violated
* $I_{DGI^1,I_b}(Invariant_b)$; Node 1 gets the invariant I_b from SD^{I_b}
* $B_{DGI^1} I_{DGI^1,I_b}(Invariant_b)$; Node 1 believes the reading from SD^{I_b}
* $T_{DGI^1,I_b}(Invariant_b)$; Node 1 trusts the reading from SD^{I_b}
* $I_{DGI^1,I_c}(Invariant_c)$; Node 1 gets the invariant I_c from SD^{I_c}
* $B_{DGI^1} I_{DGI^1,I_c}(Invariant_c)$; Node 1 believes the reading from SD^{I_c}
* $T_{DGI^1,I_c}(Invariant_c)$; Node 1 trusts the reading from SD^{I_c}
* $[B_{DGI^1} I_{DGI^1,DGI^3}(P) \wedge T_{DGI^1,DGI^3}(P)]$
  $\wedge [B_{DGI^1} I_{DGI^1,I_b}(Invariant_b) \wedge T_{DGI^1,I_b}(Invariant_b)]$
  $\wedge [B_{DGI^1} I_{DGI^1,I_c}(Invariant_c) \wedge T_{DGI^1,I_c}(Invariant_c)] \rightarrow\sim B_{DGI^1}(P)$; Node 1 does not believe the reading based over the invariant violations
* $w \vDash v_P^{DGI^1} = True$; Valuation function exists in security domain for node 1 DGI
* $I_{DGI^2,I_b}(Invariant_b)$; Node 2 gets the invariant I_b from SD^{I_b}
* $B_{DGI^2} I_{DGI^2,I_b}(Invariant_b)$; Node 2 believes the reading from SD^{I_b}
* $T_{DGI^2,I_b}(Invariant_b)$; Node 2 trusts the reading from SD^{I_b}
* $I_{DGI^2,I_c}(Invariant_c)$; Node 2 gets the invariant I_c from SD^{I_c}

* $B_{DGI^2} I_{DGI^2,I_c}(Invariant_c)$; Node 2 believes the reading from SD^{I_c}
* $T_{DGI^2,I_c}(Invariant_c)$; Node 2 trusts the reading from SD^{I_c}
* $[B_{DGI^2} I_{DGI^2,DGI^3}(P) \wedge T_{DGI^2,DGI^3}(P)]$
  $\wedge [B_{DGI^2} I_{DGI^2,I_b}(Invariant_b) \wedge T_{DGI^2,I_b}(Invariant_b)]$
  $\wedge [B_{DGI^2} I_{DGI^2,I_c}(Invariant_c) \wedge T_{DGI^2,I_c}(Invariant_c)] \rightarrow\sim B_{DGI^2}(P)$; Node 2 does not believe the reading based over the invariant violations
* $w \vDash v_P^{DGI^2} = True$; Valuation function exists in security domain for node 2 DGI

$$MSDND(ES) \neq \exists w \in W \vdash [(S_P \oplus S_{\sim P})] \wedge \left[w \vDash (\exists v_P^{DGI^1}(w) \wedge \exists v_{\sim P}^{DGI^1}(w))\right]$$
$$MSDND(ES) \neq \exists w \in W \vdash [(S_P \oplus S_{\sim P})] \wedge \left[w \vDash (\exists v_P^{DGI^2}(w) \wedge \exists v_{\sim P}^{DGI^2}(w))\right]$$

Theorem 4.3.1.8. The system is MSDND secure when Node 3 tries to falsify P_3, V_3 and θ_3

Proof: Let us assume Node 3 tried to falsify P_3, V_3 and θ_3. To represent the corrupt values, this work will consider P as the entity of exchange.

* $\sim P = True$; Generation reading reported is not normal
* $I_{DGI^1,DGI^3}(P)$; Node 1 gets generation values from node 3
* $B_{DGI^1} I_{DGI^1,DGI^3}(P)$; Node 1 believes reading from Node 3
* $T_{DGI^1,DGI^3}(P)$; Node 1 trusts Node 3
* $I_{DGI^2,DGI^3}(P)$; Node 2 gets generation values from Node 3
* $B_{DGI^2} I_{DGI^2,DGI^3}(P)$; Node 2 believes reading from Node 3
* $T_{DGI^2,DGI^3}(P)$; Node 2 trusts Node 3
* Considering Node 3 tries to falsify P_3, V_3 and θ_3 invariant I_b will be violated
* $I_{DGI^1,I_b}(Invariant_b)$; Node 1 gets the invariant I_a from SD^{I_b}
* $B_{DGI^1} I_{DGI^1,I_b}(Invariant_b)$; Node 1 believes the reading from SD^{I_b}
* $T_{DGI^1,I_b}(Invariant_b)$; Node 1 trusts the reading from SD^{I_b}

* $[B_{DGI^1} I_{DGI^1,DGI^3}(P) \wedge T_{DGI^1,DGI^3}(P)]$
  $\wedge [B_{DGI^1} I_{DGI^1,I_b}(Invariant_b) \wedge T_{DGI^1,I_b}(Invariant_b)] \rightarrow\sim B_{DGI^1}(P)$; Node 1 does not believe the reading based over the invariant violations
* $w \vDash V_P^{DGI^1} = True$; Valuation function exists in security domain for node 1 DGI
* $I_{DGI^2,I_b}(Invariant_b)$; Node 2 gets the invariant I_b from SD^{I_b}
* $B_{DGI^2} I_{DGI^2,I_b}(Invariant_b)$; Node 2 believes the reading from SD^{I_b}
* $T_{DGI^2,I_b}(Invariant_b)$; Node 2 trusts the reading from SD^{I_b}
* $[B_{DGI^2} I_{DGI^2,DGI^3}(P) \wedge T_{DGI^2,DGI^3}(P)]$
  $\wedge [B_{DGI^2} I_{DGI^2,I_b}(Invariant_b) \wedge T_{DGI^2,I_b}(Invariant_b)] \rightarrow\sim B_{DGI^2}(P)$; Node 2 does not believe the reading based over the invariant violations
* $w \vDash v_P^{DGI^2} = True$; Valuation function exists in security domain for node 2 DGI

$$MSDND(ES) = \exists\, w \in W \vdash [(S_P \oplus S_{\sim P})] \wedge \left[w \vDash (\exists\, v_P^{DGI^1}(w) \wedge \exists\, v_{\sim P}^{DGI^1}(w))\right] \wedge \left[w \vDash (\nexists\, v_{N_i}^{DGI^1}(w) \wedge \nexists\, v_{\sim N_i}^{DGI^1}(w))\right]$$

$$MSDND(ES) = \exists\, w \in W \vdash [(S_P \oplus S_{\sim P})] \wedge \left[w \vDash (\exists\, V_P^{DGI^2}(w) \wedge \exists\, V_{\sim P}^{DGI^2}(w))\right] \wedge \left[w \vDash (\nexists\, v_{N_i}^{DGI^2}(w) \wedge \nexists\, v_{\sim N_i}^{DGI^2}(w))\right]$$

Remark: Here it is worth noting that though security domains 3 and security domains 4 do have a valuation function to identify that there is something wrong with the system, however, it is not possible to identify the origin of attack. The invariant I_b can be affected both by falsifying any of P_1, V_1 and θ_1 by node 1, P_2 by Node 2 or P_3, V_3 and θ_3 by node 3. Hence, in a 3 node system it is impossible to identify which of the two nodes falsified values for invariant to report the problem in system.

Theorem 4.3.1.9. The system is not MSDND secure when Node 3 tries to falsify P_3

Proof: Let us assume Node 3 tried to falsify P_3. To represent the corrupt values, this work will consider P as the entity of exchange.

* $\sim P = True$; Generation reading reported is not normal

* $I_{DGI^1,DGI^3}(P)$; Node 1 gets generation values from node 3
* $B_{DGI^1} I_{DGI^1,DGI^3}(P)$; Node 1 believes reading from Node 3
* $T_{DGI^1,DGI^3}(P)$; Node 1 trusts Node 3
* $I_{DGI^2,DGI^3}(P)$; Node 2 gets generation values from node 3
* $B_{DGI^2} I_{DGI^2,DGI^3}(P)$; Node 2 believes reading from node 3
* $T_{DGI^2,DGI^3}(P)$; Node 2 trusts node 3
* Considering Node 3 tries to falsify P_3 invariant I_c will be violated
* $I_{DGI^1,I_c}(Invariant_c)$; Node 1 gets the invariant I_c from SD_9
* $B_{DGI^1} I_{DGI^1,I_c}(Invariant_c)$; Node 1 believes the reading from SD_9
* $T_{DGI^1,I_c}(Invariant_c)$; Node 1 trusts the reading from SD_9
* $[B_{DGI^1} I_{DGI^1,DGI^3}(P) \wedge T_{DGI^1,DGI^3}(P)]$
  $\wedge [B_{DGI^1} I_{DGI^1,I_c}(Invariant_c) \wedge T_{DGI^1,I_c}(Invariant_c)] \rightarrow\sim B_{DGI^1}(P)$; Node 1 does not believe the reading based over the invariant violations
* $w \vDash v_P^{DGI^1} = True$; Valuation function exists in security domain for node 1 DGI
* $I_{DGI^2,I_c}(Invariant_c)$; Node 2 gets the invariant I_c from SD_9
* $B_{DGI^2} I_{DGI^2,I_c}(Invariant_c)$; Node 2 believes the invariant from SD_9
* $T_{DGI^2,I_c}(Invariant_c)$; Node 2 trusts the reading from SD_9
* $[B_{DGI^2} I_{DGI^2,DGI^3}(P) \wedge T_{DGI^2,DGI^3}(P)]$
  $\wedge [B_{DGI^2} I_{DGI^2,I_c}(Invariant_c) \wedge T_{DGI^2,I_c}(Invariant_c)] \rightarrow\sim B_{DGI^2}(P)$; Node 2 does not believe the reading based over the invariant violations
* $w \vDash v_P^{DGI^2} = True$; Valuation function exists in security domain for node 2 DGI

$$MSDND(ES) \neq \exists w \in W \vdash [(S_P \oplus S_{\sim P})] \wedge \left[w \vDash (\exists v_P^{DGI^1}(w) \wedge \exists v_{\sim P}^{DGI^1}(w))\right]$$

$$MSDND(ES) \neq \exists w \in W \vdash [(S_P \oplus S_{\sim P})] \wedge \left[w \vDash (\exists v_P^{DGI^2}(w) \wedge \exists v_{\sim P}^{DGI^2}(w))\right]$$

– *Outcome:* Physical attestation of a 3 node FREEDM system is able to identify an attack over the system, however, fails to identify the attacker. This motivates us to formulate the physical attestation protocol over a 7 node system. Over the next section this

Table 4.2. 3 Node System - Invariant Violations

Malicious Node	Falsified Parameter	Invariant Violation	Comment
1	P_1	I_a	MSDND with respect to identity of attacker
1	V_1, θ_1	I_a, I_b	
1	P_1, V_1, θ_1	I_b	
2	P_2	I_b	MSDND with respect to identity of attacker
2	V_2, θ_2	I_a, I_b, I_c	
2	P_2, V_2, θ_2	I_c	
3	P_3	I_c	MSDND with respect to identity of attacker
3	V_3, θ_3	I_b, I_c, I_d	
3	P_3, V_3, θ_3	I_b, I_d	

thesis will implement physical attestation protocol over a 7 node system and formulate parameter violation patters. The analysis will show us the parameter violation over a 7 node system has a unique pattern, considering which an approach can be designed to identify attacker in the system employing physical attestation. The choice of a 7 node system is also dependent over the fact that for a Byzantine consensus formulation with 2 malicious nodes, a total of 7 nodes in the system is required. Hence, a 7 node system can be considered as an intersection of Byzantine consensus and physical attestation in Cyber Physical Systems.

4.3.2. Physical Attestation of Cyber Process in a 7 Node FREEDM System. *Understanding architecture of 7 node FREEDM system* Please consider the Figure 4.17 as power flow architecture:

The law of conservation of energy states that at points a, b, c, d, e, f and g or the points of common coupling, total energy entering should be equal to the energy leaving the point of common coupling. Therefore, the invariants at points of common coupling are given as below:

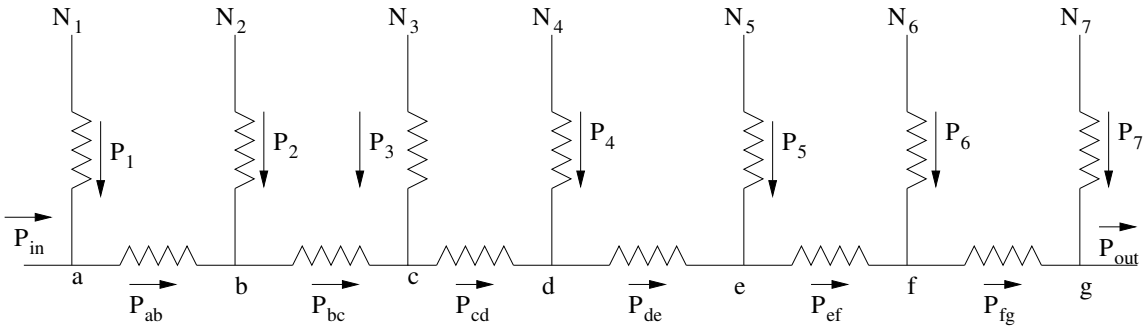

Figure 4.17. 7 Node System depicting power flows

$$I_a : P_{in} + P_1 - P_{ab} = 0$$

$$I_b : P_{ab} + P_2 - P_{bc} = 0$$

$$I_c : P_{bc} + P_3 - P_{cd} = 0$$

$$I_a : P_{cd} + P_4 - P_{de} = 0$$

$$I_b : P_{de} + P_5 - P_{ef} = 0$$

$$I_c : P_{ef} + P_6 - P_{fg} = 0$$

$$I_c : P_{fg} + P_7 - P_{out} = 0$$

- *MSDND analysis of physical attestation protocol over a 7 node FREEDM system* To verify if the system is MSDND secure in a seven node system this work will consider one node at a time and the parameter values they could falsify to affect the system. Below is the list of parameters that could be falsified along with a 7 node system architecture:

Node	Can Falsify
1	P_1, V_1, θ_1
2	P_2, V_2, θ_2
3	P_3, V_3, θ_3
4	P_4, V_4, θ_4
5	P_5, V_5, θ_5
6	P_6, V_6, θ_6
7	P_7, V_7, θ_7

Rather than going for MSDND analysis considering each node trying to falsify parameters, this work will analyze one node pattern which will have unique invariant violations. The thesis demonstrates below a detailed summary of the parameter violations and subsequent invariant violations.

Theorem 4.3.2.1. The 7 node system is MSDND secure when nodes 1 through 3 and 5 through 7 try to falsify associated parameters

Proof: As shown in the above table, when nodes other than node 4 try to falsify associated parameters, the invariant violation matches one of the other node parameter falsification. The MSDND proof of such a scenario matches any of the MSDND analysis from 3 node system. The MSDND analysis helps us to identify that there is something wrong for the system, however, it is not possible to identify the attacker in the system. As an example this work will consider MSDND of node 1. This work assumes node 1 tries to falsify its values and see what all invariants will be violated. A list of impacts over the invariants as below:

[1]MSDND with respect to identity of attacker exists when the security domains are able to identify there is something wrong in the system, however, are unable to narrow down to the causing entity. It is worth noting here that in such a situation peer nodes can narrow down to a group of malicious nodes based over the type of invariants violated. For Example: In a case where node 1 tries to falsify P_1, V_1, θ_1, sober nodes can narrow down to a group of nodes N_1 or N_2 based over the invariant violated, as the probable malicious nodes.

Table 4.3. 7 Node System - Invariant Violations

Malicious Node	Falsified Parameter	Invariant Violation	Comment[1]
1	P_1	I_a	MSDND with respect to identity of attacker
1	V_1, θ_1	I_a, I_b	
1	P_1, V_1, θ_1	I_b	
2	P_2	I_b	MSDND with respect to identity of attacker
2	V_2, θ_2	I_a, I_b, I_c	
2	P_2, V_2, θ_2	I_c	
3	P_3	I_c	MSDND with respect to identity of attacker
3	V_3, θ_3	I_b, I_c, I_d	
3	P_3, V_3, θ_3	I_b, I_d	
4	P_4	I_d	Unique pattern invariant violation
4	V_4, θ_4	I_c, I_d, I_e	
4	P_4, V_4, θ_4	I_c, I_e	
5	P_5	I_e	MSDND with respect to identity of attacker
5	V_5, θ_5	I_d, I_e, I_f	
5	P_5, V_5, θ_5	I_d, I_f	
6	P_6	I_f	MSDND with respect to identity of attacker
6	V_6, θ_6	I_e, I_f, I_g	
6	P_6, V_6, θ_6	I_e	
7	P_7	I_g	MSDND with respect to identity of attacker
7	V_7, θ_7	I_f, I_g	
7	P_7, V_7, θ_7	I_f	

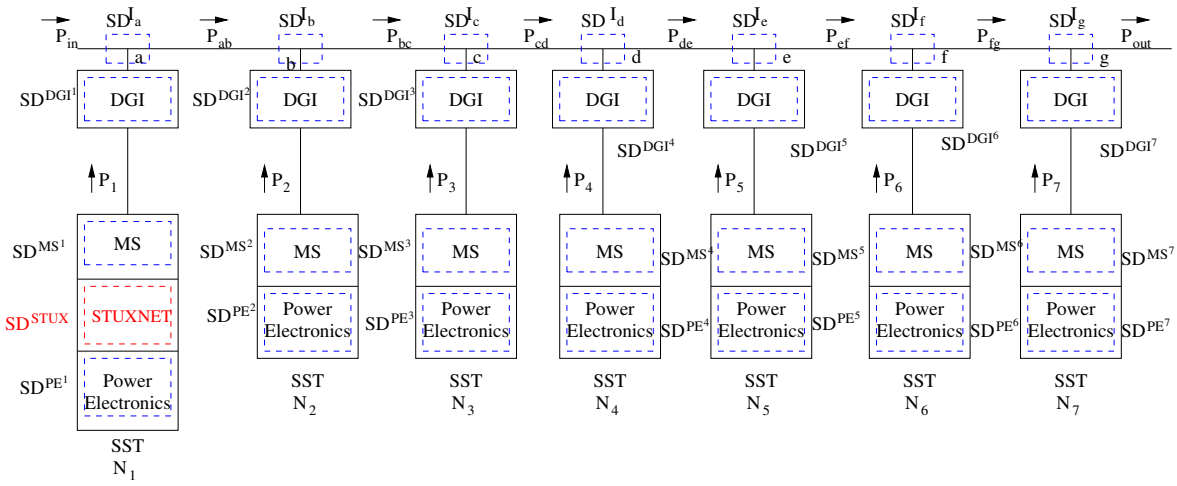

Figure 4.18. Node 1 acting as malicious node in a 7 Node system

- Falsifying P_1 will lead to an invariant I_a violation at point of common coupling a.
- Falsifying V_1 and θ_1 will lead to an invariant I_a, I_b violation at point of common coupling a and b respectively.
- Falsifying P_1, V_1 and θ_1 will lead to an invariant I_a violation at points of common coupling a and b.

The system is not MSDND secure when Node 1 tries to falsify V_1 and θ_1

Proof: Let us assume Node 1 tried to falsify V_1 and θ_1. To represent the corrupt values, this work will consider P as the entity of exchange.

- $\sim P = True$; Generation reading reported is not normal
- $I_{DGI^2,DGI^1}(P)$; Node 2 gets generation values from node 1
- $B_{DGI^2} I_{DGI^2,DGI^1}(P)$; Node 2 believes reading from node 1
- $T_{DGI^2,DGI^1}(P)$; Node 2 trusts Node 1
- Considering Node 1 tries to falsify V_1 and θ_1
- $I_{DGI^2,I_b}(Invariant_b)$; Node 2 gets the invariant I_b from SD^{I_b}
- $B_{DGI^2} I_{DGI^2,I_b}(Invariant_b)$; Node 2 believes the reading from SD^{I_b}
- $T_{DGI^2,I_b}(Invariant_b)$; Node 2 trusts the reading from SD^{I_b}

- $I_{DGI^2,I_a}(Invariant_a)$; Node 2 gets the invariant I_a from SD^{I_a}
- $B_{DGI^2}I_{DGI^2,I_a}(Invariant_a)$; Node 2 believes the reading from SD^{I_a}
- $T_{DGI^2,I_a}(Invariant_a)$; Node 2 trusts the reading from SD^{I_a}
- $[B_{DGI^2}I_{DGI^2,DGI^1}(P) \wedge T_{DGI^2,DGI^1}(P)]$
  $\wedge [B_{DGI^2}I_{DGI^2,I_b}(Invariant_b) \wedge T_{DGI^2,I_b}(Invariant_b)]$
  $\wedge [B_{DGI^2}I_{DGI^2,I_a}(Invariant_a) \wedge T_{DGI^2,I_a}(Invariant_a)] \rightarrow\sim B_{DGI^2}(P)$; Node 2 does not believe the reading based over the invariant violations
- $w \vDash v_P^{DGI^2} = True$; Valuation function exists in security domain for node 2 DGI

$$MSDND(ES) \neq \exists w \in W \vdash [(S_P \oplus S_{\sim P})] \wedge \left[w \vDash (\exists v_P^{DGI^2}(w) \wedge \exists v_{\sim P}^{DGI^2}(w))\right]$$

The system is MSDND secure when Node 1 tries to falsify P_1, V_1 and θ_1

Proof: Let us assume Node 1 tried to falsify P_1, V_1 and θ_1. To represent the corrupt values, this work will consider P as the entity of exchange.

- $\sim P = True$; Generation reading reported is not normal
- $I_{DGI^2,DGI^1}(P)$; Node 2 gets generation values from node 1
- $B_{DGI^2}I_{DGI^2,DGI^1}(P)$; Node 2 believes reading from node 1
- $T_{DGI^2,DGI^1}(P)$; Node 2 trusts Node 1
- Considering Node 1 tries to falsify P_1, V_1 and θ_1
- The invariant $I_b = P_{ab} + P_2 - P_{bc} = 0$ should be violated and, falsifying P_1, V_1 and θ_1 violates the invariant.
- $I_{DGI^2,I_b}(Invariant_b)$; Node 2 gets the invariant I_b from SD^{I_b}
- $B_{DGI^2}I_{DGI^2,I_b}(Invariant_b)$; Node 2 believes the reading from SD^{I_b}
- $T_{DGI^2,I_b}(Invariant_b)$; Node 2 trusts the reading from SD^{I_b}

- $[B_{DGI^2} I_{DGI^2,DGI^1}(P) \wedge T_{DGI^2,DGI^1}(P)]$
  $\wedge [B_{DGI^2} I_{DGI^2,I_b}(Invariant_b) \wedge T_{DGI^2,I_b}(Invariant_b)] \rightarrow\sim B_{DGI^2}(P)$; Node 2 does not believe the reading based over the invariant violations
- $w \vDash v_P^{DGI^2} = True$; Valuation function exists in security domain for node 2 DGI to identify that generation values reported are corrupt.
- $w \vDash v_{N_i}^{DGI^2} = False$; Valuation function does not exist in security domain for node 2 DGI to identify which node reported corrupt generation values.

$$MSDND(ES) = \exists\, w \in W \vdash [(S_P \oplus S_{\sim P})] \wedge \left[w \vDash (\exists\, v_P^{DGI^2}(w) \wedge \exists\, v_{\sim P}^{DGI^2}(w))\right] \wedge \left[w \vDash (\nexists\, v_{N_i}^{DGI^2}(w) \wedge \nexists\, v_{\sim N_i}^{DGI^2}(w))\right]$$

Remark: Here, the above case of invariants violation leads to MSDND secure system. From the above equation, it can be clearly demonstrated that the security domain 4 has a valuation function to identify if something wrong is going on in the system, however, it is not possible to identify the origin of the attack. The invariant I_b can be affected by falsifying either of the P_1, V_1 and θ_1 by node 1 or P_2 by node 2. Hence, in a 3 node system it is impossible to identify which of the two nodes falsified values for invariant to report the problem in system.

The system is not MSDND secure when Node 1 tries to falsify P_1

Proof: Let us assume Node 1 tried to falsify P_1. To represent the corrupt values, this work will consider P as the entity of exchange.

- $\sim P = True$; Generation reading reported is not normal
- $I_{DGI^2,DGI^1}(P)$; Node 2 gets generation values from node 1
- $B_{DGI^2} I_{DGI^2,DGI^1}(P)$; Node 2 believes reading from node 1
- $T_{DGI^2,DGI^1}(P)$; Node 2 trusts Node 1
- Considering Node 1 tries to falsify P_1

- The invariant $I_a = P_{in} + P_1 - P_{ab} = 0$ should be violated and, falsifying P_1 violates the invariant.
- $I_{DGI^2,I_a}(Invariant_a)$; Node 2 gets the invariant I_a from SD^{I_a}
- $B_{DGI^2}I_{DGI^2,I_a}(Invariant_a)$; Node 2 believes the reading from SD^{I_a}
- $T_{DGI^2,I_a}(Invariant_a)$; Node 2 trusts the reading from SD^{I_a}
- $[B_{DGI^2}I_{DGI^2,DGI^1}(P) \wedge T_{DGI^2,DGI^1}(P)]$ $\wedge [B_{DGI^2}I_{DGI^2,I_a}(Invariant_a) \wedge T_{DGI^2,I_a}(Invariant_a)] \rightarrow\sim B_{DGI^2}(P)$; Node 2 does not believe the reading based over the invariant violations
- $w \vDash v_P^{DGI^2} = True$; Valuation function exists in security domain for node 2 DGI

$$MSDND(ES) \neq \exists w \in W \vdash [(S_P \oplus S_{\sim P})] \wedge \left[w \vDash (\exists v_P^{DGI^2}(w) \wedge \exists v_{\sim P}^{DGI^2}(w))\right]$$

Theorem 4.3.2.2. The 7 node system is not MSDND secure when node 4 tries to falsify associated parameters

Proof: This work assumes node 4 tries to falsify its values and see what all invariants will be violated. A list of impacts over the invariants is as below:

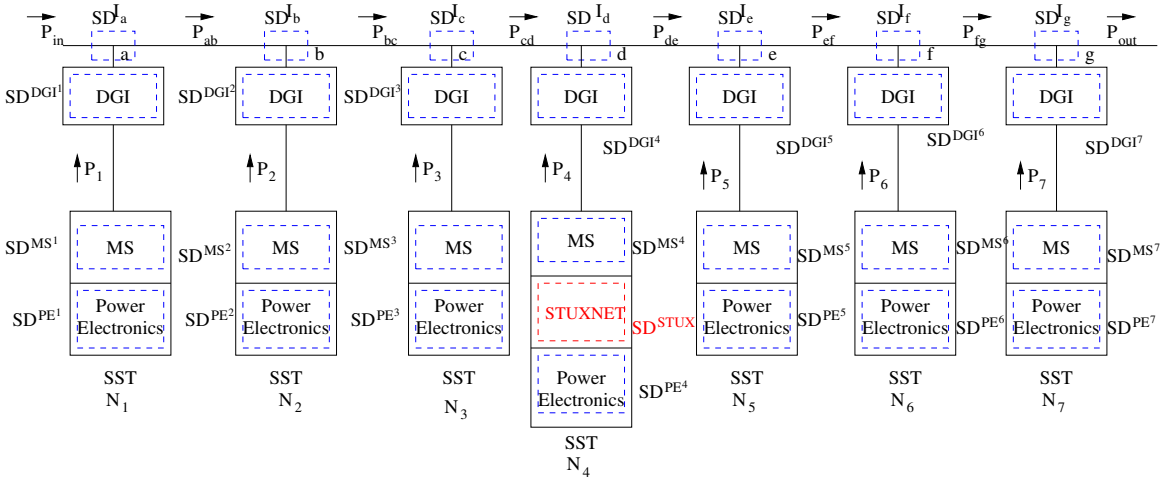

Figure 4.19. Node 4 acting as malicious node in a 7 Node system

- Falsifying P_4 will lead to an invariant I_d violation at point of common coupling d.
- Falsifying V_4 and θ_4 will lead to an invariant I_c, I_d and I_e violation at point of common coupling c, d and e respectively.
- Falsifying P_4, V_4 and θ_4 will lead to an invariant I_c and I_e violation at points of common coupling c and e.

The system is not MSDND secure when Node 4 tries to falsify V_4 and θ_4

Proof: Let us assume Node 1 tried to falsify V_1 and θ_1. To represent the corrupt values, this work will consider P as the entity of exchange.

- $\sim P = True$; Generation reading reported is not normal
- $I_{DGI^3,DGI^4}(P)$; Node 3 gets generation values from node 4
- $B_{DGI^3} I_{DGI^3,DGI^4}(P)$; Node 3 believes reading from node 4
- $T_{DGI^3,DGI^4}(P)$; Node 3 trusts Node 4
- $I_{DGI^5,DGI^4}(P)$; Node 5 gets generation values from node 4
- $B_{DGI^5} I_{DGI^5,DGI^4}(P)$; Node 5 believes reading from node 4
- $T_{DGI^5,DGI^4}(P)$; Node 5 trusts Node 4
- Considering Node 4 tries to falsify V_4 and θ_4, invariants I_c, I_d and I_e will be violated
- $I_{DGI^3,I_c}(Invariant_c)$; Node 3 gets the invariant I_c from SD_9
- $B_{DGI^3} I_{DGI^3,I_c}(Invariant_c)$; Node 3 believes the reading from SD_9
- $T_{DGI^3,I_c}(Invariant_c)$; Node 3 trusts the reading from SD_9
- $I_{DGI^3,I_d}(Invariant_d)$; Node 3 gets the invariant I_d from SD_13
- $B_{DGI^3} I_{DGI^3,I_d}(Invariant_d)$; Node 3 believes the reading from SD_13
- $T_{DGI^3,I_d}(Invariant_d)$; Node 3 trusts the reading from SD_13
- $I_{DGI^3,I_e}(Invariant_e)$; Node 3 gets the invariant I_e from SD_{17}
- $B_{DGI^3} I_{DGI^3,I_e}(Invariant_e)$; Node 3 believes the reading from SD_{17}
- $T_{DGI^3,I_e}(Invariant_e)$; Node 3 trusts the reading from SD_{17}

- $[B_{DGI^3} I_{DGI^3,DGI^4}(P) \wedge T_{DGI^3,DGI^4}(P)]$
  $\wedge [B_{DGI^3} I_{DGI^3,I_c}(Invariant_c) \wedge T_{DGI^3,I_c}(Invariant_c)]$
  $\wedge [B_{DGI^3} I_{DGI^3,I_d}(Invariant_d) \wedge T_{DGI^3,I_d}(Invariant_d)]$
  $\wedge [B_{DGI^3} I_{DGI^3,I_e}(Invariant_e) \wedge T_{DGI^3,I_e}(Invariant_e)] \rightarrow\sim B_{DGI^3}(P)$; Node 3 does not believe the reading based over the invariant violations
- $w \vDash v_P^{DGI^3} = True$; Valuation function exists in security domain for node 3 DGI
- $I_{DGI^5,I_c}(Invariant_c)$; Node 5 gets the invariant I_c from SD_9
- $B_{DGI^5} I_{DGI^5,I_c}(Invariant_c)$; Node 5 believes the reading from SD_9
- $T_{DGI^5,I_c}(Invariant_c)$; Node 5 trusts the reading from SD_9
- $I_{DGI^5,I_d}(Invariant_d)$; Node 5 gets the invariant I_d from SD_13
- $B_{DGI^5} I_{DGI^5,I_d}(Invariant_d)$; Node 5 believes the reading from SD_13
- $T_{DGI^5,I_d}(Invariant_d)$; Node 5 trusts the reading from SD_13
- $I_{DGI^5,I_e}(Invariant_e)$; Node 5 gets the invariant I_e from SD_{17}
- $B_{DGI^5} I_{DGI^5,I_e}(Invariant_e)$; Node 5 believes the reading from SD_{17}
- $T_{DGI^5,I_e}(Invariant_e)$; Node 5 trusts the reading from SD_{17}
- $[B_{DGI^5} I_{DGI^5,DGI^4}(P) \wedge T_{DGI^5,DGI^4}(P)]$
  $\wedge [B_{DGI^5} I_{DGI^5,I_c}(Invariant_c) \wedge T_{DGI^5,I_c}(Invariant_c)]$
  $\wedge [B_{DGI^5} I_{DGI^5,I_d}(Invariant_d) \wedge T_{DGI^5,I_d}(Invariant_d)]$
  $\wedge [B_{DGI^5} I_{DGI^5,I_e}(Invariant_e) \wedge T_{DGI^5,I_e}(Invariant_e)] \rightarrow\sim B_{DGI^5}(P)$; Node 5 does not believe the reading based over the invariant violations
- $w \vDash v_P^{DGI^5} = True$; Valuation function exists in security domain for node 5 DGI

$$MSDND(ES) \neq \exists w \in W \vdash [(S_P \oplus S_{\sim P})] \wedge \left[w \vDash (\exists v_P^{DGI^3}(w) \wedge \exists v_{\sim P}^{DGI^3}(w))\right]$$

$$MSDND(ES) \neq \exists w \in W \vdash [(S_P \oplus S_{\sim P})] \wedge \left[w \vDash (\exists v_P^{DGI^5}(w) \wedge \exists v_{\sim P}^{DGI^5}(w))\right]$$

The system is not MSDND secure when Node 4 tries to falsify P_4, V_4 and θ_4

Proof: Let us assume Node 4 tried to falsify P_4, V_4 and θ_4. To represent the corrupt values, this work will consider P as the entity of exchange.

- $\sim P = True$; Generation reading reported is not normal
- $I_{DGI^3,DGI^4}(P)$; Node 3 gets generation values from node 4
- $B_{DGI^3} I_{DGI^3,DGI^4}(P)$; Node 3 believes reading from node 4
- $T_{DGI^3,DGI^4}(P)$; Node 3 trusts Node 4
- $I_{DGI^5,DGI^4}(P)$; Node 5 gets generation values from node 4
- $B_{DGI^5} I_{DGI^5,DGI^4}(P)$; Node 5 believes reading from node 4
- $T_{DGI^5,DGI^4}(P)$; Node 5 trusts Node 4
- Considering Node 4 tries to falsify P_4, V_4 and θ_4, invariants I_c and I_e will be violated
- $I_{DGI^3,I_c}(Invariant_c)$; Node 3 gets the invariant I_c from SD_9
- $B_{DGI^3} I_{DGI^3,I_c}(Invariant_c)$; Node 3 believes the reading from SD_9
- $T_{DGI^3,I_c}(Invariant_c)$; Node 3 trusts the reading from SD_9
- $I_{DGI^3,I_e}(Invariant_e)$; Node 3 gets the invariant I_e from SD_{17}
- $B_{DGI^3} I_{DGI^3,I_e}(Invariant_e)$; Node 3 believes the reading from SD_{17}
- $T_{DGI^3,I_e}(Invariant_e)$; Node 3 trusts the reading from SD_{17}
- $[B_{DGI^3} I_{DGI^3,DGI^4}(P) \wedge T_{DGI^3,DGI^4}(P)]$
  $\wedge [B_{DGI^3} I_{DGI^3,I_c}(Invariant_c) \wedge T_{DGI^3,I_c}(Invariant_c)]$
  $\wedge [B_{DGI^3} I_{DGI^3,I_e}(Invariant_e) \wedge T_{DGI^3,I_c}(Invariant_e)] \rightarrow\sim B_{DGI^3}(P)$; Node 3 does not believe the reading based over the invariant violations
- $w \vDash v_P^{DGI^3} = True$; Valuation function exists in security domain for node 3 DGI
- $I_{DGI^5,I_c}(Invariant_c)$; Node 5 gets the invariant I_c from SD_9
- $B_{DGI^5} I_{DGI^5,I_c}(Invariant_c)$; Node 5 believes the reading from SD_9
- $T_{DGI^5,I_c}(Invariant_c)$; Node 5 trusts the reading from SD_9
- $I_{DGI^5,I_e}(Invariant_e)$; Node 5 gets the invariant I_e from SD_{17}
- $B_{DGI^5} I_{DGI^5,I_e}(Invariant_e)$; Node 5 believes the reading from SD_{17}

- $T_{DGI^5,I_e}(Invariant_e)$; Node 5 trusts the reading from SD_17
- $[B_{DGI^5} I_{DGI^5,DGI^4}(P) \wedge T_{DGI^5,DGI^4}(P)]$
  $\wedge [B_{DGI^5} I_{DGI^5,I_c}(Invariant_c) \wedge T_{DGI^5,I_c}(Invariant_c)]$
  $\wedge [B_{DGI^5} I_{DGI^5,I_e}(Invariant_e) \wedge T_{DGI^5,I_e}(Invariant_e)] \rightarrow\sim B_{DGI^5}(P)$; Node 5 does not believe the reading based over the invariant violations
- $W \vDash V_P^{DGI^5} = True$; Valuation function exists in security domain for node 5 DGI

$$MSDND(ES) \neq \exists w \in W \vdash [(S_P \oplus S_{\sim P})] \wedge \left[w \vDash (\exists v_P^{DGI^3}(w) \wedge \exists v_{\sim P}^{DGI^3}(w))\right]$$
$$MSDND(ES) \neq \exists w \in W \vdash [(S_P \oplus S_{\sim P})] \wedge \left[w \vDash (\exists v_P^{DGI^5}(w) \wedge \exists v_{\sim P}^{DGI^5}(w))\right]$$

The system is not MSDND secure when Node 4 tries to falsify P_4

Proof: Let us assume Node 4 tried to falsify P_4. To represent the corrupt values, this work will consider P as the entity of exchange.

- $\sim P = True$; Generation reading reported is not normal
- $I_{DGI^3,DGI^4}(P)$; Node 3 gets generation values from node 4
- $B_{DGI^3} I_{DGI^3,DGI^4}(P)$; Node 3 believes reading from node 4
- $T_{DGI^3,DGI^4}(P)$; Node 3 trusts Node 4
- $I_{DGI^5,DGI^4}(P)$; Node 5 gets generation values from node 4
- $B_{DGI^5} I_{DGI^5,DGI^4}(P)$; Node 5 believes reading from node 4
- $T_{DGI^5,DGI^4}(P)$; Node 5 trusts Node 4
- Considering Node 4 tries to falsify V_4 and θ_4, invariant I_d will be violated
- $I_{DGI^3,I_d}(Invariant_d)$; Node 3 gets the invariant I_d from SD_13
- $B_{DGI^3} I_{DGI^3,I_d}(Invariant_d)$; Node 3 believes the reading from SD_13
- $T_{DGI^3,I_{4d}}(Invariant_d)$; Node 3 trusts the reading from SD_13

- $[B_{DGI^3} I_{DGI^3,DGI^4}(P) \wedge T_{DGI^3,DGI^4}(P)]$
  $\wedge [B_{DGI^3} I_{DGI^3,I_d}(Invariant_d) \wedge T_{DGI^3,I_d}(Invariant_d)] \rightarrow\sim B_{DGI^3}(P)$; Node 3 does not believe the reading based over the invariant violations
- $W \vDash V_P^{DGI^3} = True$; Valuation function exists in security domain for node 3 DGI
- $I_{DGI^5,I_d}(Invariant_d)$; Node 5 gets the invariant I_d from $SD_1 3$
- $B_{DGI^5} I_{DGI^5,I_d}(Invariant_d)$; Node 5 believes the reading from $SD_1 3$
- $T_{DGI^5,I_d}(Invariant_d)$; Node 5 trusts the reading from $SD_1 3$
- $[B_{DGI^5} I_{DGI^5,DGI^4}(P) \wedge T_{DGI^5,DGI^4}(P)]$
  $\wedge [B_{DGI^5} I_{DGI^5,I_d}(Invariant_d) \wedge T_{DGI^5,I_d}(Invariant_d)] \rightarrow\sim B_{DGI^5}(P)$; Node 5 does not believe the reading based over the invariant violations
- $w \vDash v_P^{DGI^5} = True$; Valuation function exists in security domain for node 5 DGI

$$MSDND(ES) \neq \exists w \in W \vdash [(S_P \oplus S_{\sim P})] \wedge \left[w \vDash (\exists v_P^{DGI^3}(w) \wedge \exists v_{\sim P}^{DGI^3}(w))\right]$$

$$MSDND(ES) \neq \exists w \in W \vdash [(S_P \oplus S_{\sim P})] \wedge \left[w \vDash (\exists v_P^{DGI^5}(w) \wedge \exists v_{\sim P}^{DGI^5}(w))\right]$$

5. CONCLUSIONS

5.1. DISTRIBUTED CYBER PHYSICAL SYSTEMS

In a cyber physical system, that is distributed in nature, an important characteristic is communication among the distributed components. The message flow among these components is the basis or a primary requirement for the system to function correctly. This message communication can also be considered as the information flow. To protect the functioning of a cyber physical system it is important to protect this information flow or verify the information flowing through it.

5.2. MSDND

Multiple security domain non-deducibility helps us to segregate a cyber physical system into separate components, where the different components do not trust over the information supplied by one another. The concept of security domains, valuation functions and invariants introduced by MSDND provides us the ways in which information flows can be verified and checked among different components. The invariants help us adding in multiple paths for similar information to flow from one component to another, thereby making it more difficult for an attacker to attack the system and go unnoticed.

5.3. STATE COLLECTION PROTOCOL IN THE FREEDM SYSTEM

This work takes the FREEDM system as a target cyber physical system and identifies MSDND secure paths in the information flowing through the system.The state collection protocol produces information flow, which is based over Chandy Lamport distributed snapshot algorithm. MSDND analysis over the state collection protocol shows that the information

flow paths are MSDND secure in the presence of a STUXNET-like attack. The thesis breaks the MSDND secure information flow using Byzantine consensus solution, however, a further sophisticated attack sharing similar falsified values to distributed components is still able to hide the attack.

5.4. MSDND ANALYSIS OF THE PHYSICAL ATTESTATION PROTOCOL

MSDND analysis of the physical attestation protocol helps to introduce deducibility in the FREEDM system. This work uses a physical attestation protocol over a 3 node and a 7 node system. In a 3 node system the protocol is unable to identify the origin of the attack, however, it is able to identify that something is wrong with the system and narrows it down to a group of nodes that may be causing the problem. Extending the case to a 7 node system, physical attestation gives us a unique pattern of invariant violations that is able to narrow down to the malicious node. The same is still restrictive in implementation as a unique pattern of invariant violations has a specific requirement to be present in between 3 nodes on the either side.

5.5. SUMMARY

The MSDND model helps us to identify STUXNET-like attacks where the intention of the attacker is to corrupt the information rather than steal it. Using the MSDND model this work is able to analyze MSDND secure paths inside the FREEDM smart grid infrastructure. MSDND secure paths are bad for the system, as different components in the system are unable to verify the information being passed to them by other components. This work also uses the MSDND model along with the invariants provided by physical attestation protocol to break the MSDND secure paths. A summary of the MSDND analysis for different information paths is represented in Table 5.1

Table 5.1. MSDND analysis results

Theorem	Attack type	MSDND
DGI - Device interaction	Normal operations	No
	STUXNET-like	Yes
DGI - DGI interaction	Normal operations	No
	STUXNET-like	Yes
DGI - DGI interaction with Byzantine consensus	STUXNET-like sharing different falsified status to different nodes	No
	STUXNET-like sharing similar falsified status to different nodes	Yes
Physical attestation in a 3 node system	STUXNET-like	MSDND with respect to identity of attacker
Physical attestation in a 7 node system	STUXNET-like	No

REFERENCES

Adepu, S. and Mathur, A., 'Using process invariants to detect cyber attacks on a water treatment system,' in 'IFIP International Information Security and Privacy Conference,' Springer, 2016 pp. 91–104.

Chandy, K. M. and Lamport, L., 'Distributed snapshots: Determining global states of distributed systems,' ACM Transactions on Computer Systems (TOCS), 1985, **3**(1), pp. 63–75.

Chen, T., 'Stuxnet, the real start of cyber warfare?[editor's note],' IEEE Network, 2010, **24**(6), pp. 2–3.

Crow, M. L., McMillin, B., Wang, W., and Bhattacharyya, S., 'Intelligent energy management of the freedm system,' in 'Power and Energy Society General Meeting, 2010 IEEE,' IEEE, 2010 pp. 1–4.

Duan, J. and Chow, M.-Y., 'Data integrity attack on consensns-based distributed energy management algorithm,' in 'Power & Energy Society General Meeting, 2017 IEEE,' IEEE, 2017 pp. 1–5.

Howser, G. and McMillin, B., 'A multiple security domain model of a drive-by-wire system,' in 'Computer Software and Applications Conference (COMPSAC), 2013 IEEE 37th Annual,' IEEE, 2013 pp. 369–374.

Howser, G. and McMillin, B., 'A modal model of stuxnet attacks on cyber-physical systems: A matter of trust,' in 'Software Security and Reliability, 2014 Eighth International Conference on,' IEEE, 2014 pp. 175–183.

Huang, A. Q., Crow, M. L., Heydt, G. T., Zheng, J. P., and Dale, S. J., 'The future renewable electric energy delivery and management (freedm) system: the energy internet,' Proceedings of the IEEE, 2011, **99**(1), pp. 133–148.

Lamport, L., Shostak, R., and Pease, M., 'The byzantine generals problem,' ACM Transactions on Programming Languages and Systems (TOPLAS), 1982, **4**(3), pp. 382–401.

Liau, C.-J., 'Belief, information acquisition, and trust in multi-agent systems?a modal logic formulation,' Artificial Intelligence, 2003, **149**(1), pp. 31–60.

Liau, C.-J., 'A modal logic framework for multi-agent belief fusion,' ACM Transactions on Computational Logic (TOCL), 2005, **6**(1), pp. 124–174.

Owicki, S. and Gries, D., 'An axiomatic proof technique for parallel programs i,' Acta informatica, 1976, **6**(4), pp. 319–340.

Paul, T., Kimball, J. W., Zawodniok, M., Roth, T. P., McMillin, B., and Chellappan, S., 'Unified invariants for cyber-physical switched system stability,' IEEE Transactions on Smart Grid, 2014, **5**(1), pp. 112–120.

Roth, T. and McMillin, B., 'Physical attestation of cyber processes in the smart grid,' in 'International Workshop on Critical Information Infrastructures Security,' Springer, 2013 pp. 96–107.

Sutherland, D., 'A model of information,' in 'Proceedings of the 9th National Computer Security Conference,' NIST, 1986 pp. 225–234.

VITA

Manish Jaisinghani was born in Ajmer, Rajasthan, India. He received his Bachelor's degree in Computer Science from the prestigious university, Rajasthan Technical University, Kota, Rajasthan, India in May 2011. He then worked with Hcl Technologies Ltd. for three years as a Senior Analyst/Middleware Engineer in Noida, Uttar Pradesh,India, Ameriprise Financials as Associate/Middleware Engineer in Gurgaon, Haryana, India and IBM as Client Technical Specialist in Noida, Uttar Pradesh, India. His work was mainly focused on automation and process improvement. He was responsible for performance tuning of Middleware infrastructure, automate application and middleware integration and support java/j2ee applications supporting the business. His desire and keen interest in the fields of security and data motivated him to pursue graduate studies at the highly respected Missouri University of Science and Technology, Rolla, United States of America. During his graduate studies, he has been part of varied programs such as the Graduate Leadership program, Council of Graduate Studies and Missouri S&T Association for Computing Machinery (ACM) Special Interest Group. During his first semester at Missouri S&T he got an amazing opportunity to work over next generation cyber physical infrastructure FREEDM smart grid with his adviser, Dr. Bruce McMillin which is the base for his thesis. In May 2018 he received his MS degree in Computer Science from Missouri University of Science and Technology.