Distributed Wardrop Load Balancing in Multi-MTU SCADA Systems*

Vincenzo Suraci, Lorenzo Ricciardi Celsi, Alessandro Giuseppi,
Gioacchino Manfredi, and Alessandro Di Giorgio

***Abstract*— This paper presents a distributed strategy for load balancing in a multi-MTU SCADA system, whose automatic control layer is such that its MTU Plane is modeled as a networked dynamical system. The proposed control law, under which the considered system is proven to converge to a Wardrop equilibrium, is also used for the purpose of equilibrium recovery in load distribution among MTUs after the occurrence of a possible MTU failure event induced by a cyber-physical attack (e.g., a Denial of Service attack). Numerical simulations with respect to realistic scenarios are reported to show the effectiveness of the proposed approach.**

I. Introduction

Supervisory Control and Data Acquisition (SCADA) *systems* have been playing a role of paramount importance in several safety-critical infrastructures, e.g., electrical power grids, nuclear plants, transportation systems, gas and water distribution networks, heating, ventilation and air conditioning systems in buildings, traffic control systems in airports, etc. Due to the integration of cyber technologies with physical processes, such infrastructures have become increasingly susceptible to cyber-physical attacks. Previous related work can be found, for instance, in [1]-[5].

For instance, modern power grids are tightly coupled with a SCADA system that has to be designed in order to control and supervise their operation. Nonetheless, they are becoming increasingly vulnerable to malicious attacks targeting power generation plants as well as the transmission and distribution network [6].

According to [7], the architecture of a modern SCADA system foresees three layers:

- the *supervisory control layer*,
- the *automatic control layer*, and
- the *physical layer*,

all interconnected by means of a communication network. In particular, the automatic control layer is aimed at regulating the operation of the underlying physical processes on the grounds of (i) the control commands received from the supervisory control layer through the communication network, and of (ii) the sensor measurements received from the field devices at the physical layer through the communication network.

Within the automatic control layer, the *Remote Terminal Units* (RTUs) composing the *RTU Plane* are in charge of collecting data from sensors and control actuators possibly located at remote sites, and of sending such data back to the *Master Terminal Unit* (MTU) through the communication network. In this respect, RTU and MTU fault tolerance and attack resilience are key requirements for safety-critical processes. This issue has already been addressed with respect to RTUs in several works (e.g., in [8]), but has not been addressed yet as regards the possible event of MTU failure.

In this respect, we propose to adopt a Multi-MTU structure [9], i.e., the MTU Plane of the automatic control layer is characterized by K distinct MTUs operating in parallel with each other. Hence, we envisage a *Multi-MTU Plane* as shown in Fig. 1, where the association of the traffic coming from any RTU to the most appropriate MTU is made dynamically, based on the feedback represented by the current utilization factor of each MTU. This way, by relying on a distributed closed-loop dynamic load balancing algorithm, it is possible to ensure that the SCADA system stays *resilient* with respect to any *cyber-physical attack* (e.g., a *Denial of Service* attack originated by a Sybil attack [10]) aimed at compromising the operation of a single MTU by making it fail.

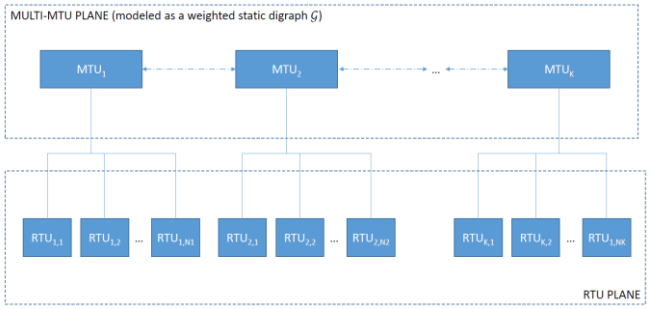

Figure 1. Enhanced automatic control layer of a SCADA system, consisting of an RTU Plane and of a Multi-MTU Plane (with K MTUs)

From the large body of literature on load balancing, we recall [11] as an example of centralized static cooperative load balancing, [12] as an example of centralized static non-cooperative load balancing, [13] as an example of centralized

*Research supported by the European Commission in the framework of the H2020 ATENA project (*Advanced tools to assess and mitigate the criticality of ICT components and their dependencies over critical infrastructures*) under Grant Agreement no. 700581.

V. Suraci is with the SMART Engineering Solutions & Technologies (SMARTEST) Research Center, eCampus University, Via Isimbardi 10, 22060 Novedrate (CO), Italy (e-mail: vincenzo.suraci@uniecampus.it).

L. Ricciardi Celsi, A. Giuseppi, G. Manfredi, and A. Di Giorgio are with the Department of Computer, Control and Management Engineering Antonio Ruberti, University of Rome La Sapienza, via Ariosto 25, 00185 Rome, Italy (email:{ricciardicelsi, giuseppi, digiorgio}@diag.uniroma1.it).

dynamic load balancing, and we also recall [14], which, instead, addresses the problem of distributed dynamic load balancing relying upon local cooperation among neighboring network nodes.

Moreover, load balancing can be dealt with by adopting advanced feedback control and machine learning methodologies also capable of exploiting, in real time, the information embedded in historical data and/or the real-time feedbacks provided by the users. We note that even the methodologies used in other application contexts (e.g., see [15] and [16] for energy control, [17] for traffic control, [18] for resource management, [19]-[21] for Quality of Experience control, and [22] and [23] for intelligent transportation systems) can be used to cope with load balancing.

The scenario considered in this paper requires a non-cooperative dynamic load balancing approach. This kind of algorithms are widely investigated in game-theoretic frameworks, where the problem can be described as a dynamic load balancing game, in which users distribute their loads in a non-cooperative and selfish fashion [24] (in some applications, these algorithms are also referred to as selfish routing ones). Moreover, in this paper we consider a renowned game-theoretic traffic model due to Wardrop [25], introduced to represent road traffic with an infinite number of agents, each being responsible for an infinitesimal amount of traffic. Within this framework, a certain amount of traffic, or flow demand, has to be routed from a given source to a given destination via a collection of paths. Each agent has the possibility to distribute its own flow among a set of admissible paths. The network is characterized by non-decreasing latency functions depending on the flows on the edges. A combination of flows such that the latencies of all the employed paths are minimal is called a Wardrop equilibrium for the network. Indeed, a Nash equilibrium is said to become a Wardrop equilibrium whenever the number of decision makers is assumed to be infinite [26].

The paper is organized as follows. Section II presents the mathematical model of the automatic control layer of a SCADA system as a networked dynamical system, and defines and discusses the distributed control problem for load balancing purposes. Section III reports some numerical examples showing both the performance of the proposed solution in different realistic scenarios and the equilibrium recovery time under the presented strategy. Concluding remarks in Section IV end the paper.

To the best of the authors' knowledge, this is the *first attempt* to solve a load balancing problem over the MTU Plane of a cyber-physical system by means of Wardrop-based arguments, also tackling the issue of Wardrop equilibrium recovery after MTU failure.

II. Cyber-Physical System Model in a Wardrop-Based Framework

A. Graph-Theoretical Tools and the Mathematical Model of the Automatic Control Layer of a SCADA System

Let us consider a generic *finite weighted static digraph* $\mathcal{G} = (\mathcal{V}, \mathcal{E}, \mathcal{A})$, where $\mathcal{V}$ is the related finite set of nodes, $\mathcal{E} \subseteq \mathcal{V} \times \mathcal{V}$ accounts for the set of edges, with $(m, m') \in \mathcal{E}$ if an arc from $m \in \mathcal{V}$ to $m' \in \mathcal{V}$ exists, and $\mathcal{A} = \{a_{m,m'}\}_{m,m' \in \mathcal{V}} \in [0, \eta]^{|\mathcal{V}| \times |\mathcal{V}|}$, with $\eta > 0$, represents the adjacency matrix and is such that $a_{m,m'} > 0$ if $(m, m') \in \mathcal{E}$, $a_{m,m'} = 0$ otherwise. In this paper, a node $m' \in \mathcal{V}$ is defined as a *neighbor* of node $m \in \mathcal{V}$ if there is an edge $(m, m') \in \mathcal{E}$ connecting them. We denote the set of neighbors of node $m \in \mathcal{V}$ with $\mathcal{N}_m$. Moreover, a weighted digraph $\mathcal{G}$ is said to be *strongly connected* if there always exists a directed path between every pair of nodes and there are no unreachable nodes. The *distance* between two nodes $m, m' \in \mathcal{V}$ is the length of the shortest path between them if m and m' are connected, it is infinite otherwise. The *diameter* of a strongly connected digraph $\mathcal{G}$ is the maximum distance between two nodes.

Let us now consider a SCADA system as a cyber-physical system whose automatic control layer is such that the presence of several distributed MTUs allows to enforce *closed-loop load balancing*, i.e., to distribute traffic among the different MTUs in order to avoid congestion and ensure that the total demand at the RTUs is satisfied. It is possible to model the Multi-MTU Plane of such a cyber-physical system (shown in Fig. 1) as a weighted static digraph $\mathcal{G}$, where the MTUs are identified as nodes, and the transmission links connecting them as edges.

An instance of the Wardrop load balancing game taken into account in this work is given by $\Gamma = (\mathcal{G}, \mathcal{L})$, namely composed of:

- the finite weighted static digraph $\mathcal{G}$ defined above, which is assumed to be strongly connected; and
- a family of non-negative *cost functions* $\mathcal{L} \coloneqq (l)_{m \in \mathcal{V}}$, denoting the current *latency* experienced the corresponding MTU.

The total demand load associated with the underlying RTU Plane and impacting on the MTUs composing the digraph $\mathcal{G}$ is denoted by λ.

As anticipated above, this paper further develops a well-known model for selfish routing [27], where an infinite population of agents carries an infinitesimal amount of load each, following the previous works in the domain of telecommunication networks [28]-[30]. In the considered scenario, a single request of the flow is approximately considered as an *agent*: in fact, even if the number of requests is finite, if the flow rates are sufficiently high, the population acceptably approximates the infinite population constraint required by Wardrop theory

Let us consider the set $\mathcal{V}$ of distributed MTUs. At a given time $t \geq 0$, each MTU $m \in \mathcal{V}$ serves a traffic load $x_m(t) \in \mathbb{R}_{\geq 0}$, which, in the considered domain, can be assumed to be measured in MBps. The flow vector $\boldsymbol{x}(t) = [x_m(t)]^T_{m \in \mathcal{V}}$ represents the traffic load served by the Multi-MTU Plane, at a given time $t \geq 0$. The initial flow vector at time $t = 0$ is indicated as $\boldsymbol{x_0} = \boldsymbol{x}(0)$. The main role of the distributed MTUs is to properly manage the overall RTU Plane traffic load λ and ensure the resilience of the considered cyber-physical system against malicious attacks (e.g., inducing failure of one or some MTUs) that may be responsible for undesirable traffic congestion. At a given time $t \geq 0$, a flow vector is feasible if the sum of the traffic loads served by the distributed MTUs is equal to the total power demand load, λ:

$$\sum_{m\in\mathcal{V}} x_m(t) = \lambda, \forall t \geq 0. \quad (1)$$

Each distributed MTU responds, to the amount of traffic load $x_m(t)$ that it is currently serving, with a nonnegative cost function l_m that depends on the value of $x_m(t)$ and denotes the current latency experienced by the MTU m itself. Hence, each distributed MTU $m \in \mathcal{V}$ has a cost function $l_m(x)$: $\mathbb{R}_{\geq 0} \to \mathbb{R}_{\geq 0}$ that maps the traffic load $x_m(t)$ to the cost that the considered MTU incurs by serving an amount of traffic load equal to $x_m(t)$.

Assumption 1. Analogously to [31], we assume the following properties to characterize the cost function $l_m(x), \forall m \in \mathcal{V}$:

1. $l_m(0) = 0$;
2. $l_m(x)$ is non-decreasing. ■

In this work, for the sake of simplicity, for $l_m(x), \forall m \in \mathcal{V}$, we choose to resort to a cost function exhibiting a *piecewise-linear + divergent-exponential* structure, which satisfies Assumption 1, as further detailed in Section III.

In particular, the distributed MTUs can exchange traffic loads with each other in order to jointly minimize their cost functions. As not all the MTUs are neighbors, then, due to network constraints, there obviously could not exist a direct transmission link (m, m') between a couple of MTUs $m, m' \in \mathcal{V}$. However, in our scenario, each couple of MTUs $m, m' \in \mathcal{V}$ is connected, meaning that, even if they are not neighbors, there exist $v \geq 1$ MTUs $m_j \in \mathcal{V}, j \in \{1,2, \dots, v\}$ such that the $v+1$ couples of MTUs $\langle m, m_1\rangle$, $\langle m_1, m_2\rangle$, ..., $\langle m_v, m\rangle$ are all neighbors. The sequence of MTUs $\langle m, m_1, \dots, m_v, m'\rangle$ is therefore a path connecting MTU m to MTU m'. All in all, the graph adjacency matrix $\mathcal{A} = \{a_{m,m'}\}_{m,m'\in\mathcal{V}}$ gives an overview of how the distributed MTUs can interact with each other. The generic element $a_{m,m'}$ represents the maximum rate at which MTU m can exchange a unitary amount of traffic load with MTU m'.

B. System Dynamics

In the presented scenario, the distributed MTUs' main objective is to cooperate with the aim of minimizing the cost associated with each MTU, while serving the corresponding amount of traffic load. This means that, at time $t \geq 0$, each distributed MTU $m \in \mathcal{V}$ migrates a certain amount of traffic load to another distributed MTU $m' \in \mathcal{V}$ in the considered cyber-physical system if $l_m(x_m(t)) > l_{m'}(x_{m'}(t))$. As a result, the system dynamics is determined based on the algorithm proposed in [32]. Hence, the differential equation describing the dynamic evolution of the traffic load served by MTU $m \in \mathcal{V}$ is

$$\dot{x}_m(t) = \sum_{m'\in\mathcal{V}} \left(a_{m',m} r_{m',m}(t) - a_{m,m'} r_{m,m'}(t)\right). \quad (2)$$

In particular, with respect to (2), the *migration ratio* $r_{m,m'}$ between two distributed MTUs $m, m' \in \mathcal{V}$ is defined as:

$$r_{m,m'}(t) = x_m(t) \cdot \mu_{m,m'}(\boldsymbol{x}) = x_m(t) \cdot \mu\left(l_m(x_m), l_{m'}(x_{m'})\right), \quad (3)$$

where $\mu(l_m, l_{m'})$: $\mathbb{R}_{\geq 0} \times \mathbb{R}_{\geq 0} \to [0,1]$ is the *migration policy function*, i.e., a function determining the amount of traffic load assigned to MTU m that is migrated to MTU m'. A commonly used migration policy is the *linear migration policy*, defined as

$$\mu(l_m, l_{m'}) = \max\left\{0, \frac{l_m - l_{m'}}{\Delta l_{max}}\right\}, \quad (4)$$

where $\Delta l_{max} = \max_{m\in\mathcal{V}} l_m - \min_{m'\in\mathcal{V}} l_{m'}$. The *migration policy set*, denoted with Ξ, is given by the set of migration policy functions associated to each couple of MTUs $m, m' \in \mathcal{V}$. If the system starts from a feasible flow vector $\boldsymbol{x_0}$, it evolves always in feasible flow vectors; indeed, the system dynamics defined in (2) has the following property:

$$\sum_{m\in\mathcal{V}} \dot{x}_m(t) = \sum_{m\in\mathcal{V}} \sum_{m'\in\mathcal{V}} (a_{m',m} r_{m',m} - a_{m,m'} r_{m,m'}) = \sum_{m\in\mathcal{V}} \sum_{m'\in\mathcal{V}} a_{m',m} r_{m',m} - \sum_{m\in\mathcal{V}} \sum_{m'\in\mathcal{V}} a_{m,m'} r_{m,m'} = 0,$$

and, therefore,

$$\sum_{m\in\mathcal{V}} x_m(t) = \sum_{m\in\mathcal{V}} x_m(0) = \lambda, \forall t \geq 0.$$

C. Wardrop Equilibrium

The objective of the system dynamics defined in (2) is the convergence towards *stable* flow vectors; a flow vector is stable when no fraction of the agents' demand can decrease the overall cost by moving unilaterally from one MTU to another. It is easy to see that this implies that all MTUs must offer the minimal cost: this condition can be defined as *Wardrop equilibrium*.

Definition 1 (*Wardrop Equilibrium*). A feasible flow vector $\boldsymbol{x} = [x_m(t)]^T_{m\in\mathcal{V}}$ is at a Wardrop equilibrium if, for every couple of distributed MTUs $m, m' \in \mathcal{V}$, with $x_m > 0$, $l_m(x_m) \leq l_{m'}(x_{m'})$ holds. ■

For practical reasons, it is not necessary to wait until the system dynamics achieves a Wardrop equilibrium. The evolution of the system dynamics can terminate whenever the maximum variation $\delta(t)$ between the costs associated with the distributed MTUs is below an acceptable tolerance δ_{max}, i.e., the convergence time, denoted with t^*, is the first time instant when the following inequality is met:

$$\delta(t) = \max_{m\in\mathcal{V}} l_m(x_m(t)) - \min_{m\in\mathcal{V}} l_m\left(x_m(t)\right) \leq \delta_{max}.$$

D. Distributed Load Balancing Problem

Definition 2 (*Distributed load balancing problem*). Given a set $\mathcal{V}$ of distributed MTUs, a total power demand λ, a set $\mathcal{L}$ of cost functions denoting the cost functions of the MTUs, an

initial flow vector $\boldsymbol{x_0} = [x_m(0)]^T_{m\in\mathcal{V}}$, a strongly connected adjacency matrix $\mathcal{A} = \{a_{m,m'}\}_{m,m'\in\mathcal{V}}$, a migration policy set $\Xi = \{\mu(l_m, l_{m'})\}_{m,m'\in\mathcal{V}}$ and a tolerance $\delta_{max} > 0$, the distributed load balancing problem Π is the tuple $\Pi = \langle \mathcal{V}, \lambda, \mathcal{L}, \boldsymbol{x_0}, \mathcal{A}, \Xi, \delta_{max}\rangle$ controlled by the system dynamics defined in (2). ■

Theorem 1. Given a distributed load balancing problem $\Pi = \langle V, \lambda, \mathcal{L}, \boldsymbol{x_0}, \mathcal{A}, \Xi, \delta_{max}\rangle$ *controlled by the system dynamics defined in (2), where:*

a. $\mathcal{V}$ *is the set of distributed MTUs with* $|\mathcal{V}| = n > 1$;
b. $\lambda > 0$;
c. $\mathcal{L}$ *is a set of cost functions associated with the MTUs, satisfying Assumption 1;*
d. $\boldsymbol{x_0}$ *is a feasible flow vector;*
e. $\mathcal{A}$ *is a strongly connected adjacency matrix;*
f. Ξ *is a set of linear migration policy functions;*
g. $\delta_{max} > 0$.

The dynamics (2) characterizing problem Π *admits a solution. More specifically, (i) the distributed load balancing problem* Π *converges towards a unique feasible flow vector* $\boldsymbol{x}^*$ *that is at a Wardrop equilibrium, and (ii) at the Wardrop equilibrium all the utilization factors are equal and minimal, that is,* $l_m(x_m^*) := l_{WE} > 0, \forall m \in \mathcal{V}$ *and, consequently, the tolerance* $\delta(t^*) = 0$. *This means that there exists a time* $\bar{t} \in [0, \infty)$ *such that* $\delta(\bar{t}) \leq \delta_{max}$. ■

Sketch of proof. Given the system dynamics defined in (2) and the migration ratio defined in (3), by enumerating the distributed MTUs in $\mathcal{V}$ from 1 to n, we can write

$$\dot{x}_m(t) = \sum_{m'=1}^{n} \left(a_{m',m} x_{m'}(t) \mu_{m',m}\big(\boldsymbol{x}(t)\big) - a_{m,m'} x_m(t) \mu_{m,m'}\big(\boldsymbol{x}(t)\big) \right).$$

By defining

$$h_{m,m'}\big(\boldsymbol{x}(t)\big) = a_{m,m'} \mu_{m,m'}\big(\boldsymbol{x}(t)\big),$$

it follows that

$$\dot{x}_m(t) = \sum_{m'=1}^{n} x_{m'}(t) h_{m',m}\big(\boldsymbol{x}(t)\big) - x_m(t) \sum_{m'=1}^{n} h_{m,m'}\big(\boldsymbol{x}(t)\big),$$

that is,

$$\dot{\boldsymbol{x}}(t) = \begin{bmatrix} -\sum_{m'=2}^{n} h_{1,m'}(\boldsymbol{x}(t)) & h_{1,2}(\boldsymbol{x}(t)) & \dots & h_{1,n}(\boldsymbol{x}(t)) \\ h_{2,1}(\boldsymbol{x}(t)) & \sum_{m'=1,m'\neq 2}^{n} h_{2,m'}(\boldsymbol{x}(t)) & \vdots & h_{2,n}(\boldsymbol{x}(t)) \\ \vdots & \vdots & \vdots & \vdots \\ h_{n,1}(\boldsymbol{x}(t)) & h_{n,2}(\boldsymbol{x}(t)) & \dots & -\sum_{m'=1}^{n-1} h_{n,m'}(\boldsymbol{x}(t)) \end{bmatrix} \boldsymbol{x}(t).$$

The system can be rewritten in compact form as

$$\dot{\boldsymbol{x}}(t) = \phi\big(\boldsymbol{x}(t)\big)\boldsymbol{x}(t) := f\big(\boldsymbol{x}(t)\big), \quad \boldsymbol{x}(0) = \boldsymbol{x}_0.$$

We therefore obtain a nonlinear autonomous dynamical system. In particular, $f\big(\boldsymbol{x}(t)\big)$ satisfies the standard conditions for the global existence and uniqueness of a solution [33] since $f\big(\boldsymbol{x}(t)\big)$ is Lipschitz-continuous with respect to $\boldsymbol{x}(t)$ and t.

Moreover, from assumption c., the cost function $l_m(x_m)$ has the following properties, i.e., $\forall m \in \mathcal{V}$:

- $l_m(0) = 0$;
- $l_m(x_m)$ is strictly increasing.

The proof then follows immediately from the proof of Theorem 1 in [30], which demonstrates the convergence to Wardrop equilibria in the more general case of time-varying graphs. As in this paper the considered cost functions are strictly increasing, from [32] it follows that the Wardrop equilibrium is unique.

E. MTU Failure and Wardrop Equilibrium Recovery

Once a Wardrop equilibrium condition is achieved, it may happen that one of the MTUs characterizing the considered cyber-physical system fails, thus triggering an undesired perturbation onto the overall traffic load distribution. Such an event of *MTU failure* may be due to a cyber-physical attack that is specifically struck against a single MTU in order to knock it out (e.g., a Denial of Service attack originated by a Sybil attack [34]).

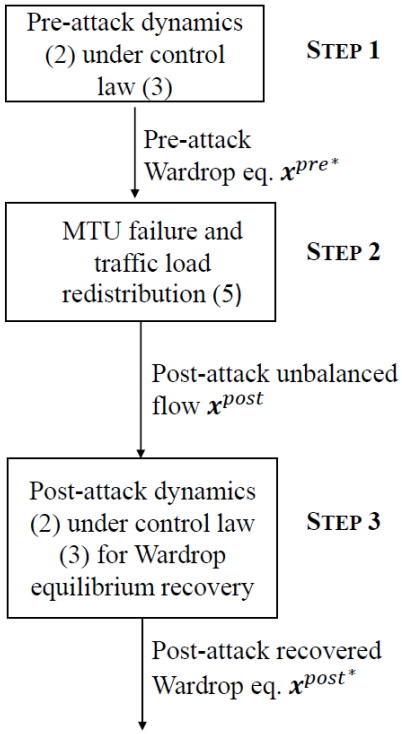

Figure 2. Workflow of the proposed strategy for Wardrop equilibrium recovery after MTU failure.

Therefore, it is necessary to develop strategies that, in case of an MTU failure event, ensure the cyber-physical system resilience by (i) *redistributing* the overall traffic load as a result of MTU failure, and (ii) *recovering* a Wardrop equilibrium condition in a reasonable amount of time.

One particular issue to deal with is that, when an MTU m fails, the load x_m^{pre} it served before failure must be immediately redistributed among the failing MTU's neighbors. One possible approach could consist in loading one randomly chosen MTU m' among the neighbors of m with x_m^{pre} so that the load to be served by m' after the attack is $x_{m'}^{post} = x_{m'}^{pre} + x_m^{pre}$, but such a recovery strategy risks overloading m' while leaving the other neighbors of m unaffected. Instead, we propose to equally distribute x_m^{pre} among all neighbours of MTU m, so that

$$x_{m'}^{post} = x_{m'}^{pre} + \frac{x_m^{pre}}{|\mathcal{N}_m|}, \forall m' \in \mathcal{N}_m, \quad (5)$$

yielding an equal redistribution of the overall traffic load after the attack.

All in all, assuming that only one MTU at a time may fail, we identify three steps as shown in Fig. 2:

- **Step 1.** *Pre-attack* Wardrop equilibrium achievement for the flow vector $\boldsymbol{x}^{pre}(t) = \left[x_m^{pre}(t)\right]_{m\in\mathcal{V}}^T$ subject to the dynamics (2) under the control law (3);
- **Step 2.** Cyber-physical attack inducing the failure of a single MTU;
- **Step 3.** *Post-attack* Wardrop equilibrium recovery for the flow vector $\boldsymbol{x}^{post}(t) = \left[x_m^{post}(t)\right]_{m\in\mathcal{V}}^T$ subject to the dynamics (2) under the control law (3), after applying the traffic load redistribution policy (5).

We assume the event of MTU failure to be instantaneous; moreover, it is interesting to assess how long it takes to recover the Wardrop equilibrium after the attack and determine the relationship between such recovery time and the number of available MTUs, as pointed out in Section III with respect to selected network topologies for the Multi-MTU Plane.

III. Numerical Simulations

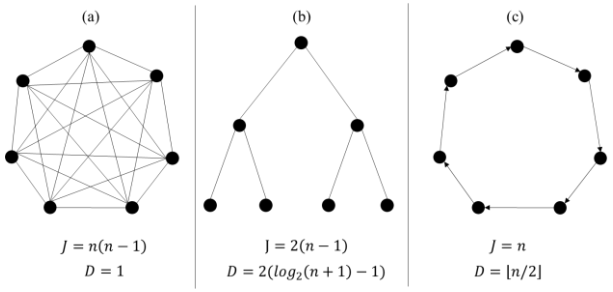

Figure 3. SCADA multi-RTU network topologies: (a) undirected full-mesh; (b) undirected binary tree; (c) directed token-ring. Each topology reports the number of directed links J and its diameter D.

To assess the performance of the proposed solution, the authors carried out simulations for different SCADA multi-MTU problems $\Pi = \langle \mathcal{V}, \lambda, \mathcal{L}, \boldsymbol{x_0}, \mathcal{A}, \Xi, \delta_{max} \rangle$ characterized by the system dynamics defined in (2). Three multi-RTU network topologies have been considered: (a) undirected full-mesh; (b) undirected binary tree; (c) directed token-ring, as shown in Fig. 3.

For each topology an increasing number of nodes $|\mathcal{V}| \in \{7, 15, 31, 63\}$ and a tolerance value $\delta_{max} = 10^{-3}\ s$ have been considered. Since the MTUs' latency functions vary depending on the MTU equipment, we considered three different types of machines having 1, 2 and 4 cores. Each core can process up to B_{max} data per second. In all the simulations, the overall RTUs' bandwidth λ counts $n_{core} \cdot B_{max}$ Mb/s to be distributed among the MTUs, being n_{core} the total number of cores. Table 1 shows the number of MTUs having 1, 2 or 4 cores and the overall bandwidth λ, considering $B_{max} = 8\ MBs$.

TABLE I. Number of MTUs, Cores and bandwidth λ

# MTU	**# CORE**			$\boldsymbol{n_{core}}$	$\boldsymbol{\lambda}$ [$\boldsymbol{Mb/s}$]
	1	**2**	**4**		
7	2	4	1	**14**	**112**
15	4	8	3	**32**	**256**
31	8	16	7	**68**	**544**
63	16	32	15	**140**	**1120**

The set $\mathcal{L}$ is given by 3 piecewise-linear + divergent-exponential cost functions having $n_c \in \{1,2,4\}$:

$$l(x) = \begin{cases} x/(n_c B_{max}) & 0 \le x \le n_c B_{max} \\ e^{(x - n_c B_{max})} & x > n_c B_{max}. \end{cases}$$

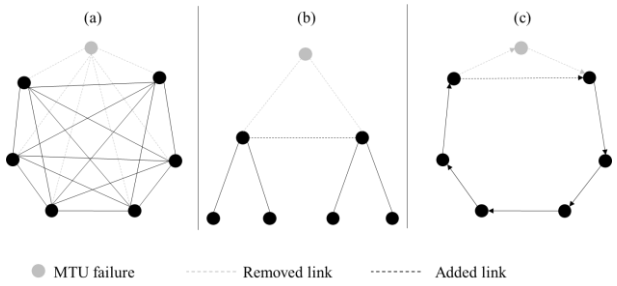

Figure 4. Recovery from an MTU failure in different network topologies: (a) undirected full-mesh; (b) undirected binary tree; (c) directed token-ring.

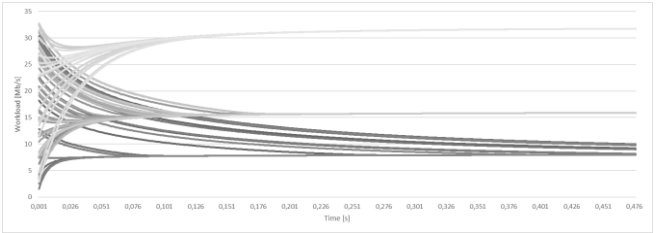

Figure 5. Workload dynamics for the three groups of MTUs.

The set Ξ uses the linear migration policy function specified in equation (4). In each simulation, we consider the scenario of recovery in case of a 4-core MTU failure.

As shown in Fig. 4, once an MTU failure event occurs, the MTUs' network is reconfigured, adding the links needed to maintain the topology: (a) undirected full-mesh; (b) undirected binary tree; (c) directed token-ring. The workload associated with the failed MTU is equally redistributed among its neighbors, leading to an unstable state from which the system dynamic evolves toward another Wardrop equilibrium. In our simulations, we consider negligible the time needed to reconfigure the topology and to reallocate the workload to the remaining MTUs.

To show how the proposed control law converges to a balanced solution, we considered an undirected full mesh topology with $|\mathcal{V}| = 63$ nodes, namely having (according to Table I) 16 MTU with 1 core, 32 MTU with 2 cores and 15 MTU with 4 cores. The simulation of the MTUs' dynamics shows that the MTUs' load dynamics converges exponentially to three different steady-state values (approximately 8.5, 15.9 and 31.7 Mb/s for each MTU having 1, 2 and 4 cores, respectively; see Fig. 5).

To show how the proposed control law ensures the convergence to a balanced solution, once an MTU failure event occurs, we considered the aforementioned three topologies with an increasing number of MTUs $|\mathcal{V}| \in \{7, 15, 31, 63\}$ and a tolerance value $\delta_{max} = 10^{-3}\ s$. The recovery time to a Wardrop equilibrium is reported in the following table.

TABLE II. RECOVERY TIMES FROM A MTU FAILURE

# *MTU* (before failure)	*Recovery time by topology* [*s*]		
	a*) *full-mesh	***b*) *binary tree***	***c*) *token ring***
7	8.1	63.3	111.3
15	5.6	225.7	475.7
31	3.9	1044.5	1684.5
63	2.3	1769.4	3253.2

The simulation results in Table II show that the convergence time depends on the number of interconnections between the distributed MTUs. In the undirected full-mesh topology (a), when the number $|\mathcal{V}|$ of MTUs increases, the recovery time decreases. In the undirected balanced binary tree topology (b), the simulations show that, when $|\mathcal{V}|$ increases, the recovery time increases rapidly. In the directed token ring topology (c), when $|\mathcal{V}|$ increases, the recovery time increases exponentially. Topologies (a) and (b) are representatives of full connected and hierarchical networks (e.g., IEEE 802.3 based protocols), while topology (c) is representative of token-ring networks (e.g., IEEE 802.5). Finally, we developed a web based interface [35] that can be easily set up to replicate the above-described simulation scenarios.

IV. CONCLUSION

The paper proposes a distributed control law to efficiently handle the load balancing problem in multi-MTU SCADA systems, with the aim (i) to minimize the overall latencies experienced by the MTUs, and (ii) to enforce a recovery strategy for preserving traffic load stability in case of the event of failure of an MTU (e.g., due to a cyber-physical attack). The paper shows that the presented control law, under proper assumptions, ensures the convergence to a Wardrop equilibrium. In particular, the simulation results show that the Wardrop equilibrium recovery time after MTU failure depends on the number of interactions and on the network diameter. Moreover, the numerical simulations pave the way for undertaking further studies – e.g., demonstrating the convergence velocity (in comparison with [36]), and improving the proposed control law in order to deal with time-varying graph topologies and to ensure its robustness with respect to the presence of time delays impacting on the measurement of the MTU latencies.

ACKNOWLEDGMENT

The authors wish to thank Dr. A. Pietrabissa for the fruitful discussions and comments on the paper's content. The authors also gratefully acknowledge the members of the ATENA project and, in particular, the ATENA participants from the Consortium for Research in Automation and Telecommunications (CRAT), Rome, Italy.

REFERENCES

[1] Pasqualetti, F., Dörfler, F., Bullo, F. "Control-theoretic methods for cyberphysical security: Geometric principles for optimal cross-layer resilient control systems," *IEEE Control Systems*, vol. 35, no. 1, pp. 110-127, 2015.

[2] Y. Mo and B. Sinopoli, "On the Performance Degradation of Cyber-Physical Systems Under Stealthy Integrity Attacks," *IEEE Transactions on Automatic Control*, 61(9), 2618-2624, 2016.

[3] P. Capodieci, R. Setola, F. Delli Priscoli, M. Castrucci, V. Suraci et al., "Improving Resilience of Interdependent Critical Infrastructures via on-line Alerting System," *Complexity in Engineering Conf. (Compeng 2010)*, Rome, pp. 88-90, December 2010.

[4] S. Canale, F. Delli Priscoli, A. Di Giorgio, A. Lanna, A. Mercurio, M. Panfili, V. Suraci, "Resilient Planning of PowerLine Communications Networks Over Medium Voltage Distribution Grids," *20th Mediterranean Conference on Control and Automation (MED12)*, Barcelona (Spain), July 2012, pp. 710-715.

[5] F. Delli Priscoli, A. Fiaschetti, V. Suraci, "The SHIELD Framework: how to control Security, Privacy and Dependability in Complex Systems," *2012 IEEE Workshop on Complexity in Engineering*, Doi: 2-s2.0-84866534292.

[6] S. Amini, F. Pasqualetti, and H. Mohsenian-Rad, "Dynamic Load Altering Attacks against Power System Stability: Attack Models and Protection Designs," *IEEE Trans. on Smart Grid*, in press, 2016.

[7] V.L. Do, L. Fillatre, I. Nikiforov, and P. Willett, "Security of SCADA systems against cyber–physical attacks," *IEEE Aerospace and Electronic Systems Magazine*, vol. 32, no. 5, pp. 28-45, May 2017.

[8] S. Misbahuddin, "Fault tolerant remote terminal units (RTUs) in SCADA systems," in *Proceedings of the 2010 International Symposium on Collaborative Technologies and Systems*, Chicago, IL, pp. 440-446, 2010.

[9] R. Kumar and M.L. Dewal, "Multi-Supervisory Control and Data Display," *International Journal of Computer Applications*, vol. 2, no. 1, pp.1-5, 2010.

[10] R. Pecori, "S-Kademlia: A trust and reputation method to mitigate a Sybil attack in Kademlia," *Computer Networks*, 94, pp. 205-218, 2016, doi:10.1016/j.comnet.2015.11.010

[11] S.U. Khan and I. Ahmad, "A Cooperative Game Theoretical Technique for Joint Optimization of Energy Consumption and Response Time in Computational Grids," *IEEE Trans. Parallel Distrib. Syst.*, vol. 20, no. 3, pp. 346–360, Mar. 2009.

[12] D. Grosu and A.T. Chronopoulos, "Noncooperative load balancing in distributed systems," *J. Parallel Distrib. Comput.*, vol. 65, no. 9, pp. 1022–1034, Sep. 2005.

[13] E. Even-Dar and Y. Mansour, "Fast convergence of selfish rerouting," in *16th annual ACM-SIAM symposium on Discrete algorithms, Society for Industrial and Applied Mathematics*, 2005, pp. 772–781.

[14] S. Shah and R. Kothari, "Convergence of the dynamic load balancing problem to Nash equilibrium using distributed local interactions," *Inf. Sci. (Ny).*, vol. 221, pp. 297–305, Feb. 2013.

[15] A. Di Giorgio, F. Liberati, R. Germanà, M. Presciuttini, L. Ricciardi Celsi, and F. Delli Priscoli, "On the Control of Energy Storage Systems for Electric Vehicles Fast Charging in Service Areas," in *Proceedings of the 24th Mediterranean Conference on Control and Automation (MED 2016)*, pp. 955-960, Doi: 10.1109/MED.2016.7535947.

[16] V. Suraci, L. Ricciardi Celsi, A. Giuseppi, A. Di Giorgio, "A distributed Wardrop control algorithm for load balancing in smart grids," in *Proceedings of the 25th Mediterranean Conference on Control and Automation (MED 2017)*, pp. 761-767, Doi: 10.1109/MED.2017.7984210.

[17] F. Delli Priscoli, A. Isidori, "A Control-Engineering Approach to Integrated Congestion Control and Scheduling in Wireless Local Area Networks," *Control Engineering Practice*, IFAC (Great Britain), vol. 13, no. 5, pp. 541-558, May 2005.

[18] S. Canale, F. Delli Priscoli, S. Monaco, L. Palagi, V. Suraci, "A reinforcement learning approach for QoS/QoE model identification," *Chinese Control Conference (CCC15)*, pp. 2019-2023, 2015, doi:10.1109/ChiCC.2015.7259941.

[19] S. Battilotti, F. Delli Priscoli, C. Gori Giorgi, M. Panfili, A. Pietrabissa, L. Ricciardi Celsi, and V. Suraci, "A Multi-Agent Reinforcement Learning Based Approach to Quality of Experience Control in Future Internet Networks," in *34th IEEE Chinese Control Conference (CCC2015)*, 2015, pp. 6495–6500, Doi: 10.1109/ChiCC.2015.7260662.

[20] L. Ricciardi Celsi, S. Battilotti, F. Cimorelli, C. Gori Giorgi, S. Monaco, M. Panfili, V. Suraci, and F. Delli Priscoli, "A Q-Learning based approach to Quality of Experience control in cognitive Future Internet networks," in *2015 23rd Mediterranean Conference on Control and Automation (MED)*, 2015, pp. 1045–1052, Doi: 10.1109/MED.2015.7158895.

[21] F. Delli Priscoli, A. Di Giorgio, F. Lisi, S. Monaco, A. Pietrabissa, L. Ricciardi Celsi, V. Suraci, "Multi-Agent Quality of Experience Control," *International Journal of Control, Automation, and Systems*, vol. 15, no. 2, pp. 892-904, 2017, Doi: 10.1007/s12555-015-0465-5.

[22] S. Canale, A. Di Giorgio, F. Lisi, M. Panfili, L. Ricciardi Celsi, V. Suraci, and F. Delli Priscoli, "A Future Internet Oriented User Centric Extended Intelligent Transportation System," in *Proceedings of the 24th Mediterranean Conference on Control and Automation (MED 2016)*, pp. 1133-1139, Doi: 10.1109/MED.2016.7535967.

[23] L. Ricciardi Celsi, A. Di Giorgio, R. Gambuti, A. Tortorelli, F. Delli Priscoli, "On the many-to-many carpooling problem in the context of multi-modal trip planning," in *Proceedings of the 25th Mediterranean Conference on Control and Automation (MED 2017)*, pp. 303-309, Doi: 10.1109/MED.2017.7984135.

[24] H. Ackermann, S. Fischer, M. Hoefer, and M. Schöngens, "Distributed algorithms for QoS load balancing," *Distrib. Comput.*, vol. 23, no. 5–6, pp. 321–330, Dec. 2010.

[25] J.G. Wardrop, "Some Theoretical Aspects of Road Traffic Research," *ICE Proc. Eng. Div.*, vol. 1, no. 3, pp. 325–362, Jan. 1952.

[26] H. Kameda, J. Li, C. Kim, and Y. Zhang, *Optimal Load Balancing in Distributed Computer Systems*. London: Springer London, 1997.

[27] S. Fischer, H. Räcke, and B. Vöcking, "Fast Convergence to Wardrop Equilibria by Adaptive Sampling Methods," *SIAM J. Comput.*, vol. 39, no. 8, pp. 3700–3735, Jan. 2010.

[28] G. Oddi, A. Pietrabissa, "A distributed multipath algorithm for wireless ad - hoc networks based on Wardrop routing", *Proc. 21st Mediterranean Conference on Control and Automation (MED 2013)*, June 25-28, 2013, Platanias-Chania, Crete, Greece, pp. 930-935, doi: 10.1109/MED.2013.6608833

[29] F. Cimorelli, F. Delli Priscoli, A. Pietrabissa, L. Ricciardi Celsi, V. Suraci, and L. Zuccaro, "A Distributed Load Balancing Algorithm for the Control Plane in Software Defined Networking," in *Proceedings of the 24th Mediterranean Conference on Control and Automation (MED 2016)*, pp. 1033-1040, June 21-24, 2016, Athens, Greece, DOI: 10.1109/MED.2016.7535946.

[30] A. Pietrabissa and V. Suraci, "Wardrop Equilibrium on Time-Varying Graphs," *Automatica* (Elsevier, Great Britain), Vol. 84, 2017, pp. 159-165, DOI: 10.1016/j.automatica.2017.07.021

[31] V. Suraci, C. Gori Giorgi, S. Battilotti, F. Facchinei, "Distributed workload control for federated service discovery," *Procedia Computer Science*, vol. 56, no. 1, pp. 233-241, 2015, Doi: 10.1016/j.procs.2015.07.221.

[32] S. Fischer, B. Vöcking, "Adaptive routing with stale information," *Theoretical Computer Science*, vol. 410, no. 36, 2009, pp. 3357-3371.

[33] H. K. Khalil, *Nonlinear Systems*, Third Edition, Pearson, 2001.

[34] R. Pecori, L. Veltri, "Trust-based routing for Kademlia in a Sybil scenario," *22nd International Conference on Software, Telecommunications and Computer Networks, SoftCOM* 2014, art. no. 7039131, pp. 279-283, 2014, doi: 10.1109/SOFTCOM.2014.7039131

[35] Web based interface used to set up the numerical simulations: http://www.icaruservices.it/wardrop/web/wardrop.php?sim=scada

[36] P. Berenbrink, M. Hoefer, T. Sauerwald, "Distributed Selfish Load Balancing on Networks," *ACM Transactions on Algorithms*, 2014.