Noname manuscript No.
(will be inserted by the editor)

Robust QoS-aware Communication in the Smart Distribution Grid

Kubilay Demir, Daniel Germanus and Neeraj Suri

Received: date / Accepted: date

Abstract The increasing penetration of distributed generation into the power distribution domain necessitates reliable and QoS-aware communication in order to safely manage the grid. To achieve this, heterogeneous networks (a combination of the Internet and private networks) offer a promising approach due to the potential cost effectiveness and leveraging the ubiquitous coverage. However, the current Internet infrastructure does not support end-to-end (E2E) QoS-guaranteed communication. To cope with this challenge, we propose a novel overlay network architecture, termed **HetGrid**, with a dedicated QoS routing mechanism. It provides QoS guarantees across the network, taking into account three parameters: reliability, latency and bandwidth for power distribution grid applications. To achieve this, we also develop two elements, namely (a) multipath routing mechanism compensating the critical applications for their high reliability requirements by employing E2E physically-disjoint paths, and (b) altruistic resource allocation with the QoS routing mechanism targeting QoS-guaranteed communication for applications having strict QoS requirements. Our results demonstrate that the proposed overlay network approach provides highly efficient, reliable and QoS-aware communication in heterogeneous networks.

Keywords Overlay Networks · Smart Grid · Robustness · QoS

K. Demir
Hochschulstr. 10, Piloty Bldg, DE 64289 Darmstadt, Germany
E-mail: kubidem@cs.tu-darmstadt.com

D. Germanus
E-mail: daniel.germanus@enx.com

N. Suri
E-mail: suri@cs.tu-darmstadt.de

1 Introduction

The power distribution grid, which typically supports one-way distribution, increasingly needs to also handle bi-directional electricity flows produced by the distributed generation resources. This requires an evolution towards the smart distribution grid (SDG), which typically requires the ability to actively manage both varied loads and varied power sources. This evolution should also address new operational and control issues such as voltage and frequency fluctuation, fault current and unintended islanding/isolation to prevent faulty circuit energization. To achieve this, a variety of distribution automation (DA) applications have been proposed such as fault detection, isolation, and reconfiguration, Volt/VAR control, and adaptive protection among others [1]. The aim of DA applications is real-time handling of altering loads, generation, and failure states of the distribution grid by exploiting real time sub-second measurements.

To support the communication requirements of DA, utilities typically prefer dedicated private E2E communication networks. However, this may not always be accomplished due to cost and technical restrictions. Therefore, the SDG communication network could become a heterogeneous network consisting of multiple private networks and Internet service providers (ISPs). Furthermore, the scale of SDG communication networks might span a territory (e.g., a state or metropolitan area) with millions of nodes. While some SDG communication nodes (e.g., substations) have high computation capacity and multihoming with high outgoing bandwidths, other nodes (e.g., smart meters, sensors and circuit breakers) may only have basic functionalities [2, 3].

Irrespective of the type of DA schema, the common element across them is the need for reliable, timely and responsive communication to facilitate effective sensing and control. Most of these applications have stringent latency (in the range of 100 ms to 5 s) and reliability (99.00%-99.9999%) requirements [3, 4]. Unfortunately, the present Internet infrastructure does not innately provide the necessary QoS guarantees for such safety-critical applications which essentially require both low latency and high reliability. One reason for this deficiency being that the routing among Autonomous Systems (ASes) (typically utilizing BGP:Border Gateway Protocol) on the Internet depends on commercial considerations, resulting from contracts among these ASes. They promote low cost links rather than low latency links, although there are more paths that BGP can accommodate in the Internet infrastructure. In addition, the BGP convergence time (i.e., time needed for all routers to have a consistent view of the network after a failure) might take several or even tens of minutes. This can cause delays or even loss of traffic [5]. Furthermore, in such heterogeneous networks[1], E2E QoS cannot be guaranteed by employing the current underlying QoS approaches (e.g., DiffServ [6], IntServ [7], MPLS [8]), due to administration configuration differences in each domain [2].

To meet the QoS requirements for smart grid applications, multiple approaches have been proposed such as INTEGRIS [9], GridStat [10], and CRUTIAL [11]. While INTEGRIS and GridStat mainly focus on dedicated private networks, CRUTIAL targets reliable communication between control centers and substations (but not all SDG devices) by employing multihoming techniques. In addition to these approaches, overlay networks have emerged as an effective way to improve the performance of real-time Internet applications [12, 13, 14, 15, 16]. The overlay routing solutions use overlay nodes to bypass performance degradation on Internet paths without requiring changes in the underlying network layer. They can provide timely and relatively reliable Internet services. Nevertheless, these works do not target (1) delivery guarantee for each message (high reliability) even in case of permanent underlay failures in addition to (2) application-adaptive and criticality aware resource allocation.

[1] In this work, heterogeneous networks implies a composite of public (on the Internet) or private networks.

Paper contributions

On this background, we propose HetGrid as an overlay based communication infrastructure that provides the following capabilities and contributions:

1. *High reliability in the heterogeneous networks:* HetGrid strives to build physically-disjoint multipaths, and meets the strict QoS requirements of DA applications via a light-weight low-overhead communication architecture. To achieve high reliability, it employs Source Routing-based QoS Routing (SRQR) and Compensative Multi-Routing (CMR) mechanisms.

2. *Application-adaptive and criticality aware resource allocation:* DA applications not only need flow-based (periodic) data acquisition, but also aperiodic data accusation (e.g., alert messages) with diverse QoS requirements. This necessitates a smart resource allocation on the overlay network. Thus, HetGrid employs Altruistic Flow Allocation (AFA) in order to reserve/allocate the "best" paths (in terms of QoS metrics) for high priority (critical) applications in a distributed manner.

Overall, HetGrid's overlay network obtains QoS- satisfied paths for each DA application by using SRQR and AFA on the heterogeneous networks. In addition, CMR strives to maintain the communication at the required latency and reliability level. Our evaluation focuses on QoS-satisfaction of each application with the diverse reliability, latency and bandwidth requirements.

Since TCP provides a reliable connection between end hosts, the current IP-based industrial critical applications typically rely on TCP connections. This is a pragmatic solution and widely used approach in industrial systems if the TCP overhead is small compared to the application payload size. Unfortunately, the typical DA applications message payloads are less than 1000 bytes [21]. Consequently, the TCP's additional overhead (e.g., larger header, session establishment messages etc.) entails an unacceptably large protocol overhead not viable for DA applications. Hence, HetGrid advocates and employs the lower-overhead UDP connection between peers.

We evaluate HetGrid by comparing the direct TCP Vegas[2] [17] connection (between the end hosts) based on the applications' QoS-satisfaction rate. The evaluation is performed in four perturbation scenarios: 1. dynamic link state changes in the underlay network, 2. failure in the underlay routers, 3. heavy congestion in the underlay routers, and 4. bursty traffic on the overlay network. We do note that in existing works, although there are many direct TCP connection and overlay based QoS enhancement comparisons [11, 13, 14], they focus on the performance improvement in terms of

[2] In this paper, TCP is used to refer to TCP Vegas.

latency and loss rate but not delivery guarantee in time for each message (high reliability) in case of large-scale failures.

Paper scope and structure

This paper, utilizing the foundations developed in our preliminary work [18], develops novel mechanisms to provide for the new and composite targets of performance, fault tolerance and efficient E2E communication for DA applications. Our work in [18] mentioned the needs for QoS, multipath routing, and resource allocation mechanisms in basic forms. This paper comprehensively develops these issues to provide enhanced performance and fault tolerance for DA applications. The comprehensive system model (Section 3) along with the software architecture (Section 5) and especially the new mechanisms (Sections 4 & 6) fully detail the developed idea. The paper contains extensive simulation results (Section 7) to include the assessment of (a) the QoS-satisfaction rate of each application, and (b) the fault tolerance to common Internet perturbations (c) network overhead of both approaches. Overall, the proposed approach contributes to (a) a comprehensive discourse on the feasibility of supporting DA on heterogeneous networks via the use of HetGrid, and highlights (b) the impact of path redundancy plus multihoming in the underlay network.

The remainder of the paper is organized as follows. Section 2 introduces QoS requirements and challenges for DA applications communicating over heterogeneous network. Subsequently, Section 3 details the system, traffic and perturbation models followed by Sections 4, 5, and 6, which respectively develop the overlay construction, the SW architecture and routing algorithms. The evaluation is presented in Section 7.

2 QoS requirements and challenges for heterogeneous network-based DA applications

As highlighted in the previous section, E2E ownership of the network for SDG may not always be possible because of cost consideration, spectrum availability etc. While heterogeneous networks are proposed as potential solutions, detailing the challenges that DA applications will encounter is very much an open issue. Before introducing our proposal, the major communication requirements and challenges for DA applications communicating over the heterogeneous networks are discussed in the rest of this section.

E2E latency guarantee: Many types of information delivery between power devices are only meaningful if they arrive within a predefined time frame (i.e.,deadline). Delayed information is of limited value, and in the worst case, damage might occur in the distribution grid. For example, the islanding protection actions must be made within a time window of 150-300 ms [19]. As public network such as the Internet typically provide best-effort services, a time-sensitive applications running on such a best-effort network potentially results in damage to the grid. In case of the usage of public network, the network should be supported by additional measures e.g., multihoming in critical end host.

Reliability: From [20], Smart Grid reliability is defined as the degree to which a communication system must remain operational. The operability of smart grid devices relies on the communication infrastructure in order to maintain the stability of the grid in their respective domains. Hence, the communication infrastructure must be fault-tolerant, especially for safety critical applications, to protect the distribution grid and ensure efficient operation. In particular, the communication reliability in the Internet is affected by a number of possible failures. For example, BGP failure and congestion introduce high reliability risks due to BGPs convergence time and its policy based routing approach. To cope with this, a self-organizing overlay network, supported by multi-homing for critical end points, is a potential alternative to satisfy the communication requirements on the heterogeneous networks.

Furthermore, in cellular networks the failure of core network resources potentially leads to disconnection of many power devices to pose safety risks in the grid. To mitigate this, ad-hoc connections with physically-near devices, which connect to different ISPs, can be provided in order to obtain fault tolerant communication for the critical applications.

Scalability: Due to the continual growth of the SDGs, an *a priori estimation* of the network scale is difficult to ascertain. In addition, the workload of DA applications can increase rapidly depending on conditions such as the weather or the electricity price [21]. As the workload of the network increases, meeting latency and reliability requirements of safety critical applications becomes more challenging. Hence, the communication network for the DA applications should be scalable and adaptive to the changing network dynamics.

End-to-End QoS guarantee: DA applications have diverse QoS requirements. Moreover, some of DA applications may need different priorities for their messages under different conditions depending on the function of that data. For example, periodic metering measurement traffic typically has a lower priority, whereas these

metering measurements may necessitate higher priority when such measurements are required in active demand response applications [2]. Moreover, after a power outage, if a large number of meters must be registered in a short time, the meter registration traffic may be considered higher priority and critical. Hence the need is of a QoS mechanism that discovers the resources across the network and allocates them in a distributed manner depending on the applications' real-time QoS requirements. Moreover, it should not be centralized in order to avoid a single point failure.

3 System Model

We consider that SDG communication nodes (e.g., intelligent electrical devices (IED), substations and control centers of SDG) span a large geographical area and connect to wide area network of the utility via diverse ISPs. Hence, the SDG communication network comprises many Autonomous Systems (AS). In addition, transmission/distribution substations and control centers are multihomed, i.e., multiple ISP connections, and have direct fiber optic links between them. As a result, the SDG communication network is considered as a heterogeneous network. We now progressively present the underlay, and overlay models, the data types and application models that underlie the development of HetGrid.

3.1 Underlay Model

We model the underlay topology, which corresponds to the SDG communication network, as a directed graph $G_u = (V_u, E_u)$ where V_u and E_u are the set of vertices and edges. The vertices refer ASes, or private LANs, and the edges represent the peerings between them. Although there are many internal routers inside an AS and a private LAN, we consider them as underlay nodes to simplify the route calculation between pairs.

3.2 Overlay model

To pave the way for obtaining E2E physically-disjoint paths, containing no common underlay router and overlay node, and QoS-provisioning in a lightweight manner, the bootstrap node, a node in the overlay network that provides initial configuration information to newly joining nodes, clusters these communication nodes depending on their autonomous system (AS) and selects the nodes with the highest computational capacity from each cluster as supernode (SN) (a mater SN and $d-1$ redundant SN, cf. Section 4.1). This results in a two layer overlay for HetGrid as illustrated in Figures 1. We define a primary layer overlay as a directed graph $G_p = (V_p, E_p)$. Vertices refer all overlay nodes (including SNs and normal nodes (NNs), which run on SDG communication nodes (e.g, IEDs)). Edge set E_p represent virtual links between NNs and their SNs (each NN is connected to only SNs in the same cluster).

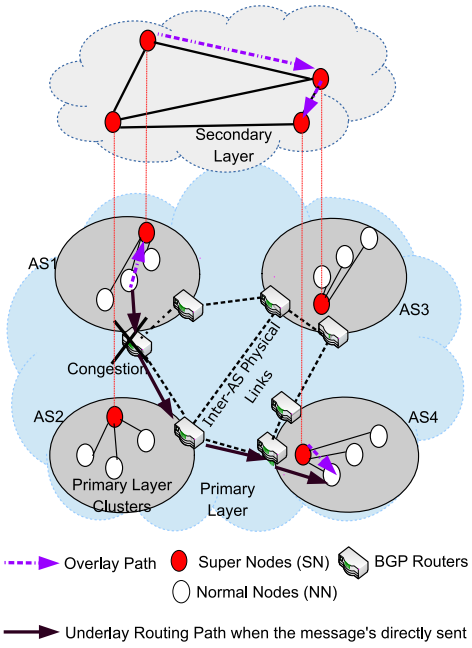

Fig. 1 Basic HetGrid Architecture

A secondary layer is also defined as a directed graph $G_s = (V_s, E_s)$. Vertices in V_s only consist of SNs that participate in both layers, i.e., SN is a gateway, and therefore, $V_s \subset V_p$. If a physical link (the peering) $e_u \in E_u$ exists between two ASes or the private LANs, there exists a secondary layer edge $e_s \in E_s$.

3.3 Data type and delivery model of DA applications

There are three types of data traffic in DA applications: (D1) Sensing traffic, (D2) Control traffic and (D3) Coordination traffic. All data traffic types can be periodic or aperiodic, and their sizes are typically less then 1 Kb [22].

We classify data delivery requirements of DA applications into four different modes: (M1) guarantee, (M2) no-guarantee, (M3) in-time, and (M4) best-effort time. As an example, while a protection application requires delivery in M1 and M3, a video surveillance application can be based on M2 and M3. In all modes, the packets are formed by employing the UDP protocol. In order to

address UDP's reliability shortcomings and guarantee data delivery, we make use of the adaptable Ack mechanism (AAM) in M1. To obtain timely data delivery in M3, a source routing-based QoS routing (SRQR) mechanism is employed considering latency constraints. Furthermore, for an application that needs both M1 and M3, in addition to SRQR, the data is routed over multiple redundant paths to exploit physical path diversity using compensative multipath routing (CMR) mechanism.

We use a priority scale ranging from high to low priority (high, medium, and low priority). We assume that safety or mission critical applications with low latency and high reliability requirements are allocated as a high priority.

3.4 Application model

We consider diverse DA applications to comprehensively evaluate our proposal. Hence, we employ the following application characterizations according to the above data traffic types: we firstly categorize the DA applications into two classes, sensing A_s, and controlling A_c applications. While A_s transmits its data in a periodic manner (flow), A_c delivers data aperiodically (occasional). Furthermore, these applications are assigned to different classes based on their priorities, e.g., A_{sh}, A_{sm}, and A_{sl} and A_{ch}, A_{cm}, and A_{cl}.

3.5 Assumptions

In this work, the link state between two overlay nodes (u, v) is denoted by bandwidth B_{uv}, latency L_{uv}, reliability (simply loss rate) R_{uv}. We assume that each primary layer node p regularly derives its available computation capacity C_p and link state information between itself and its SNs and transmits them to its SNs. On the other hand, each secondary layer node u obtains C_u and its adjacent links' available link state information, and disseminates them to all V_s (SNs). We consider that the bootstrap node broadcasts the updated membership list over the secondary layer, only on change of membership of the clusters. We expect that the overlay network has a low churn rate given the operational characteristics of the SDG communication nodes. Moreover, when a NN sends a packet to its SN in order to deliver it to its destination over QoS-satisfied path(s), the SN employs a Bloom Filter model to find the SN to which the destination node belongs (inspired by [23]). Finally, we assume that each application has a unique ID. For each application ID, priority and QoS requirements information exists in all overlay nodes. The application ID is a part of the packet payload and written by the sending power application.

4 Construction of supernode-based two-layer overlay network

The goals of the HetGrid's overlay network design are twofold: (1) To mitigate the overhead of the QoS routing that probes the underlying network to find paths satisfying the QoS requirements, and (2) To obtain physically disjoint redundant paths for the multipath routing mechanism, which provides fault-tolerant communication for the critical applications.

4.1 Clustering of nodes and SN selection

To mitigate the overhead of the overlay-based link state routing and to improve routing scalability and performance on the overlay network, the bootstrap node clusters nodes depending on their AS, and then selects SNs from each cluster depending on their resources (i.e., computation capacity, outgoing bandwidth, and multihoming). This results in a two layer overlay design. The secondary layer only consists of the SNs, which are interconnected with each other. The primary layer, on the other hand, consists of all NNs and SNs in their respective clusters. Whereas the primary layer clusters are structured using a star topology, secondary layer links are constructed according to the physical links that connect ASes or the private LANs.

In order to cluster nodes according to their AS, we can utilize the approach from Ren [24]. The procedure is based on that: BGP updates can be regularly accessed by the bootstrap node. By using these updates, IP prefix of ASes and the AS-AS connection relationships can be obtained. AS-based clusters are then constructed by the bootstrap node, matching the IP-prefixes of ASes with node IPs.

Moreover, the bootstrap node defines a master SN (mSN) and $d - 1$ redundant SNs (rSN) from the selected SNs for each cluster. The mSN together with the rSNs provide at least d redundant disjoint paths for each pair in the overlay network. Moreover, in case of mSN failures, the rSNs can take over the mSN tasks. This is possible as rSN regularly check the mSN by using heartbeats in addition to periodically synchronize the required data with mSN. The transition, by an overseeing rSN, is accomplished by disseminating a leadership message "I'm the new-mSN" to all overlay nodes of its cluster. This takes less than 10 s in our implementation.

While the selection criteria for mSN is being the "strongest" one in the cluster, the criteria for $d-1$ rSNs are provision of the "highest" path diversity (in terms of underlay routers) between each pair within the cluster in addition to a sufficiently high computation capacity. However, selecting the overlay nodes in a cluster providing physically-disjoint paths between each pair is a difficult task. To cope with this, each peer (including SNs and NNs) runs the traceroute tool towards the others within its cluster to obtain the underlay routers pattern between them. They relay the traceroute data to the mSN, which then heuristically chooses $d-1$ rSN that statistically provide 'the least' correlated paths (in terms of underlay routers patterns) between each pair in their cluster (cf. Han [25]). Since the underlay topology changes only infrequently (months or even longer), this traceroute operation adds only limited additional overhead [25].

4.2 Obtaining disjoint redundant paths

In order to obtain a fault-tolerant communication system for the critical applications, HetGrid aims to determine E2E physically-disjoint redundant paths between each pair (of NNs) by using the constructed overlay network.

The connection between a pair can be intra-AS or inter-AS. Thus, the determination of redundant disjoint paths on the network requires different approaches for each scenario. For intra-AS connections, HetGrid enables NNs to transmit their data through mSN and $d-1$ rSN, providing the "highest" path diversity, to any other NN as explained above. Thus, the NN can send its data, replicated d times, over their respective SNs (1 mSN and $d-1$ rSN) to any other NN in the same AS in order to obtain reliable and timely data delivery guarantees.

In case of inter-AS connections, mSN calculates multiple disjoint paths towards each destination of a given application unlike intra-AS connection which provides adequate path diversity by simply sending the replicated data over their respective SNs. Since the secondary layer is based on physical connectivity of the underlying network, mSN can readily define inter-AS disjoint redundant paths towards any other SN by omitting the path(s) which have the same overlay nodes with already selected path(s). However, some ASes have single upstream (i.e., single BGP router to connect to another AS). This disturbs the E2E path disjointness. To cope with this, mSN takes advantage of multihoming features of its cluster's d SNs to obtain disjoint upstreams for each redundant paths (we assume that SNs have multiple network connections, e.g., different carrier connections in a substation, a meter concentrator etc.). Furthermore, the mSN organizes the d SNs to provide different upstream networks, when multiple disjoint paths towards a destination of an application are defined. Thus, HetGrid ensures E2E physically-disjoint path for the critical applications in the Internet infrastructure.

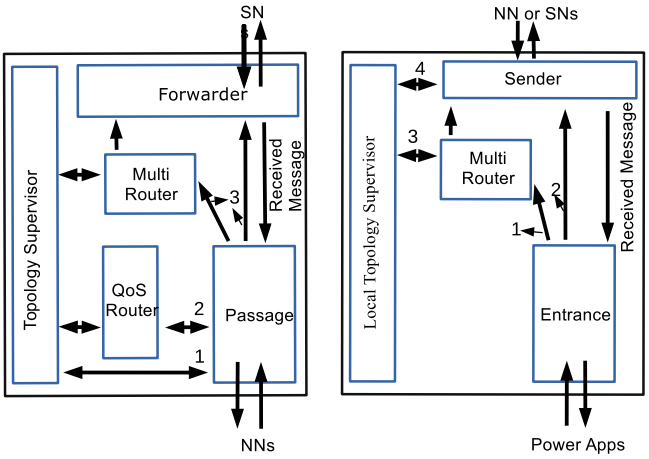

Fig. 2 The architecture of software on a SN and NN, respectively

5 The Software architecture of HetGrid

Figure 2 depicts the conceptual software architecture (stack) for the SN (left side) and the NN (right side). We first detail the NN operations. The *Entrance* component serves as a gateway for exchanging data between power applications and the NN stack. After receiving a packet from a power application, the *Entrance* component determines the priority of the packet by using the application ID. If the packet is of high priority, the *Entrance* relays it to the *Multi Router* (#1 in Figure 2), if not, to the *Sender* (#2). *Multi Router* replicates the packet d times and then hands them over to the *Sender* (#3) to be delivered to d SNs (the details below). On the other hand, *Sender* relays medium and low priority packets depending on their destination domain: whereas packets which are destined to extra-AS are sent to mSN, packets that are destined to intra-AS are directly transmitted to the destination NN[3]. In addition, the *Local Topology Supervisor*, which main-

[3] As Internet service providers (ISP) can assure reconvergence time in the range of a few seconds by employing MPLS within AS, we do need to use any overlay routing inside the cluster. However, for high priority applications, HGN still sends the messages over d SN's that provide disjoint paths over a given AS routers.

tains local network discovery, gives information about the addresses that packets are destined (#4).

Let us assume that a packet destined to an extra-AS is received by a mSN's *Passage* component, which is functioning as a gateway for exchanging packets between ingress SNs and NNs. At the other hand, as mentioned above, intra-AS deliveries are fulfilled either directly (medium or low priority) or over d SNs (high priority).

The *Passage* component first determines the QoS requirements for the packet using the application ID tag. In the next step, the *Passage* component consults the *Topology Supervisor*, which is responsible for network discovery and maintenance, about the destination NN's mSN (#1). Then, the *QoS Router* is queried to find a suitable routing path between itself and the mSN, which has to satisfy the QoS requirements (#2).

If the packet is of high priority, it is first processed by the *Multi Router* before delivering to *Forwarder*. If not, it is handed over to the *Forwarder* (#3) after tagging with the route information. If it is of high priority, which implies $d-1$ rSN also received the replicated packet, *Multi Router* in the mSN identifies SNs (among d SN) which should relay the replicated packet (cf. Section 6.4) and their routes over secondary layer. This information is then transmitted to the defined rSNs. Finally, the defined SN's *Multi Router* emits the packet, tagged with the respective route information, to the *Forwarder*. *Forwarder*'s task is to send the packet to the next address in the packet header irrespective of its priority.

Once the QoS routing path(s) are determined for the destinations of a given application in the ingress mSN, that information can be stored and reused if the application needs a periodic data flow towards the destinations. Hence, packets with already known application IDs can be directly handed over to the *Forwarder*. However, in case of significant network state changes, the *Topology Supervisor* causes a reset of the stored information to allow the system to adapt to the new network state. In addition, all aperiodic packets are simply relayed to d SNs to route over their the "best" path towards the destination, which is reserved (cf. Section 6.3).

6 Routing

The fundamental differences of DA applications from current Internet-based applications are their stringent QoS requirements and needs of timely delivery guarantee for each message (e.g., islanding protection messages). However, the current Internet infrastructure mainly provides a best-effort delivery. Hence, any communication system that is proposed for SDG should 1) provide QoS-satisfied paths for each application and 2) be fault-tolerant to support the timely delivery guarantee for each message of the critical applications by employing multipath routing and smartly allocating the resources. To address these requirements, the following mechanisms are employed on the **secondary layer** overlay network in an application-adaptive manner: HetGrid provides the QoS-satisfied paths for each application by employing a Source Routing-based QoS Routing (SRQR). Furthermore, to obtain timely delivery guarantee for each message of the critical applications, it takes advantage of Compensative Multi-Routing (CMR) in addition to Altruistic Flow Allocation (AFA) mechanism. We introduce these mechanisms and detail how they cooperate in a self-adaptive way.

6.1 Source routing-based QoS routing (SRQR)

SRQR basically takes advantage of the shortest path algorithm to make routing decisions on secondary layer, considering QoS metrics, i.e., reliability, latency and bandwidth. Moreover, SRQR employs *source routing* in order to aid multihop routing by speeding up the transmitting path at overlay nodes. It also helps bind a packet flow to a selected path (barring significant link state changes sensed by the heartbeat mechanism), making performance more predictable, and support for multipath routing in HetGrid. When the strict QoS requirements of DA applications are considered, using the *source routing* to obtain predictable network performance can be an efficient method.

The paths are constructed using the shortest path algorithm with hop normalized path weights for bandwidth, reliability, and latency to result in equation 1 as:

$$PathWeight = \alpha_b \sum_{i=0}^{n} \left(\frac{B_{i,i+1}}{B_{i,i+1} - R_B}\right)/n * \\ *\alpha_r \frac{-\sum_{i=0}^{n} logR_{i,i+1}}{\sum_{i=0}^{n} logR_{i,i+1} - logR_R} * \alpha_l \frac{R_L}{R_L - \sum_{i=0}^{n} L_{i,i+1}} \quad (1)$$

In the equation (1), n is the number of hops in the path. While $B_{i,i+1}$, $R_{i,i+1}$ and $L_{i,i+1}$ are residual bandwidth, current reliability, and latency of the link, R_B, R_R and R_L denote required bandwidth, reliability and latency, respectively. The alpha coefficients enable tuning of influence that the individual components have on the overall path weight.

This formula combines the influence of the multiplicative (reliability), concave (bandwidth) and additive (latency) metrics in a proportional manner to calculate the path weights while assuring that only paths which satisfy all metrics are selected. It ensures the best available path in terms of the metrics [18].

The main goal of SRQR is to bypass performance degradation on the Internet path by having multihop routing on the overlay network. However, a drawback of this approach is that it entails additional hops leading to performance degradation in the overlay network. In order to overcome this drawback, we employ the following approach: The idea being that after the start of the flow over the path (which is allocated by mSN), each overlay node on the path probes the destination to decide whether direct communication meets the QoS requirements. If yes, then the overlay node skips the rest of overlay nodes on the path and sends directly to the destination. When a significant link state change is reported, the overlay node, skipping the rest of path, probes the direct link whether it still satisfies the flow's requirements. This approach provides a significant performance improvement for SRQR.

6.2 Resource monitoring

To obtain QoS-satisfied communications by using SRQR, available resources of the links (i.e., link bandwidth, reliability, and latency) need to be monitored. Thus, HetGrid employs pinging and direct bandwidth measurement methods in each mSN to obtain its adjacent links' states, as in Li [13]. Each mSN disseminates the gathered link state information to the other mSNs when significant changes occur on the links. However, these measurements might be noisy, and this leads to oscillation or the wrong selection in the path allocation. To avoid this, HetGrid applies a 5% hysteresis bonus to the "last good" measurements for the three metrics, thus providing a reasonable trade-off between responsiveness to the link state change and the oscillations.

6.3 Altruistic flow allocation (AFA)

DA applications have both periodic (flow) and aperiodic data traffic. Assuring availability of the resources for critical/high priority data traffic in such a network is a difficult task. Existing works try to cope with resource allocation by building different virtual networks for QoS requirement classes on top of an overlay network and smartly allocate the resources, as done with policy routing in [12]. However, these methods base on static resource allocation for the applications that need

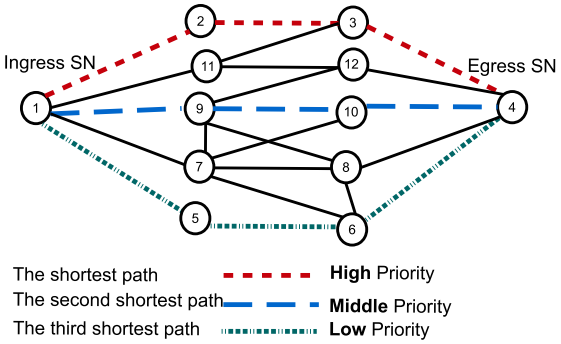

Fig. 3 Basic illustration of AFA

static QoS requirements and introduce best-effort performance but not predictable. For DA applications with changeable and strict QoS requirements [3], these are not efficient approaches.

AFA introduces an implicit allocation mechanism for quick adaptation to the dynamic background traffic of the overlay network. The implicit allocation fundamentally relies on binding a flow to a specific path by utilizing source routing. To make this happen, the other nodes in the overlay network also refrain from using the resources on that path by following the restrictions from resource monitoring mechanism. Moreover, to assure availability of the resources for critical/high priority data traffic, AFA selects a path from k paths[4] depending on the application's priority, as illustrated in Figure 3. Thus, the low priority applications sacrifice the "best" resources (but their requirements are still satisfied with the path allocated for them) in exponential manner for the sake of the critical applications in a distributed manner. Moreover, our AFA approach implicitly provides a resource reservation for aperiodic and critical messages. For a pair belonging to an application, a corresponding path (indicated by z) is chosen by the ingress mSN between the first/shortest path and k_{th} path by using the following equation:

$$\lambda = k(\frac{e^{\rho} - 1}{e - 1}) \tag{2}$$

$$z \leftarrow \lfloor \lambda \rceil$$

z is the integer value where $\lfloor \rceil$ indicates rounding λ to the nearest integer and ρ represents priorities in the range [0-1], e.g., 0, 0.5, and 1 represent low, medium and high priority respectively. Employing the equation, the z_{th} path is identified by the ingress mSN for the flow allocation. If k equals to 0, the equation 2 cannot

[4] k paths are found by using the k shortest path algorithm and equation 1. We do not put a limit on k to pave the way for obtaining more disjoint paths. In our implementation, k is observed between 5-20

find a path and multiple paths are required to compensate the reliability requirement of the application. To do this, HetGrid employs the following multi-routing CMR mechanism.

6.4 Compensative multi routing (CMR)

In case that SRQR fails to find any path that satisfies the QoS requirements ($k = 0$), the CMR mechanism, which is running on mSNs, tries to find multiple paths whose total reliability (packet loss rate) satisfies the application. Once CMR has found the paths, it relays redundant replicated data over them. On the other hand, it strives to discover disjoint paths rather than transmitting single path, which has the highest reliability degree, by aiming to cope with permanent failures as well. To do this, mSN running CMR organizes the d SN in its cluster for the assignment of disjoint redundant paths, thus achieving E2E disjointness. However, the open question is how to determine the number of SNs (among d SNs) whose paths provides the required reliability degree. To address it, we propose the following approach:

$$PR_i^D = \prod_j^N RL_j \tag{3}$$

$$R_R \leq 1 - \prod_i^M (1 - PR_i) \tag{4}$$

where PR_i^D is the reliability degree of path i towards the destination D, while RL_j is the reliability degree of the link on the path (containing N links). While equation (3) calculates path reliability, equation (4) computes total reliability of M parallel paths, and compares the total reliability with the required reliability degree. CMR employs an iterative algorithms for finding the number of parallel paths (M), which compensate the required reliability degree R_R. Moreover, while selecting the parallel paths, this algorithm tries to eliminate the path whose similarity (in terms of SNs) on the already selected path(s) are higher than a threshold value, heuristically defined.

6.5 Adaptable Ack mechanism (AAM)

For an application that needs feedback or delivery guarantee, HetGrid introduces AAM. It supports an adaptable acknowledgment mechanism by allowing applications to adjust the delay of sending acknowledgment depending on their latency requirements. Thus, several ACK responses may be combined together into a single response (by combining the number of network updates), thus reducing protocol overhead. Since many DA applications have small payloads (e.g., 100-200 bytes) [21], it is clear that AAM obtains efficient data transmission by minimizing the Ack traffic. We build AAM inspired by TCP's delayed acknowledgment technique.

6.6 Putting it all together

The SRQR protocol strives to find the QoS-satisfied path for each application according to their QoS requirements (e.g., bandwidth, latency, reliability) in addition to traffic balancing over the secondary layer of the overlay network. However, as SRQR employs the shortest path algorithm that tends to greedy resource usage, this can lead to a lack of resource for the critical application. AFA provides a solution by reserving the "best" resources for high priority applications. If SRQR cannot find a path that satisfies the applications' reliability requirements, CMR can compensate by employing multipath (in adequate number) routing for the affected applications. Finally, AAM guarantees data delivery in addition to reducing the protocol overhead in the network by employing an adaptive mechanism, which configures the delay of Ack messages depending on time-sensitivity of applications. HetGrid provides QoS-satisfied and fault tolerant communication without producing expensive overhead as it is able to employ these mechanisms depending on the application requirements.

7 Evaluation

HetGrid is implemented by using the OverSim [26] and INET framework that run on OMNeT++ [27]. This simulation setup paves the way for our perturbation scenarios. The main purpose of our simulation-based evaluation is to assess HetGrid against direct TCP connection according to (1) QoS-satisfaction of each application, and (2) fault-tolerance in the system, e.g., the effect of failures on the critical applications. We deploy TCP Vegas from among TCP flavors in our implementation as it can address the heterogeneous networks better than the other flavors [32] and obtains between 40 and 70% better throughput, with $1/5^{th}$ to 1/2 the losses, as compared to the TCP Reno [33].

We first present underlay topology and background traffic model, followed by overlay network, traffic demands, and metrics.

Table 1 Performance evaluation parameters

App.	Msg. size	Para.	Prio.(p)	R_R	R_L	Deli. Mode
Ash	32 B	1 event /15s	high (1)	high (99.90%)	Low(< 150ms)	M1, M3
Asm	32 B	1 event /15s	medium (0.5)	medium (99%)	medium (150ms <,<2s)	M3
Asl	32 B	1 event /15s	low (0.1)	low(97%)	High (>2s)	M2, M4
Ach	32 B	1 event /120s	high (1)	high (99.90%)	Low (<150ms)	M1, M3
Acm	32 B	1 event /120s	medium (0.5)	medium (99%)	medium (150ms <,<2s)	M3
Acl	32 B	1 event /120s	low (0.1)	low(97%)	High (>2s)	M2, M4

7.1 Underlay network topology

We randomly produce a hierarchical topology using BRITE [29] in order to construct an Internet-like underlay topology. The topology includes 20 nodes (we consider that each node denotes an AS's BGP router) for the AS level and 10 nodes (i.e, IGP routers) under each BGP router with an edge density changing from 2 to 5. For inter-AS and intra-AS networks, two bandwidth configurations are used: all links are either OC3 (i.e., 51.84 Mbps) or OC48 (i.e., 155.52 Mbps). The propagation delay of each link is randomly chosen between 0-10 ms subject to a uniform distribution.

7.2 Background traffic

A dynamic background traffic load across the network is generated during simulation in order to assess HetGrid's success in the case of dynamic latency and bandwidth in the underlay network. To produce this background traffic, we deploy 200 servers (each one connects to each edge router) that relay a packet (1-100kb) per sec to a random server.

7.3 Overlay network and traffic demands

In the simulation, $|V_o|$=1000, including (|mSN|=20 and |NN|=980), and these overlay nodes are randomly deployed to 20 ASes. The AS-based clusters have two rSN ($d-1=2$, total |rSN| = 40) and their computation capacities are adequate and larger than the other NNs. The outgoing bandwidth of SNs and NNs are 10 Mbps and 1 Mbps, respectively.

According to data traffic requirements of DA applications [22], six application models as shown in Table 1 are employed. Each overlay node randomly runs one of the six applications and chooses a destination node to relay the application's messages. In the simulation, each node measures its adjacent links' latency, bandwidth and loss rate every 5 seconds and if there is more than 5% change [12], e.g., a significant alternation of the three metrics or an outage in the network, it broadcasts the measured values of the link(s).

7.4 Metrics

HetGrid is assessed based on the QoS-satisfaction of each application and the fault-tolerance in the system. QoS-satisfaction of a given application is computed based on its data delivery monitoring results, i.e., latency and loss rate. A dropped or timed out message is specified as an unsuccessful message delivery. To quantify the satisfaction of a communication, QoS-satisfaction rate (QSR) is formalized as:

$$QSR = 1 - \frac{DroppedOrTimedoutMessages}{SentMessages} \quad (5)$$

7.5 Simulation methodology

Our evaluation is carried out in four different scenarios. The first three scenarios aim to realize the most common Internet perturbations in order to assess HetGrid's QoS-satisfaction performance on the Internet. The final one's aim is to investigate the scalability of HetGrid if the overlay traffic sharply increases. Lastly, we compare the network overhead of the both approaches to highlight the caveats of the approaches.

Dynamic link state: To realize the dynamic behavior of the Internet, we periodically (every 10 sec.) and randomly switch bit error rate (BER) of links from the range of (1e-10, 1e-7) to (1e-10, 1e-3) as well as the background traffic produced by the servers. In this scenario, we aim to evaluate whether HetGrid provides an adequate QoS-satisfaction level for DA applications on a best-effort network like the Internet (considered as the Internet provides unstable performance).

2% Underlay router failure: As mentioned in section 3, BGP router failures and their re-convergence time are severe problem for the applications which have stringent QoS requirements. To investigate the effectiveness of HetGrid on these failure types, 2% of the underlay routers fail around 10 min (like typical BGP

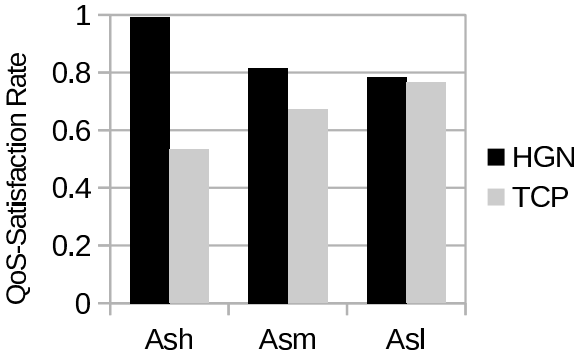

Fig. 4 Dynamic link state scenario: Sensing applications

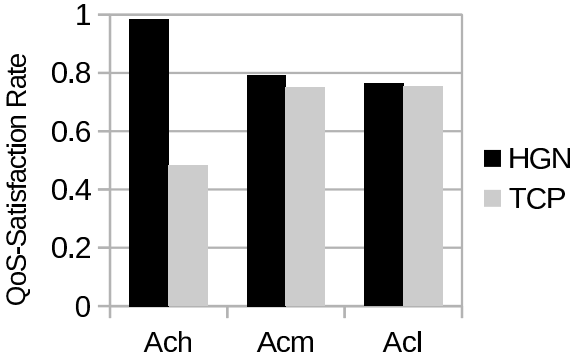

Fig. 5 Dynamic link state scenario: Control applications

re-convergence time [5]). These router failures repeat every 10 min in randomly selected routers during the simulations. 2% of the routers is fixed as 1 BGP and 1 IGP router in our simulation. This scenario helps assess HetGrid's failure recovery mechanism, as well as the fault tolerance efficiency of CMR for critical applications, in case of the resource failures occur in the Internet.

Heavy congestion scenario: When the majority of Internet users are concurrently online, the traffic congestion leads to long lag time for the users. To realize this perturbation, the delivery rate of the background traffic is increased by being sent a packet every 100 ms, instead of every 1 s, by 40% of the servers (random selection). Employing this scenario, we assess the "best" path selection efficiency of SRQR.

Bursty traffic on the overlay network: To assess the scalability of HetGrid in case of bursty traffic on the overlay network, we increase delivery rate of the sensing applications in three step, i.e., 1 msg. /15 sec, 1 msg. /10 sec, and 1 msg. /5 sec (DA applications' traffic volume can change depending on some conditions [19]). The main aim of this scenario is to investigate whether AFA smartly allocates resource for critical applications even in bursty overlay traffic.

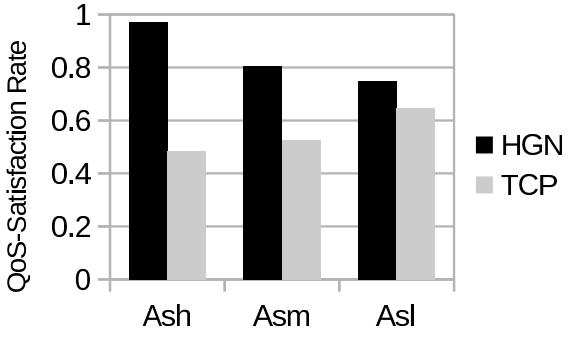

Fig. 6 2% Underlay Router Failure: Sensing applications

7.6 Simulation results and discussion

In our simulations, we consider that while the sensing applications require periodic data delivery, e.g., periodic voltage measurements, the control applications need aperiodic data delivery, e.g., command messages. However, while these applications share the overlay network, AFA allocates resources for only the sensing applications, but not for the control applications. Hence, we compare HetGrid (HGN) with direct TCP connection differing in both the control and the sensing applications to assess their performance for both traffic types. Simulation results are first investigated for each specific scenario and then discussed holistically.

Dynamic link state: Figure 4 depicts QSR of HGN and direct TCP connections for the sensing applications with three different priorities, i.e., high, medium, and low priority. It shows that HGN remarkably provides higher QSR in each priority level in comparison to direct TCP connections between pairs thanks to SRQR. In addition, although the high priority applications have stringent QoS requirements, HGN provides significant QSRs for higher priority applications in contrast to direct TCP connections owing to AFA's priority-based flow allocation mechanism. On the other hand, Figure 5 shows that HGN presents a performance near sensing applications for control applications thanks to AFA's the "best" resource reservation for aperiodic messages (considered as high priority). However, TCP also provides a performance close to the sensing applications (middle/low priority), but not with a consistent behaver. The reason of TCP's inconsistency is its lack of adaptability to the link state change in the inter-AS connections.

2% Underlay router failure: Figure 6 shows QSR of HGN and direct TCP connections for the sensing applications when 2% of the underlay routers fail. In the Figure 6, whereas HGN provides QSR with slight degradation for each priority, TCP connections present a remarkable QSR degradation in comparison to their dy-

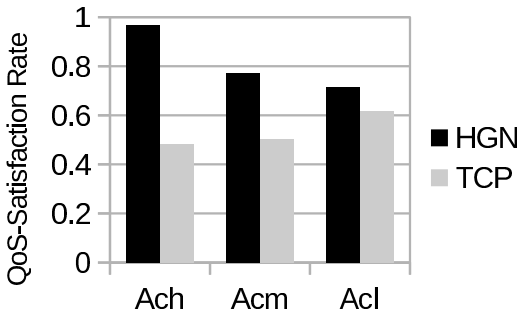

Fig. 7 2% Underlay Router Failure: Control applications

namic link state scenario results. Owing to HGN's fast recovery system, the sensing applications using HGN experience slight degradation in comparison to TCP connections. In particular, the high priority applications experience lower degradation than the others in HGN thanks to CMR's sufficient multipath routing mechanism. Moreover, Figure 7 depicts HGN nearly maintaining its QSR performance also for aperiodic application.

Heavy congestion scenario: The effects of heavy congestion on the QoS-satisfaction of the sensing applications are shown in Figure 8. HGN provides significant QSRs for high and medium priority messages in comparison to TCP connections. However, both HGN and TCP presents almost the same QSR performance for the low priority since AFA allocates the limited resources for higher priority applications in such a heavy congested network. In addition, Figure 9 depicts that HGN provides a similar performance to the sensing applications for the control applications even under heavy congestion.

Bursty traffic on the overlay network: Figure 10 shows the efficiency of HGN while increasing the work load on the overlay network. We can observe that HGN saves QSR of high priority applications compared with medium and low priority applications. This provides relatively an adequate QSR for the high priority/critical applications if the bursty traffic is occasionally experienced by the overlay network.

Network overhead comparison: Figure 11 shows that network overhead comparison of the both approaches in different failure scenarios: D.L.S., 2% F. and H.C. denote Dynamic Link State, 2% Underlay Router Failure, and Heavy Congestion scenarios respectively. It is clear to see in figure 11 that TCP Vegas produces more overhead than AAM in D.L.S. scenario, despite HGN's additional source routing overhead. The reason for this is that whereas TCP Vegas employs fast retransmission for each applications, AAM uses an adaptive acknowledge mechanism in addition to UDP transport protocol. Moreover, as TCP's a higher header size (20 bytes) yields additional protocol overhead for DA applications requiring small size packet delivery (e.g., 100-200 bytes) [22], TCP is not convenient transport protocol. On the other hand, as shown in figure 11, when the failure/congestion area expands in the network, HGN network's overhead can surpass TCP's, since it must disseminate more link state information. However, the infrequent occurrence of long failures or heavy congestions in the Internet offer a pragmatic basis for the additional overhead for HGN.

Discussion: In our evaluation, we assessed QSR performances of HGN and direct TCP connection in common Internet perturbations, as well as overlay bursty traffic. We separately evaluate their QSR performances for periodic and aperiodic traffic by produced the sensing and the control DA applications, respectively. The result shows that HGN presents a significant QSR for DA applications on the Internet-like network in scalable manner thanks to its clustering mechanism. In particular, its QSR for high priority applications shows that employing of HGN enables the usage of the heterogeneous network for DA applications. The maintained QSR for high priority applications, in even the underlay failures or heavy congestions, is also a notable feature for DA applications. Furthermore, although HGN saves the resources for the sake of high priority applications by sacrificing the QoS of medium and low priority applications, HGN's QSR performances for medium and low priority applications still outperform TCP connection. HGN also shows that if bursty traffic happens on the overlay traffic, it does not allow significant QSR degradation for high priority application. On the other hand, in the simulation experiments, since HetGrid has a reactive link state dissemination mechanism and a low overhead transport mechanism (UDP + AAM), we do not observe a remarkable overhead rise in comparison to TCP Vegas. Finally, despite a significant decline in the number of the unsatisfied high priority messages in the use of HetGrid, the unsatisfied messages could cause severe problems in the grid. This can be handled by investing for more multihoming and direct fiber optic links between SNs.

8 Related works

To put our contributions in context, the related works span two distinct subjects fields: (i) Resilient and QoS-aware communication systems for Smart Grid, and (ii) Systems providing reliable and real-time communication on the Internet.

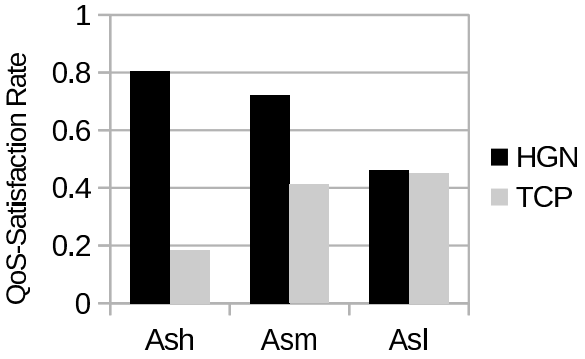

Fig. 8 Heavy Congestion Scenario: Sensing applications

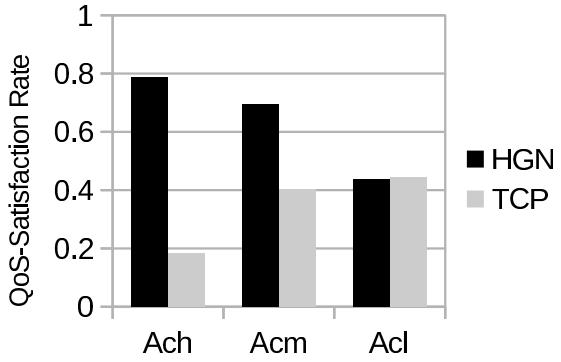

Fig. 9 Heavy Congestion Scenario: Control applications

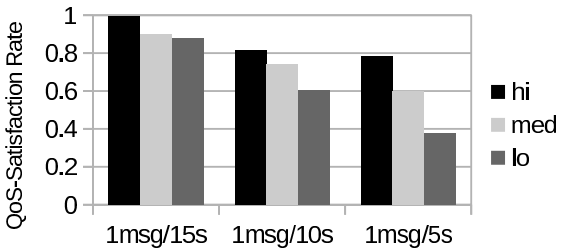

Fig. 10 Bursty Traffic on the overlay network: Sensing applications

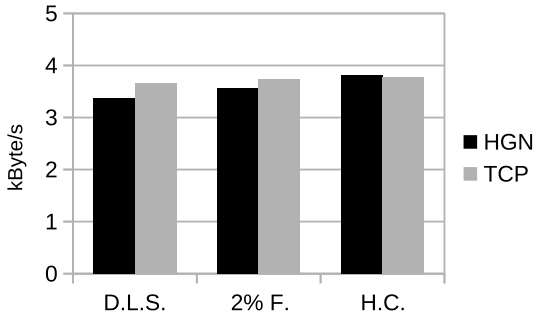

Fig. 11 Overhead comparison in different failure scenarios: D.L.S., 2% F. and H.C. denote Dynamic Link State, 2% Underlay Router Failure and Heavy Congestion scenarios respectively.

8.1 Resilient and QoS-aware communication systems for smart grid

Recently, many middleware approaches simplifying application development on a variety of platforms, operating systems, networking technologies are proposed for supporting the data plane dimension of the smart grid.

The INTEGRIS [9] project proposes the use of a QoS broker device to enhance the QoS in SDG by employing a centralized QoS management. It suggests a novel information and communication technologies (ICT) infrastructure based on mixing heterogeneous OSI layer 2 technologies (PLC, wireless, etc.) integrated through a middleware. Since they offer a QoS management mechanism for a dedicated heterogeneous network, this proposal can be implemented for only utility owned communication network. The GridStat [10] project proposes a pub-sub network of message routers controlled by a hierarchical management plane to satisfy the NASPInet QoS requirements. However, GridStat assumes that it receives certain QoS guarantees from the underlay network and the network topology is fully known. Further, it uses static routing to avoid the overhead of dynamic link-state-based routing. This proposal cannot obtain E2E guaranteed delivery in the use of public carriers since its design is not formed depending on the best-effort Internet infrastructure but dedicated networks.

The SmartC2Net [32] project aims to develop, implement and validate robust solutions that facilitate Smart Grid operation on top of heterogeneous off-the-shelf communication infrastructures with diverse properties. The functions of the obtained new middleware are: (1) adaptive network and grid monitoring, (2) control methodologies for communication network configurations and QoS settings, and (3) models of the extended information and procedures for adaptive information management. SUNSEED [33] proposes an evolutionary approach to usage of the existing communication networks from both energy and telecom operators by improving their robustness/reliability. The project proposes an exposed application programming interfaces (API) based on open standards (W3C) to enable third-party creation of new businesses related to energy and communication sectors (e.g. virtual power plant operators).

M. Albano, et al. [32] overview varied categories of communication middleware focusing on message oriented middleware (MOM). They particularly address data distribution services (DDS) targeting distributed real-time systems (for smart grid applications) with complex distributed applications, where prioritization requirements have to be assured. On the other hand, T. Prodejev, et al. [33] devise a working architecture

that relies on the ETSI M2M components (upgraded by CoAP and Websockets), and is mapped to the Smart Grid. The authors analyze whether the heterogeneous solution is able to meet the communication requirements of the diverse Smart Grid applications. Due to the lack of underlay topology-awareness of these approaches, the critical application's reliability and latency requirements cannot be met by employing only these approaches.

SeDAX [34] proposes a data-centric communication method on a secure overlay network on top of the existing TCP/IP network. This method provides good routing performance and self-configurable group communication. However, it is inapplicable for real-time applications, e.g, DA, and distributed generation, since it does not guarantee E2E latency. Deconinck G., et al. [35] propose a dependable infrastructure for autonomous decentralized microgrid control. It enables power devices to interact over a self-organized and semantic peer to peer overlay network on top of the existing TCP/IP network, called Agora. Since this work concentrates on non-time-critical applications (secondary and tertiary voltage control), it cannot cope with the strict timely communication requirements of DA applications.

8.2 Systems providing reliable and real-time communication on the Internet

Although there have been advances in the QoS provisioning in network-level approaches, the models such as DiffServ [6], IntServ [7] and MPLS [8] are still far from deployment in the Internet due to the change requirements in the networking infrastructure or the configuration differences among the domains. Although MPLS/VPN [36] is introduced as a QoS- guaranteed communication protocol, its QoS-guarantee implies not guarantee for inter-AS connections but only within an AS.

As the Internet is increasingly used for the mission critical applications, connection reliability and latency are becoming severe challenges. To address these challenges, service overlay networks managed by third party providers are advocated. The providers target to offer QoS-guaranteed service for multiple applications and clients on the Internet, RON [12], OverQoS [14], and NGSON [16]. RON and NGSON are well defined and known service overlay network approaches. They provide reliable and timely communication on the wide area networks for the distributed applications. However, they do not offer timely delivery guarantee per message for safety-mission critical applications, e.g., the islanding protection in SDG. In addition, no adaptive QoS and reliability mechanism depending on application criticality are introduced in those projects. For safety critical applications, even short-lived failures of the Internet infrastructure can pose significant damage risk on the grid. As a remedy of these problems, Han [25] proposes a topology aware overlay framework to maximize path independence for better availability and performance of E2E communication in the Internet. However, it does not introduce any traffic prioritization and resource allocation mechanisms in its work. All of the above works lack at least one of the following criteria: (i) fault tolerance, (ii) scalability, (iii) adaptive QoS management.

9 Summary

We have shown that HetGrid provides reliable and QoS-aware communication on heterogeneous public and private network, considering the DA applications' requirements. It selects and employs overlay nodes with the most resources to manage inter-AS communication rather than place dedicated servers into each domain and needs only local underlay knowledge to enable reliable communication across the network. To provides reliable and QoS-aware communication, HetGrid employs the following mechanisms in a self-adaptive manner: (1) SRQR finds the "best" path considering bandwidth, latency, and reliability requirements of the applications. It also uses altruistic flow allocation (AFA) to reserve the "best" path for high critical applications. (2) To obtain fault tolerant communications for high priority applications, CMR employs adequate paths for multipath routing depending on the reliability requirement of the application.

The simulation result demonstrates that HetGrid provides a significant QoS-satisfaction rate for each application compared with direct TCP connection between pairs. In addition, even for BGP router failures or heavy Internet congestions, it provides practical QoS- satisfaction rates by employing the above mechanisms in an adaptive manner. Thus, HetGrid demonstrates both the feasibility of using a heterogeneous public/private network for DA applications and also the architecture to achieve the robust QoS-aware communication.

References

1. Gungor VC, et al. (2013) A Survey on Smart Grid Potential Applications and Communication Requirements. Industrial Informatics, IEEE Transactions on 9(1):28-42
2. KC Budka, et al. (2010) Communication network architecture and design principles for smart grids. Bell Labs Tech. Journal. 15(2):205-228

3. US Dept. of Energy (July 12, 2010) Implementing the National Broadband Plan by Studying the Communications Requirements of Electric Utilities To Inform Federal Smart Grid Policy. Tech. rep. Retrieved June 14, 2015, http://energy.gov/sites/prod/files/gcprod/documents/UtilitiesTelecom_Comments_CommsReqs.pdf
4. Yannan W, (2015) Decentralized Communication and Control Systems for Power System Operation. Smart Grid, IEEE Transactions on. 6(2):885-893
5. Wang G, et al. (2013) An efficient relay node selection scheme to improve the performance of P2P-based VoIP applications in Chinese internet. Multimedia Tools Appl. 64(3):599-625
6. Differentiated services (DiffServ) Retrieved June 14, 2015, from http://www.ietf.org/html.charters/ diffserv-charter.html.
7. Integrated Services (IntServ), Retrieved June 14, 2015, from http://www.ietf.org/html.charters/intserv- charter.html
8. Multiprotocol Label Switching Architecture (MPLS), Retrieved June 14, 2015, from https://www.ietf.org/rfc/rfc3031.txt
9. Vallejo A, et al. (2012) Next-generation QoS control architectures for distribution smart grid communication networks. IEEE Commun. Mag. 50(5):128-134
10. Bakken DE, et al.(2011) Smart generation and transmission with coherent, real-time data. in Proc. of the IEEE. 99(6):928-951
11. Dantas WS, et al. (2009) Not quickly, just in time: Improving the timeliness and reliability of control traffic in utility networks. In Proc. of the 5th Workshop on Hot Topics in System Dependability HotDep09
12. Andersen DG, et al. (2001) Resilient overlay network. in Proc. of the ACM SOSP, pp 131-145
13. Li Z, Mohapatra P (2004) QRON: QoS-aware routing in overlay networks. IEEE Journal on Selected Areas in Communications. 22(1):29-40
14. Subramanian L, et al. (2004) OverQoS: An Overlay Based Architecture for Enhancing Internet QoS. NSDI 4(6):71-84
15. Vulimiri A, et al. (2012) More is less: reducing latency via redundancy. In: Proc. of ACM Workshop on Hot Topics in Networks, pp 13-18
16. Lee S, Kang S (2012) NGSON: features, state of the art, and realization. Communications Magazine, IEEE. 50(1):54-61
17. Brakmo LS, O'Malley SW, Peterson LL (1994) TCP Vegas: New techniques for congestion detection and avoidance 24(4):24-35
18. Demir K, et al. (2014) Robust and Real-time Communication on Heterogeneous Networks for Smart Distribution Grid. Smart Grid Communications (SmartGridComm). IEEE International Conference on, pp 392-397
19. Kanabar PM, et al. (2009) Evaluation of Communication Technologies for IEC 61850 Based Distribution Automation System with Distributed Energy Resources. Proc. of the IEEE PES General Meeting, Calgary, pp 26-30
20. US Dept. of Energy (October 5, 2010) Communications Requirements of Smart Grid Technologies. Tech. rep. Retrieved June 14, 2015, http://energy.gov/sites/prod/files/gcprod/documents /Smart_Grid_Communications_Requirements_Report_10-05-2010.pdf
21. Khan RH, Khan JY (2013) A comprehensive review of the application characteristics and traffic requirements of a smart grid communications network. Computer Networks. 57(3):825-845
22. Qiang Y, et al. (2011) Communication infrastructures for distributed control of power distribution networks IEEE Trans. Ind. Informatics. 7(2):316-327
23. Zhao BY, et al. (2002) Brocade: Landmark Routing on Overlay Networks. in Proc. of IPTPS, pp 33-34
24. Ren S, et al. (2006) Asap: an as-aware peer-relay protocol for high quality voip. In Proc. of Int. Conf. on Distributed Computing Systems, pp 70-79
25. Han J, et al. (2008) Enhancing end-to-end availability and performance via topology-aware overlay networks. Computer Networks. 52(16):3029-3046
26. Baumgart I, et al. (2007) OverSim: A Flexible Overlay Network Simulation Framework. in Proc. GI at INFOCOM, pp 79-84
27. Pongor G (1993) OMNeT: Objective Modular Network Testbed. in Proc. of MASCOTS, pp 323-326
28. Elmannai W, Razaque A, Elleithy K (2011) Simulation based Study of TCP Variants in Hybrid Network. In proc. of int. conf. on ASEE'11 Northeast Section Conference
29. Medina A, et al. (2001) BRITE: An approach to universal topology generation. in Proc. of MASCOTS, pp 346-353
30. Ciontea C, et al. (2015) Smart grid control and communication: The SmartC2net Real-Time HIL approach. in PowerTech'15, IEEE Eindhoven, pp 1-6
31. Stefanovic C, et al. (2014) SUNSEED An evolutionary path to smart grid comms over converged telco and energy provider networks. in Wireless Communications, Vehicular Technology, Information Theory and Aerospace & Electronic Systems (VITAE), 4th International Conference on, pp 1-5
32. Albano M, Ferreira LL, Pinho LM, Alkhawaja AR, (2015) Message-oriented middleware for smart grids", Computer Standards & Interfaces (38):133-143
33. Predojev T, Al-Hezmi A, Alonso-Zarate J, Dohler M (2014). A real-time middleware platform for the smart grid. In Green Communications (OnlineGreencomm), 2014 IEEE Online Conference on, pp 1-6
34. Kim Y, et al. (2012) SeDAX: A Scalable, Resilient, and Secure Platform for Smart Grid Communications Selected Areas in Communications. IEEE Journal on. 30(6):1119-1136
35. Deconinck G, et al. (2010) Communication overlays and agents for dependable smart power grids. Critical Infrastructure (CRIS). 5th International Conference on, pp 1-7
36. El H, et al. (2008) Efficient QoS Implementation for MPLS VPN. Advanced Information Networking and Applications (AINAW). 22nd International Conference on, pp 259-263