Appendix A
Resiliency Threat Analysis for SCADA

This chapter presents a formal model that automatically verify the resiliency of the SCADA system, particularly the resilient data acquisition for reliable execution of control operations. This formal model can verify the system with respect to the given resiliency specifications, as similar to the model presented in Chap. 3. While the previous solution looks for the satisfaction of the resilient observability constraint, this formal model searches for threat vectors that fail the resiliency requirement. The unsatisfiable outcome certifies that the system is resilient with respect to the specified resiliency.

A.1 *k*-Resilient Secured Observability Threat Model

The notations used in the following formal modeling are followed from those defined in Chap. 3. The modeling of the resiliency threat verification needs to utilize the secured data delivery constraint.

Secured Data Delivery The assured data delivery constraint (as defined in Chap. 3) verifies whether data can reach from the source to the destination, e.g., from a field device to the MTU, through zero, one, or more intermediate devices, but does not ensure if the transmission has occurred under necessary security measures. Although this constraint checks security pairing between the communicating parties, it is only to ensure necessary handshaking for communication. The secured data delivery constraint (*SecuredDelivery*) verifies whether data is sent under proper security measures, particularly authentication and integrity protection, including the assured data delivery. That is, the communicating nodes, e.g., an RTU and the MTU, may have correct security pairing, as they are using the same security protocol Challenge-Handshake Authentication Protocol (CHAP). However, this security pairing on CHAP only ensures authentication. In this case, the transmission will not

E. Al-Shaer, M.A. Rahman, *Security and Resiliency Analytics for Smart Grids*,
Advances in Information Security 67, DOI 10.1007/978-3-319-32871-3

be data integrity protected. Moreover, it is required to consider the vulnerabilities of the security measures in use. For example, if Data Encryption Standard (DES) is used for data encryption, the transmitted data cannot be considered as protected, as a good number of vulnerabilities of DES have already been found.

The formalization of the secured data delivery includes two more constraints, *Authenticated* and *IntegrityProtected*, that ensure the authentication of the communicating parties and the integrity of the transmitted data, respectively. The following equation presents the formalization of secured data delivery:

$$
\begin{aligned}
&\exists_K(\exists_k CryptType_{i,k} = K)\wedge \\
&\quad(\exists'_k CryptType_{i,k'} = K)\wedge \\
&\quad((CAlgo_K = hmac \wedge CKey_K \geq 128) \vee \ldots)) \\
&\qquad\rightarrow Authenticated_{i,j}
\end{aligned}
$$

$$
\begin{aligned}
&\exists_K(\exists_k CryptType_{i,k} = K)\wedge \\
&\quad(\exists'_k CryptType_{i,k'} = K)\wedge \\
&\quad((CAlgo_K = sha2 \wedge CKey_K \geq 128) \vee \ldots)) \\
&\qquad\rightarrow IntegrityProtected_{i,j}
\end{aligned}
$$

$$
\begin{aligned}
&Ied_I\wedge \\
&\exists_z\forall_{l\in|\mathscr{P}_{I,j,z}|}\ \{i',j'\} \in NodePair_l\wedge \\
&\quad Node_{i'} \wedge Node_{j'} \wedge Reachable_{i',j'}\wedge \\
&\quad CommPropPairing_{i',j'} \wedge CryptoPropPairing_{i',j'} \\
&\quad Authenticated_{i',j'} \wedge IntegrityProtected_{i',j'} \\
&\qquad\rightarrow\ SecuredDelivery_I
\end{aligned}
$$

The main difference between this formalization of *SecuredDelivery* and that presented in Chap. 3 is that the sides of the implies relation exchanged. This is because, unlike the previous modeling, this formal modeling is designed to look for the cases that make the secured observability fail.

Failure of Secured Observability The secured measurements are logically identified from the mappings between communicating field devices and measurements. Whether the system is observable securely is verified using the mappings between the secured measurements and the states. Let S_Z be a Boolean variable denoting whether measurement Z is secured. Then, the following two conditions ensure if measurement Z is secured:

$$\forall_{I\in IedSet}\forall_Z\ (Z \in MsrSet_I \wedge SecuredDelivery_I) \rightarrow S_Z$$

If a measurement is secured, the variables corresponding to this measurement can be securely estimated. If SE_X denotes whether state X is securely estimated, then the following must hold:

$$\forall_Z \ \forall_{X \in StateSet_Z} \ S_Z \rightarrow SE_X$$

The set of securely delivered unique measurements (with respect to $UMsrSet_E$) needs to be identified. Let $SecUMsr_E$ be this set. Then, it is formed as follows:

$$\forall_E \ \exists_{Z \in UMsrSet_E} S_Z \rightarrow \ SecUMsr_E$$

The secured observability (*SecuredObservability*) ensures that the minimum number (i.e., at least m) of secured measurements are received and all states are covered by these secured measurements. Thus, the system is securely unobservable ($\neg$*SecuredObservability*) when either or both of the following two conditions fail:

$$\neg SecuredObservability \rightarrow$$
$$(\exists_X \neg SE_X) \vee (\sum_E SecUMsr_E < m)$$

***k*-Resilient Secured Observability Threat** This constraint verifies whether secured observability is ensured even if k field devices (or k_1 IEDs and k_2 RTUs) are unavailable due to technical failures or cyber attacks. The verification of k-resilient secured observability is verified by searching for threat vectors under the specification of maximum k failures. When the number of unavailable devices is no larger than k devices (or k_1 IEDs and k_2 RTUs), the threat against the k-resilient secured observability constraint ($\neg$*ResilientSecuredObservability*) is formalized as follows:

$$((N - \sum_{1 \leq i \leq N} Node_i) \leq k) \wedge \neg SecuredObservability$$
$$\rightarrow \ \neg ResilientSecuredObservability$$

$$((N_1 - \sum_{1 \leq i \leq N} (Node_i \times Ied_i)) \leq k_1) \wedge$$
$$((N_2 - \sum_{1 \leq i \leq N} (Node_i \times Rtu_i)) \leq k_1) \wedge$$
$$\neg SecuredObservability$$
$$\rightarrow \ \neg ResilientSecuredObservability$$

The threat vector (**V**) includes a list of devices such that if they fails the secured observability is impossible. In this way, this proposed modeling synthesizes attack vectors and, thus, provides inputs to learn the dependability breach points.

A.2 A Case Study

This section presents an example that illustrates the execution of the model in two synthetic attack scenarios. These scenarios demonstrate the k_1, k_2-resilient secured observability constraint.

SCADA Topology 1 This example considers the 5-bus SCADA system as shown in Fig. 3.5 of Chap. 3. The input is partially shown in Table A.1. The input includes primarily the Jacobian matrix corresponding to the bus system, the connectivity between the communicating devices, the association of the measurements with the IEDs, and security profiles of each communicating host pair. Each row of

Table A.1 The input to the case study

Number of states and measurements
5 14
Jacobian matrix (mapping between the states and the measurements)
0 -5.05 5.05 0 0
0 -5.67 0 5.67 0
0 -5.75 0 0 5.75
0 0 0 -23.75 23.75
16.9 -16.9 0 0 0
4.48 0 0 0 -4.48
0 5.67 0 -5.67 0
0 5.75 0 0 -5.75
0 0 5.85 -5.85 0
0 0 0 23.75 -23.75
-16.9 33.37 -5.05 -5.67 -5.75
0 -5.05 10.9 -5.85 0
0 -5.67 -5.85 41.85 -23.75
-4.48 -5.75 0 -23.75 37.95
Number of each type of devices in the topology
IEDs (Id 1-8), RTUs (Id 9-12), MTU (Id 13), Router (Id 14)
8 4 1 1
Topology (Links)
13 #Number of communicating links
1 9
2 9

(continued)

Table A.1 (continued)

```
3 9
. . . . . .
# Measurements corresponding to IEDs
1 1 2
2 3 5
3 11
4 12
5 4 7 9
6 13
7 6 8 10
8 14
# Security profile (if exists) between the communicating entities
11 # Number entries of security profiles
1 9 hmac 128
2 9 chap 64 sha2 128
3 9 chap 64 sha2 128
5 11 chap 64 sha2 256
6 11 chap 64 sha2 256
7 12 chap 64 sha2 128
8 12 chap 64 sha2 128
9 13 rsa 2048 aes 256
10 11 hmac 128
11 13 rsa 4096 aes 256
12 13 rsa 2048 aes 256
# k-resiliency requirements (IED, RTU)
1 1
```

the Jacobian matrix corresponds to a measurement. The first row corresponds to measurement 1, and similarly the rest. Each row has five entries (columns) which correspond to five buses or states. It is assumed that the measurements are recorded by different IEDs only, and these measurements are sent to the MTU (i.e., the SCADA server at the control center) through RTUs. The server needs these measurements to estimate the current states of the system. The resiliency requirement specify that the secured observability must be satisfied even if one IED and one RTU are unavailable (due to being suffered by technical failures or cyber attacks).

In this case of $(1, 1)$-resiliency verification, the model provides a *sat* result. That is, the system is not $(1, 1)$-resilient for secured observability, although it is $(1, 1)$-resilient observable. According to the result, if IED 3 and RTU 11 are unavailable, it is not possible to observe the system securely. There are 4 more threat vectors that can make the system unobservable. The reason is, as the result also shows, that measurements from IED 1 and RTU 9 are not data integrity protected, and as a result

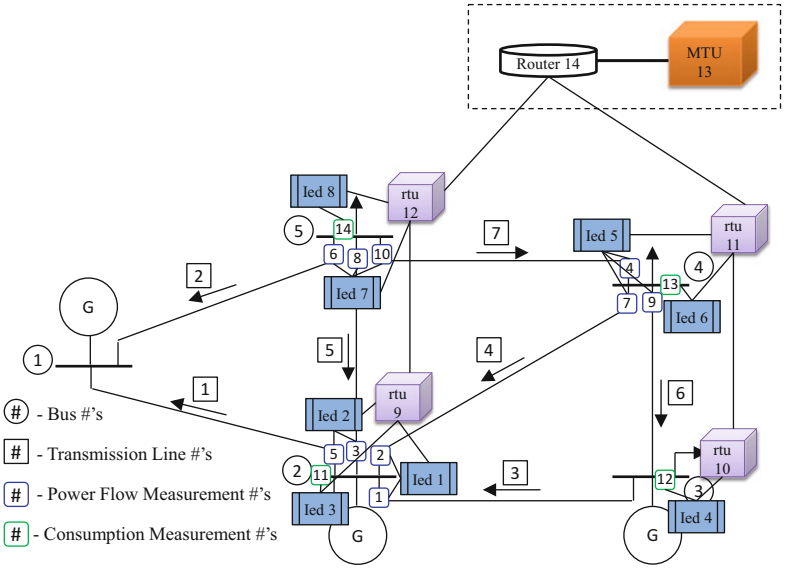

Fig. A.1 The SCADA topology of the 5-bus power grid (example scenario 2)

thus the secured observability. If the resiliency specification is reduced to $(1, 0)$ or $(0, 1)$, the model gives *unsat* result. That is, the system is securely observable even if any IED or RTU fails.

SCADA Topology 2 This scenario considers the topology shown in Fig. A.1. This SCADA topology is similar to that of Fig. 3.5, except RTU 9 is now connected with RTU 12. In this scenario, the system is not resilient any more for one RTU failures. However, there are only one threat vector (unavailability of RTU 12) to fail the secured observability.

Index

E. Al-Shaer, M.A. Rahman, *Security and Resiliency Analytics for Smart Grids*,
Advances in Information Security 67, DOI 10.1007/978-3-319-32871-3