# MPTCP-H: A DDoS Attack Resilient Transport Protocol to Secure Wide Area Measurement Systems

Kubilay Demir[1], Ferdaus Nayyer, and Neeraj Suri

*Dept of CS, TU Darmstadt, Germany*

**Abstract**

The penetration of distributed generators into the power distribution grid requires real-time control of the grid by monitoring the state of the power distribution grid. Such a large-scale monitoring cannot be performed by using traditional Supervisory Control and Data Acquisition (SCADA) systems due to its lack of the scalability. To address this issue, contemporary Wide Area Measurement Systems (WAMS) are deployed, which provide the dynamic snapshots of the power system. However, WAMS's more open structure versus SCADA poses a risk of WAMS being vulnerable to cyberattacks. In particular, due to high responsiveness and availability requirements of WAMS applications, attacks i.e, Denial-of-Service (DoS) and Distributed DoS (DDoS) are of primary concern for WAMS.

In this paper, we focus on internal DoS/DDoS attacks launched against the WAMS devices by exploiting the vulnerabilities. To counter such attacks, we propose a proactive and robust extension of the Multipath-TCP (MPTCP) transportation protocol, termed as MPTCP-H. The proposed extension mitigates the internal attacks by using a novel stream hopping mechanism, which periodically renews the subflows to hide the open port numbers of the connection. By doing so, MPTCP-H significantly increases the attacker's cost for a successful attack without perturbing the WAMS data traffic. The experimental results show that the proposed MPTCP-H provides a significant DoS/DDoS attack mitigation for WAMS at the expense of reasonable overheads, i.e., additional latency and message.

*Keywords:* Availability, Security, Multipath TCP, DDoS attack, Smart Grid

## 1. Introduction

The Smart Grid (SG), differing from the classical power grid with fixed generation sources, dynamically coordinates multiple heterogeneous power sources and load balancing activities in the power distribution grid to provide reliable and cost efficient energy services. This is achieved by tightly interlinking the power producers and consumers (the physical resources) using advanced computing/communication technologies (the cyber resources) to form an adaptive cyber-control system, i.e., a state machine [1]. The effectiveness of such cyber-control systems is based on achieving real-time and accurate state information as obtained from an efficient and reliable communication scheme. Thus, runtime state estimation constitutes a critical element to maintain performance and resilience of the SG over any network failures transpiring as either operational failures or as deliberate attacks. In practice, this state assessment is achieved by using Wide Area Monitoring Systems (WAMS). WAMS uses Phasor Measurement Units (PMUs, and also known as Synchrophasors) for data acquisition to monitor real-time power transmission and to detect grid instabilities [2]. The PMUs periodically sample the voltage and current parameters of the power system, and subsequently forward the sampled data to the Phasor Data Concentrator (PDC) for processing.

As WAMS form the core of SG operations, this criticality also makes the WAMS susceptible to attacks that can exploit communication level vulnerabilities to compromise the critical WAMS requirements, e.i., low-latency and high-availability. In particular, Denial-of-Service (DoS) and Distributed DoS (DDoS) attacks can be conducted towards the PMUs or PDCs to cause transmission delays or loss of measurements. Consequently, this can result in a severe degradation in SG perfor-

[1]Email Adresses: {kubidem, suri}@cs.tu-darmstadt.de, ferdaus.nayyer@stud.tu-darmstadt.de
Corresponding Author: Kubilay Demir,
Research supported in part by EC H2020 CIPSEC GA #700378.
Dept of CS, TU Darmstadt Hochschulstr. 10, 64289 Darmstadt, Germany Phone: +49-6151-16-25225 Fax: +49-6151-16-25230

mance in terms of inaccurate predictions of transmission status, network metering failures or delays in the mitigation of power network failures.

In this paper, we extend upon the advocated Multipath-TCP (MPTCP) approach to provide a resilient and efficient communication scheme for the WAMS phasor measurement processes. The basic MPTCP provides long-duration communication connections [3] and provides reactive mitigation against attacks with its diverse multi-path functionality. However, in order to achieve proactive and robust protection of the transport and application layer from DoS/DDoS attacks, we introduce a novel stream hopping mechanism, which is directly integrated into MPTCP, termed MPTCP-H. The proposed hopping mechanism hides open port numbers by refreshing of the sub-flows over time, with new port numbers, without causing data traffic interruptions. This mechanism is shown to provide high protection against transport and application layer DoS/DDoS attacks. The results from MPTCP-H demonstrate that the proposed approach indeed secures the system with minimal additional latency and message overhead.

*Paper Contributions:*

- A practical threat model where the DoS/DDoS attacks can occur in the WAN via compromised devices, and accordingly saturate the WAMS devices.
- A novel defense mechanism that mitigates DoS/DDoS attacks by periodically switching the MPTCP connection subflows.
- Empirical validation of the MPTCP-H's overhead and availability provided by MPTCP-H under DoS attacks.

This paper, which utilizes the foundations developed in our preliminary work [4], has different objectives and significantly extends our preliminary work with mechanisms to improve performance, and a resilient and secure communication. Specifically, the basic stream hopping and the authentication mechanisms are fully developed to provide a better performance and DDoS attack resilience for wide area monitoring systems (WAMS). The expanded thread model (Section 3) along with the MPTCP-H architecture (Section 4) fully detail the developed idea. Further, the paper includes new experiment results (Section 6) such as the assessment of (a) additional message and latency overhead, and (b) the availability and latency performance of the proposed mechanism (MPTCP-H) under DoS attack. The new material enables a better understanding of the feasibility of MPTCP-H for WAMS applications, and highlights the DoS attack mitigation performance of MPTCP-H.

The remainder of the paper is organized as follows. Section 2 provides the background on WAMS and MPTCP. Subsequently, Section 3 outlines the system and threat models, and the corresponding security considerations. Section 4 introduces our proposed approach, termed as MPTCP-H, and is followed by Section 5 that provides the security analysis for MPTCP-H. Section 6 details the implementation of MPTCP-H. Section 7 presents the evaluation of our proposal. We discuss the related works in Section 8.

## 2. Background

This section outlines the technical characteristics of WAMS in a SG. We also provide a background on MPTCP operations that are used in our proposed MPTCP-H extension.

### *2.1. Wide Area Measurement Systems (WAMS)*

Accurate estimation and monitoring of the state of the power network is critical for SG operations. The traditional Supervisory Control and Data Acquisition (SCADA) systems are employed for periodically sampling at predefined time intervals, e.g., per second. In order to manage the SG in a reliable and efficient manner, WAMS offer high sampling rate (e.g., >60 frames per second (fps)), low-latency, high-precision and time-synchronized measurements by taking advantage of phasor measurements (both magnitude and phase angle) obtained from the deployed Phasor Measurement Units (PMUs). Whereas SCADA systems are unable to handle the dynamic snapshots of a power system, the advanced WAMS support real-time behavior of the power system to mitigate unexpected power blackouts. While the WAMS technology supports the SG control functions with real-time state monitoring, any inaccuracies in the state information arising from communication perturbations or assessment errors, can also detrimentally affect the SG stability.

In this paper, we focus on a multi-tier WAMS architecture that interfaces, in turn, with the high voltage (HV) substation PMUs followed by substations PDCs, regional PDCs and control center PDC (cf. Fig. 1 [5]), where the HV substation PDCs also connected with PMUs in the neighboring substations (ca. 20-40 PMUs) [5].

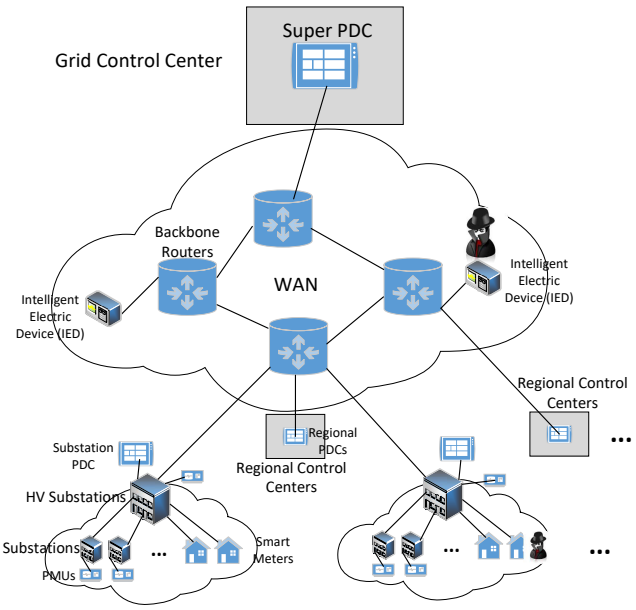


Figure 1: An SG network overview

In the hierarchical architecture, the measurements of PMUs are forwarded to the substation PDCs that sort the received data by timestamps and examine any missing data for requisite analysis. The substation PDCs then transmit the prepared measurements to the regional PDCs for subsequent forwarding to the national monitoring centers, as shown in Figure 1. The characteristics of WAMS are as follows [5].

A HV substation of the Power Grid (Substation PDC):

- ~ 20-40 PMUs connected to the PDC.
- PMU data rates (60-120 fps for 60Hz systems).
- Tolerable internal latency (~3-10 ms).
- Applications requiring fast response as well as local visualization and archiving.

Regional centers of WAMS (Regional PDC):

- Responsible for a large number of PMUs (~50-500).
- Data rates between 30-60 fps.
- Tolerable internal latency (~10-100 ms).
- Applications for regional operation, e.g. state estimation.

Main control center (Super PDC):

- Accommodation of a very large number of PMUs (a few thousand PMUs).
- Low data rates (~1-30 fps).
- Tolerable internal latency (~100 ms-1s).
- Applications that perform visualization combining SCADA and Synchrophasor data.

### 2.2. *Multipath TCP (MPTCP)*

Multipath TCP is a recent TCP extension [6] and an Internet Engineering Task Force (IETF) standard, which is still in its experimental phase. MPTCP allows a single TCP connection to make simultaneous use of multiple paths by opening several subflows, each using a different interface and routed through a different path in the network. In practice, MPTCP is a TCP connection that uses TCP options to enable multipath functionality without requiring any changes at the application level. Hence, for a given application, an MPTCP connection behaves exactly like a regular TCP connection.

In MPTCP, the initial 3-way handshake consists of a SYN, a SYN/ACK and an ACK, as in the regular TCP. The difference with MPTCP is that each party asks the other party through an `MP_CAPABLE` TCP option whether it supports MPTCP. At this stage, they also share their keys in cleartext in order to identify and

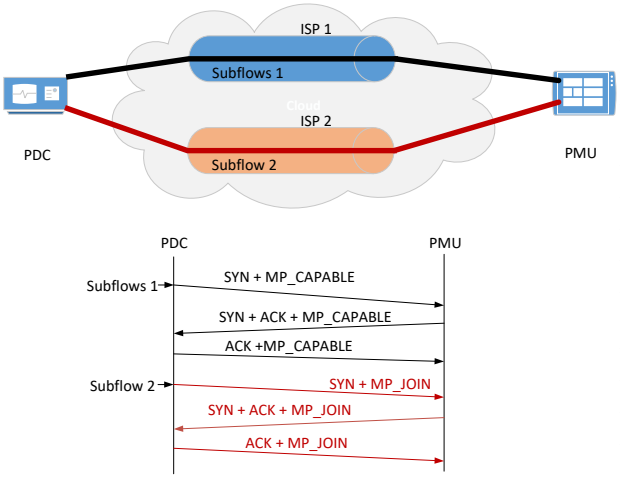


Figure 2: MPTCP connection

authenticate future subflows for the connection. This handshake and the subflows are depicted in Fig. 2.

Each subflow is identified with a 4-tuple of <source address/port, destination address/ port>, which is created after the initial MPTCP handshake and exchange of keys. To add new subflows into an existing connection, a token derived from the initial key and `MP_JOIN` in the TCP options are used in the handshake process of the new subflows, as illustrated in Fig. 2 [6].

Note that each subflow has its respective sequence numbers similar to a regular TCP connection. In addition, the specification of MPTCP identifies a different sequence number that interrelate packets delivered over multiple subflows within a single MPTCP connection [6].

#### 2.2.1. *Comparison between MPTCP and other Multipath Transport Protocols*

MPTCP is not the only solution for multipath reliable transmission. There are other mechanisms for multipath transmissions such as MCTCP (Multi Connection TCP) [7], CMT-SCTP (Concurrent Multipath Transfer for SCTP) [8], R-MTP (Reliable Multiplexing Transport Protocol) [9], etc.

However, switching to CMT-SCTP causes a pain for TCP applications due to the requirement of programmers' learning a new API with different semantics. R-MTP focuses on channel aggregation in mobile devices by using multiple link-layer technologies but not end to end different connections. Therefore, employing these two technologies for WAMS applications is not efficient and feasible.

On the other hand, MCTCP provides very similar features to MPTCP. The difference between these two similar technologies are reported in [7] as follows:

- MCTCP do not need to use TCP options, being present in many packets, as much as MPTCP, since it exchanges the control information in the payload. Thus, MCTCP exchanges control information without length limitation.
- Since TCP options is not used by MCTCP as much as MPTCP, its operation is more robust when considering middleboxes that strip, duplicate, or modify TCP options.
- In the case of multi-addressed hosts behind Network Address and Port Translation (NAPT) gateways, parsing and modifying MCTCPs control is much more complex than parsing TCP options for NAPT helper (stateful). This makes MPTCP easy to implement in the WAN.

#### 2.2.2. *The Advantages of Utilizing MPTCP and MCTCP in the Phasor Measurement Communication of WAMS*

High communication latency, resultant from a connection re-establishment of TCP due to a broken or stalled connection, can violate the latency requirements of phasor measurements [10]. In contrast for MPTCP, when the first subflow is initialized to transmit phasor measurements, the other subflows are created concurrently. Since one of the MPTCP subflows used to transmit the measurements is likely functioning normally (with high likelihood), thus the overall phasor measurement traffic is not disturbed or delayed.

Moreover, MPTCP provides a higher network utilization and a fairer allocation of resources to subflows by efficiently addressing the congestion response of the corresponding subflows. The detailed advantages of MPTCP-based networks appear in [3].

On the other hand, MCTCP can provide the advantages aforementioned, supported by MPTCP for WAMS applications. Moreover, minimal requirement for kernel-layer change makes MCTCP easy to implement for WAMS applications. However, we select MPTCP to implement our approach due to the following reasons: 1-) MPTCP is a more established multipath transport protocol, since more researchers work on it in addition to its many real-world usage. 2-) MPTCP API supports opening new subflows on defined addresses and closing the subflows anytime, which enables us to

implement our stream hopping approaches. 3-) MCTCP involves a initiator connection that keeps fixed IP addresses and port numbers during the lifetime of the session. This violates our main target, which is periodically change of all addresses/port numbers of the connection to hide them from the attacker launching DDoS attack.

## 3. System and Security Models

In this section, we first present the SG system and threat models. Subsequently, we outline the potential compromise of SG devices and the resultant security vulnerabilities in the SG networks. We also discuss the deficiencies of current intrusion detection systems to detect these threats.

### *3.1. System Model*

Similar to contemporary SG models, we consider that the power utility employs private networks to construct a SG wide area network (WAN) for cost-effectiveness and applications availability. For WAN, the utilities could use the links leased from the carriers and also dedicated network links. WAN is typically used not only for various kinds of WAMS devices but also for different types of SG devices such as Smart Meters.

In addition, we assume that gateway-to-gateway (versus host-to-host) virtual private networks (VPNs) exist in the WAN to provide secure channels. Thus, every node at a given local area network can access the other local area networks only through the gateway-to-gateway tunnels [1].

In the geographically demarcated SG operational area where the WAMS acquire the state measurement data, some SG devices might be compromised by exploiting the vulnerabilities. The compromised devices could grant the attackers elevated privileges for overwhelming the devices resources, as illustrated in Fig. 3.

We consider that both the PMUs and the PDCs support the IEC 61850-90-5 standard to provide MPTCP connection authentication through the standardized key distribution center (KDC) [11]. IEC 61850-90-5 recommends UDP for data transmission of WAMS as a transport layer protocol due to its a lightweight mechanism [11]. However, in this work, we employ MPTCP for the data transmission and show that it provides similar performance characteristics to UDP for phasor measurement traffic.

### *3.2. Attack and Threat Model*

Our threat model covers two types of Denial-of-Service attacks, namely: (1) transport layer attacks, where the adversary consumes the device's processing and networking resources by exploiting protocols vulnerabilities, and (2) application layer attacks, which exploit the vulnerability of the application to saturate the device resources. However, our approach is not designed to counter transport layer flooding attacks that saturate the link bandwidth.

In our threat model, the attackers are malicious entities which are compromised devices able to access the WAN (Intranet) where the phasor measurement devices are located. Furthermore, the malicious devices are assumed to have the ability to launch DoS/DDoS attacks to saturate the resources of PDCs and PMUs if the attackers can discover the open port numbers. In addition, we do not trust the devices inside the WAN. We preclude the case of an insider attacker physically accessing the phasor measurement devices.

### *3.3. Compromise of SG Devices*

The deployment of devices in a wide geographical area makes it difficult to protect them from being physically compromised. This is often observed in devices used for monitoring the grid where an attacker can access the physical devices and compromise them. For example, a house owner can have full physical access to many deployed devices e.g., smart meter [12].

The device can be compromised either by using login credentials or by exploiting a vulnerability. 1) Login credentials can be obtained using: social engineering, side channel attacks, eavesdropping (unprotected communication), and passwords guessing, and 2) Identifying a vulnerability is possible for an attacker either by buying zero-day exploits or by scanning the device. The attacker also needs to develop an exploit code using the vulnerability to plant malware on the device to exploit it. In addition, to compromise the devices, the attacker can also directly connect to the local network behind the firewall that the devices are connected to [13].

As the compromised nodes act similar to the normal nodes, such "internal" attacks pose a higher threat potentially leading to significant damages to the SG communication network and even to the control system of power network. As a result, the compromised nodes can be exploited by different malware or viruses attacking critical SG devices [12].

In particular, the SG can be significantly affected by DoS/DDoS attacks since it heavily depends on the availability of the communication network. In this paper, we mainly focus on internal DoS/DDoS attacks in WAN networks where the attackers use the malicious devices inside a WAN to launch DoS/DDoS attacks on critical

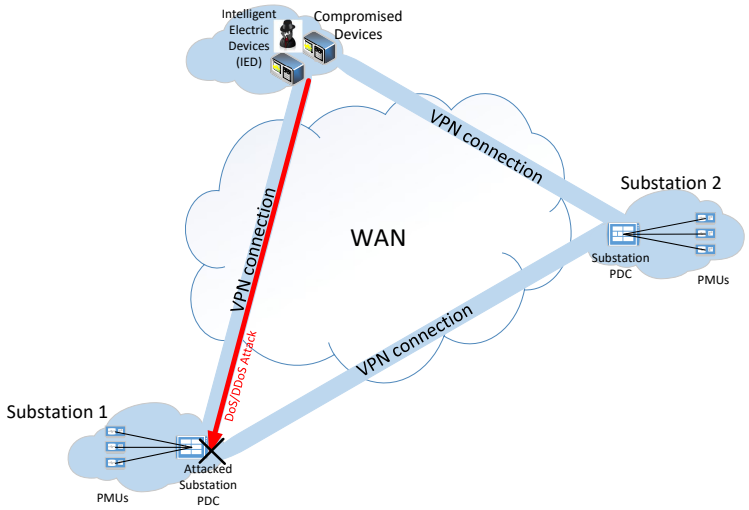


Figure 3: Illustration of Network and Attack Models

SG devices (i.e., PDCs or PMUs) to induce data transmission delays or block data delivery [12].

### 3.4. Security Vulnerabilities of WAMS

We outline a study conducted on a testbed using real WAMS devices [14] to highlight their security vulnerabilities.

Morris et al. [14] conducted tests to evaluate the vulnerability of PMUs and PDCs in terms of the attacks originating from inside a WAN by building a testbed consisting of PMUs, PDCs, a router and a Network Analyzer [14]. They launched TCP flooding (SYN and FIN) and UDP garbage flooding attacks on the devices for both specific and also random ports. The test results showed that all devices under flooding attacks are eventually overwhelmed and start to deny service when the traffic volume increases beyond the data processing ability of the device.

Based on the collected results, the authors of [14] suggestion to mitigate these issues is that utilities should be enabled to monitor the volume of the network traffic in order to detect and/or limit transmission of the traffic to the devices. Moreover, the fuzzing tests conducted in [14] show that even individual packets can result in device failures i.e., resetting the devices.

These test results indicated that DoS/DDoS attacks can be a serious threat to the safety and reliability of the power network. Such DoS/DDoS attacks can lead to partial loss of availability, and thus leading to the incorrect state estimation of the power network, or, impediments to the mitigation on power system failures. For this reason, a proactive defense mechanism needs to be employed to mitigate the DoS/DDoS attacks for WAMS.

### 3.5. Deficiencies in Intrusion Detection Systems

For providing security protection to IT infrastructures, the traditional security solutions, e.g, firewalls, intrusion detection systems (IDS), or Virtual Private Networks (VPN), are both common and efficient. However, as SG devices are typically resource constrained (computational, bandwidth, memory), the direct adoption of these IT-level security solutions is not practical [15].

Typical IT servers need stronger security protection than the edges/clients. However, in SG communication networks, the control center servers and edge nodes (e.g., relays, circuit breakers) require the same level of security, since the edge nodes can also pose safety similar to that of the servers. Moreover, given that SG devices have constrained resources, directly utilizing the IT-based DDoS defense/authentication mechanisms might not provide the expected security protection for the SG applications. Therefore, lightweight and proactive DDoS protection mechanisms are desired for securing SG communication networks [15].

Moreover, the classical Intrusion Detection Systems (IDS) or Intrusion Prevention Systems (IPS) are not adequate for guaranteeing SG communication security. SG communication systems have also inherited many new challenges and security threats from its own machine to machine communication structures and other issues of computer networking technologies. For this reason,

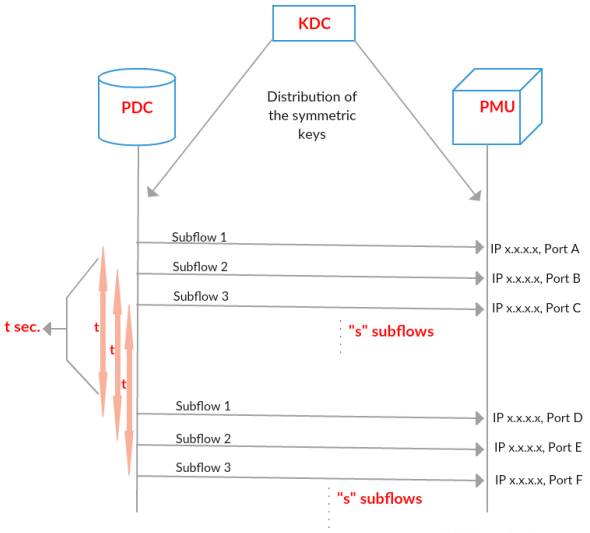


Figure 4: Stream hopping of MPTCP-H

the IDS systems designed for SG communication have to address the issue of handling resource-frugal devices over both traditional computer networks and M2M networks [12].

Based on this background, we now present our proposed approach that provides efficient defense against the transport and application layer DoS attacks on WAMS.

## 4. MPTCP-H Architecture

The MPTCP-extension (MPTCP-H) aims to provide proactive protection against the transport and application layer DoS attacks. The main idea behind MPTCP-H is to employ a stream hopping mechanism alongside multipath functionality of MPTCP. In order to achieve that, MPTCP-H develops two innovations:

1. Stream Hopping, where subflows are switched over random ports which increases the attack cost, unlike in the typical fixed MPTCP flow.
2. Authentication, which handles the authentication between the PMU and the PDC whenever a new connection and subflow is created.

### *4.1. The Stream Hopping Technique*

The traditional security systems such as firewalls, IDS and IPS are unsatisfactory to defend phasor measurement traffic against DoS/DDoS attacks due to their passive and unaccomplished structure. In existing IT systems, the continuous change of network attack type gives an advantage to the attackers over the protection systems. The malicious attacker is in the dark side, while the protector is in the bright side. Therefore, the adversary solely requires discovery of a few vulnerabilities whereas the protector must guarantee that the system does not have any exploitable vulnerabilities [16].

To address the advantage of attackers over the protectors, moving target defense (MTD) methods have been proposed [17]. This mechanism is a new proactive defense method in which the protector constantly changes the attack surface of the system to boost the cost of an successful attack for the attacker. Port hopping [18, 19] is a specific MTD method that periodically switches a port of a service in a pseudorandom manner, confusing potential intruders. The port hopping mechanism facilitates both the detection and filtering of unauthenticated packets and does not need require changes in the existing systems and protocols [16].

However, this port hopping scheme requires all clients to know a secret key used by the server to calculate the port number for the current time slot. In the case of disclosure of the secret key, the open port of the devices can be direct target of DoS/DDoS attacks, which exposes high security risks for WAMS. Furthermore, the implementation of the port hopping technique is not practically feasible for TCP connections.

On the other hand, MPTCP allows simultaneous use of $s$ subflows over different paths[2] to distribute data across these subflows, while maintaining a standard TCP interface for the applications. This characteristic of the MPTCP connection enables the implementation of a port hopping-like technique, called stream hopping, by periodically switching the subflows over different IP-addresses/interfaces[3].

#### *4.1.1. Subflow Switch*

To realize the stream hopping technique of MPTCP-H, we extend the functionality of MPTCP by periodically opening new subflows that use different paths, each of which is used for an allocated time period $t$. In

[2] In this work, a path between a sender and a receiver is defined by a 4-tuple of source and destination address/port pairs. Changing one of the tuples creates a new path. We interchangeably use the subflow and path terms.

[3] Moreover, in MPTCP, the single-homed nodes can create subflows over different port numbers of IP-addresses pair using MPTCP "ndiffport" path manager [20]. Since PMUs are single-homed devices, for each new subflow we use different port numbers but the same pair of IP-addresses. Furthermore, MPTCP provides higher performance and robustness than normal TCP when the number of subflows per pair of IP addresses gets increased [21]. The reason for the performance improvement is the utilization of available network paths in an efficient manner.

MPTCP-H, only PDC is allowed to initiate $s$ new subflows using TCP-like handshake. The periodic subflow switching of MPTCP-H is illustrated in Fig. 4. After establishing an MPTCP connection with a PMU, the PDC opens new subflows by selecting new random port numbers on its side. To establish a new subflow, the PDC periodically sends a SYN packet containing an `MP_JOIN` option to the PMU. After checking the authentication of the new subflow, the PMU acknowledges the SYN with the same type of message (`MP_JOIN`) and binds the new subflow to the MPTCP connection. The three-way handshake ends with the acknowledgement message of the PDC.

MPTCP-H also allows a given PMU to randomly select new port numbers on their side for new subflows establishment. In order to do this, each PMU periodically hands over the selected port numbers to the PDC, such that the PDC can use them to connect to the PMU. To this end, PMUs transmit a `ADD_ADDR`/`REMOVE_ADDR` message through an existing subflow, which informs the PDC of the PMU's alternative existing addresses/no longer existing addresses, respectively. The PDC initiates new subflows over the delivered port numbers of each PMU by performing a three-way handshake carrying `MP_JOIN` command as illustrated in Fig. 2. Subsequently, the expired subflows are closed by sending `FIN`. This periodic switching of subflows is the basis for the subflow hopping technique which makes reconnaissance of the victim's address difficult for attacker.

#### *4.1.2. Phase Shift*

To keep the renewing period of subflows shorter than the attacker's subflow port number reconnaissance time, MPTCP-H creates multiple subflows with $t/s$ phase shifts versus multiple subflows activated for the same time period $t$. In Fig. 5, stream hopping in conjunction with the phase shift is depicted where each shaded bar represents a subflow of the active connection ($s = 3$) at a particular point in time. Each subflow is active for the allocated time $t$ and is substituted with a new subflow with a new port number when the allocated time expires. The renovation of the subflows do not overlap each other, but take place with a $t/s$ phase shift. By doing so, we assure the MPTCP-H connection of having a subflow initialized within a period of time not exceeding $t/s$ at each instance. In addition, by finely calibrating the number of the subflows $s$ on $t/s$, depending on the attacker's the reconnaissance time, we can assure that the MPTCP-H connections have a functional subflow throughout the attack duration. The reason is that, throughout the attack, there is a subflow whose lifetime is shorter than the $t/s$ which is the time for the reconnaissance of a subflow by attacker.

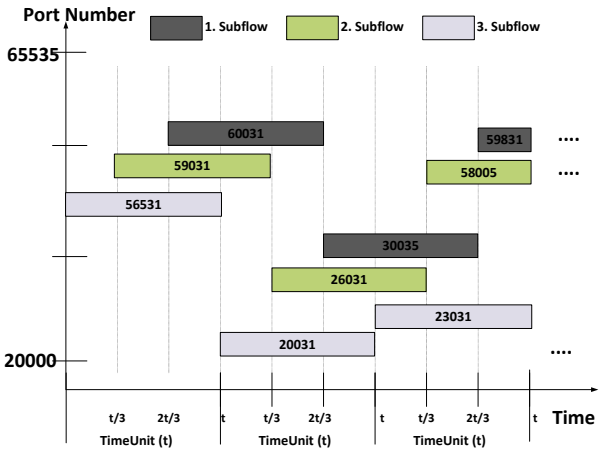


Figure 5: Phase Shift of MPTCP-H

#### *4.1.3. Attack-resistance*

The shuffling of the active port numbers (and the subflows) increases the difficulty for an attacker who discovers the port number of subflows through port scanning to launch connection-flooding attacks. As the subflows expire after the allocated time, the possible maximum damage caused by an attacker who discovers the port numbers of the subflows is limited to that specific time duration. As new subflows get activated, the attacker must guess or once again scan the port numbers for the new subflows to maintain the attack. This limits the attacker to mount persistent attacks on the active ports or forces them to blindly guess or aggressively scan the active ports. The consequence of either is the limited damage potential from an attack.

Furthermore, as PMU and PDC randomly and separately choose their next ports, MPTCP-H does not need a shared secret key to determine the port number while opening a new subflow, unlike existing pseudorandom port hopping mechanisms. This protects the system from the effects of a probable shared key disclosure.

In MPTCP, allowing only one side to initiate new subflows is possible and we delegate this responsibility to PDCs. Since the PDCs typically have higher importance than a single PMU, MPTCP-H configures PDCs to initiate new subflows. Therefore, even if an attacker uncovers the varying open port numbers to some extent, he is unable to saturate the PDC resources by sending forged messages to initiate new subflows.

The proposed stream hopping mechanism of MPTCP-H is akin to Frequency Hopping Spread Spec-

trum (FHSS) [22] technique which enables secure radio communication. If an attacker plans to jam or decipher the radio signal in FHSS, he needs to discover the hopping sequence or monitor the entire wide frequency band to capture the signal. Likewise, the subflow hopping of MPTCP-H has the same impact - increasing the difficulty for the attacker by changing port number over time. In addition, when DoS/DDoS attacks take place, the data traffic can be distributed or duplicated over several subflows for redundancy/resiliency.

#### 4.1.4. Performance Consideration

Since MPTCP-H requires frequent opening and closing of subflows (TCP connections), a probable degradation in the performance and throughput of the system should be considered. Firstly, we introduce an equation that calculates the additional data traffic overhead (per second) of MPTCP-H:

$$\begin{aligned} \textbf{Message Overhead} = \\ s * 1/t * (4 * handshake\ message\ (MP\_JOIN) \\ +4 * FIN\ message) + ADD\_ADDR\ message \\ +REMOVE\_ADDR\ message * 1/t \end{aligned} \quad (1)$$

As seen in the equation (1), $t$ and $s$ are key factors in the calculation of the overhead. We present two scenarios to show their effects on the overhead. Then, we assess the scenarios' results to see how to properly calibrate the factors' values.

*The first scenario:* If $t$ is equal to 1 second, $s$ is 10 subflows, and the packet length is equal or greater than 40 bytes in the equation (1), then the overhead is 3280 bps (between a PDC and a PMU).

*The second scenario:* If t is equal to 5 seconds, $s$ is 5 subflows, and the packet length is equal or greater than 40 bytes in the equation (1), then the overhead is 326 bps (between a PDC and a PMU).

Considering the second scenario, if there are 40 PMUs that connect to a PDC, $40 * 326/2kbps = 6.48kbps$ inbound traffic and $40 * 326/2\ kbps = 6.48\ kbps$ outbound traffic (overhead) are created by MPTCP-H.

To compare the overhead with the measurement traffic, we need to calculate the max PMUs traffic for a PDC: $40\ PMUs * 70 < bytes\ (packet\ size) * 120fps = 336\ kbps$

When we compare the overhead of the second scenario (4.32 kbps) with the inbound traffic of PDC (336 kbps), we see that MPTCP-H introduces a DDoS mitigation mechanism at the expense of a reasonable overhead (14.5%). In addition, it is worth noting that the difference between the first scenario and the second scenario indicates that decreasing $t$ and rising $s$ sharply boost the total overhead, meaning the calibration of those values has high importance for obtaining the minimal overhead with the required security.

Furthermore, as detailed in the evaluation section, we did not observe any perturbation in the system performance while frequently switching the subflows (TCP connections).

### 4.2. Authentication for Initiating New Subflows

A MPTCP connection is initiated by exchanging initial keys that are used to authenticate new subflows for the connection. However, no secure mechanism is declared by the MPTCP specification for the exchange of the initial keys. IEC 61850-90-5 specifies the key distribution center (KDC) [11], which introduces a symmetric key coordination between the publishers and subscribers (i.e., PMU-PDC).

To provide secure authentication, we use keys provided by KDC instead of the initial keys. The idea is akin to the one reported in [23], where application-layer keys (SSL/TSL) are proposed to be used for the authentication.

By using an application-layer key, i.e., the KDC keys, instead of the initial keys exchanged inside the cleartext, we address the existing MPTCP's security issue related to key disclosure. By doing so, PMUs and PDCs become more robust against JOIN-flooding attacks.

On the other hand, since MPTCP-H provides long-duration connection for phasor measurement systems, and placement of the phasor measurement systems does not frequently change in the communication network, we consider a network management system (NMS) that opens a temporary port for the first connection between PMU and PDC. By doing so, phasor measurement devises (PMU and PDC) can be protected from DoS/DDoS attacks against the static open port that is necessary for the first connection.

Moreover, MPTCP-H secures the handshake process of establishing new subflows as follows: When initiating a new subflow, the PDC transmits the initial synchronization message including a 32-bit token which is a cryptographic hash of the PDC's initial (KDC) key, produced by the SHA-1 algorithm, and truncated to the most significant 32 bits. This token is used to associate the subflows to the MPTCP connection and also provide the security mechanism to block unauthenticated new subflows initiated by attackers [6].

Upon receiving a SYN that contains an `MP_JOIN` option, a valid token, and a random number, the

PDC responds by sending a SYN/ACK including an MP_JOIN option, a random number, and a truncated (leftmost 64 bits) Hash-based Message Authentication Code (HMAC). Finally, following the PDC's transmission of an ACK with a HMAC, the PMU sends an ACK to the PDC, which makes the connection ready for data transfer. The random numbers (nonces) averts replay attacks on the authentication method. The HMAC exchange along with the random number secures the establishment process, since if the HMAC is incorrect, the connection is refused [6].

## 5. Security Analysis of MPTCP-H

We now present the threat scenarios and the related security analysis for the proposed MPTCP-H technique.

Computer network attacks can be categorized as: (i) active attacks, and (ii) passive attacks. An active attack involves the exploitation of compromised data or devices to mount attacks on the network, such as data injection, data modification or packet drop attacks. In a passive attack, the attacker needs to collect critical information on the network and to learn network properties or transmitted data by using attack types such as sniffing or eavesdropping. Passive attacks are widely employed to collect information paving the way for an active attack [13].

The SG can be targeted to induce a power outage which can be performed by portioning the power grid. The power grid portioning can be carried out in cyber means, by intentionally transmitting a trip command to a circuit breaker (CB). Triggering trip commands can be accomplished by launching the following active attacks: 1) directly compromising the CB; 2) prompting a wrong control decision at the central controller which sends a trip message to the CB; or 3) changing the controller commands while they are on the path between CB and the central controller [13].

As we focus on the security of phasor measurement traffic between PMU and PDC in this work, the second method is the most probable to be used by an attacker to conduct an attack on the grid after gathering critical information using passive attack methods. The attacker can cause an incorrect control decision in the controller by perturbing the phasor measurement traffic, providing information about the state of the grid. To accomplish this, the attacker mounts a DoS/DDoS attack against the open ports of either the PMU generating the measurements or the PDC processing those measurements. However, since MPTCP-H reshuffles the open ports, the attacker must guess or discover the open ports to launch a DoS/DDoS attack. A blind attacker is very unlikely to realize a successful attack by randomly selecting a port number and flooding garbage data to affect the phasor's operation. Even if the attacker successfully guesses or discovers the open port, the available time for attacking is limited, since after the allocated time $t$, the ports get shuffled. In the case of maintaining a DOS/DDoS attack against the discovered open ports, the attacker has to continually scan the ports of the devices and continually adapt its attack according to the periodically varying port numbers of the subflows. This makes conducting an efficient attack a difficult task for the attacker, making MPTCP-H a successful mitigation technique against such attacks.

Another threat includes the compromising of the KDC keys in the exchange of the initial key. These devices have scarce resources and can be saturated using a relatively small number of malicious authenticated connection requests by the attacker. Therefore, exposing the open port numbers for a short time would be enough to overwhelm the service of the devices. To protect the PDCs, carrying more importance than PMUs, from the above mentioned attack, MPTCP-H grants the right of opening new subflows to the PDCs. Thus, the PDCs are able to refuse any requests to open new subflows and protect their resources from being depleted by the attacker. A complementary scheme that adds protection on the keys can also be included in MPTCP-H.

Configuring PMUs to accept traffic only from the PDCs (and vice versa) also represents a suitable defense approach for the PMUs. This can be achieved through a white-listing approach that provides the PMUs (or PDCs) with a list of the authorized PDCs (or PMUs). For an attacker spoofing the IP addresses, MPTCP-H renders such a DoS attack to become unlikely by periodically varying the MPTCP subflows using new port numbers. To do so, each subflow is continuously recreated after some lifetime $t$ using new port numbers. This introduces a defense against threats related to attacker spoofing the IP address to consume the target's resources by transmitting forged packets to its open ports.

MPTCP inherently introduces new challenges for the traditional security approaches, making them no longer sufficient for MPTCP. For instance, since an IDS monitors and categorizes the traffic of a connection based on the 5-tuple, it sees the subflows of an MPTCP connection as an independent TCP connection, and thus cannot discover the correlation to reassemble MPTCP traffic correctly. Moreover, MPTCP enabling a sender to employ all available routes at the same time causes the fragmentation of data among the routes. For this reason, an IDS cannot have adequate knowledge on any of the streams to detect the malicious data, which leads to an

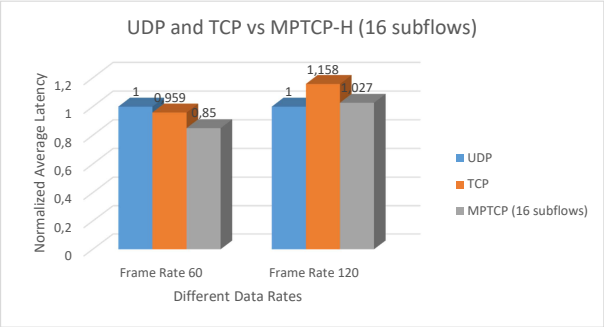


Figure 6: Normalized latency of MPTCP-H (4 network interfaces with 16 subflows), UDP and TCP in the WAN built on the NorNet

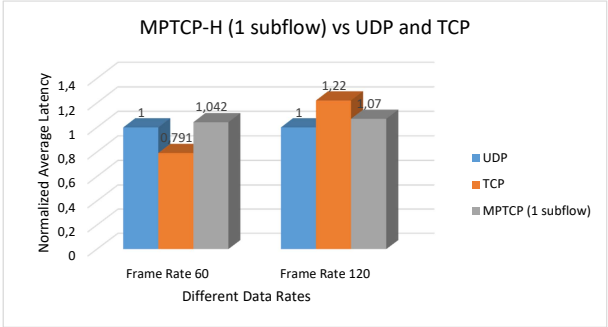


Figure 7: Normalized latency of MPTCP-H (1 network interface with 1 subflow), UDP and TCP in the WAN built on the NorNet

exploitable vulnerability for cross-path data fragmentation attacks. Z. Afzal [17] investigates possible attacks using these vulnerabilities and introduces solutions to address them.

Overall, MPTCP-H constitutes a proactive defense mechanism for time-critical communications. We opted for a proactive mechanism vs. a reactive mechanism, as deploying a reactive approach e.g., Intrusion Detection Systems (IDSs) would consume more time for mitigation. Reactive mechanisms have to detect the attacker at first and then report the attack to the systems or administrators for prevention. Moreover, a careful placement of IDSs in the network is required to detect internal attacks. Still, MPTCP-H can be used complementary to an IDS.

## 6. MPTCP-H Implementation

For the implementation of our mechanism we use the Linux Kernel implementation of Multipath-TCP (mptcp_v0.91) [20] which is the reference and most common implementation of IETF [6]. We implement our MPTCP-H mechanism using the Enhanced Socket API of B. Hesmans et al.[24], which enables us to have control over individual subflows. This API allows us to open new subflows with custom IP addresses/port numbers and closing them whenever needed. G. Demaude and P. Ortegat [25] develop a Java Native Interface (JNI) tool, which enables us to use Java language to manage the Native C socket API. In the implementation of MPTCP-H on a Virtual Machine (the Linux Kernel with mptcp_v0.91), we manage the native C socket API with the above mentioned tools.

In our implementation, while PMU runs on the host (physical computer), PDC runs on a Virtual Machine. In WAMS, the phasor measurement traffic between a PMU and PDC is similar to a server-client model. The PMU acts as a server by sending measurement messages each time the PDC (the client) transmits a request message for the measurement. To implement this scenario, we develop a middleware between the application layer and MPTCP stack in the client side for MPTCP-H, and provide two applications acting as PMU-PDC in client and server sides. After establishing a MPTCP connection, the PDC (client) additionally opens a fixed number of Multipath-TCP subflows *s* for the connection. The subflows are periodically switched by the PDC (client). In other words, the subflows are closed over time and replaced with new subflows. Each of the new subflows is created with a random port number as explained in Section 4.1. The implementation of the idea and threat model are fulfilled by Ferdaus Nayyer during his master thesis as a joint work.

## 7. MPTCP-H Evaluation

As the proposed defense mechanism is targeted at time-sensitive critical WAMS applications, we need to particularly assess the system availability and the overhead, in terms of additional latency and message. Thus, we employ three metrics in the evaluation of the approach: (1) the system availability, (2) the latency, and (3) the overhead messages caused by MPTCP-H. Firstly, in Section 7.1, we evaluate our approach regarding the second and the third metrics, i.e., latency and message overhead, in attack-free conditions by testing our approach in WAN in the case of different network topologies and data rates. Secondly, in Section 7.2, we test MPTCP-H under both DoS attack and attack-free conditions in terms of the system availability (the first metric) and additional latency (the second metric) by comparing TCP. In this paper, network availability

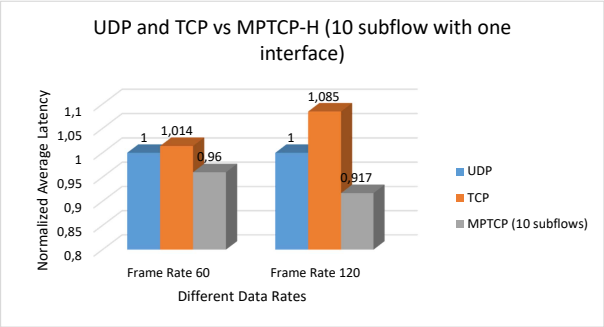


Figure 8: Normalized latency of MPTCP-H (10 subflows in one network interface), UDP and TCP in the WAN built on the NorNet

refers to the success rate of timely delivery of phasor measurement messages from PMU to PDC.

### *7.1. Attack-free conditions*

In the following sections we evaluate our approaches under DoS attack conditions.

#### *7.1.1. Latency Assessment for MPTCP-H*

To assess the impact of our approach on latency in a WAN, the NorNet testbed is used to create the WAN, which provides realistic results [26]. The WAN consists of a collection of multihomed nodes of the NorNet distributed throughout Norway. Two nodes with 2-3 network connections representing a PMU and PDC are driven by daemons. In our experiments evaluating the impact on latency, three representative types of PMU-PDC topologies are implemented in the WAN: 1) 4 network interfaces for both PMU and PDC, and 16 subflows (full-mesh), 2) a single network interface for both PMU and PDC and a single subflow, and 3) a single network interface for both PMU and PDC but multiple subflows.

We utilize two different data rates (60 fps and 120 fps) in each experiment to simulate realistic phasor measurement traffic of WAMS in the WAN. As the measurement traffic of WAMS typically has proscribed data rates, we evaluate the proposed approach regarding induced latency or congestion rather than throughput of the system.

According to IEEE C37.118.2-2011, Synchrophasor measurement traffic can be transmitted over TCP/IP or UDP/IP. UDP provides faster data delivery given its lightweight characteristics [2]. We compare the proposed approach with TCP and UDP in the transmission of Synchrophasor measurements to assess its performance.

Fig.6 presents the normalized average latency versus data rates for varied protocols. The latency values are normalized by utilizing the latency of UDP as a base - as suggested for Synchrophasor data transfer by the IEEE Standard for Power Systems C37.118.2-2011 [2]. Fig. 6 shows that MPTCP-H introduces less latency than TCP (and even UDP) in transmitting 60 frames per second (fps). On the other hand, for the 120 fps data rate, while TCP provides the worst latency, UDP outperforms MPTCP-H in terms of latency. We see from Fig.6 that TCP's latency is relatively low for the data rates of 60 fps due to its congestion handling mechanisms. However, when the data rates are high (120fps), UDP's connectionless approach provides better latency than TCP. That being said, MPTCP-H with multiple subflows provides latency results close to UDP even in the case of high data rates (120 fps).

We also conducted experiments on single-homed PMU and PDC to analyse if MPTCP-H has any shortcomings in these scenarios. Fig.7 shows that while the latency results for TCP are similar to the results of the previous experiment, MPTCP-H's latency degrades slightly. However, the overall latency of MPTCP-H is still relatively close to the latency of the UDP for both data rates of 60 fps and 120 fps.

Finally, to demonstrate the effect of the port-based multiple subflows structure of the MPTCP-H on the latency, we conducted experiments that compare UDP and TCP with MPTCP-H that uses 10 subflows over single-homed PMU and PDC (with 1 network interface). Fig. 8 highlights that MPTCP-H does not introduce any additional latency, and, instead, decreases latency even when the data rate increases to 120 fps. TCP's latency increases with the data rate.

#### *7.1.2. Message Overhead of MPTCP-H*

To measure the additional overhead, we deploy a PMU and a PDC on a host and on Virtual Machines, respectively. In this work, while the message overhead refers to the protocol-specific message transmission, all traffic implies the message overhead plus the application layer message transmission. To calculate the message overhead, we run each experiment for 5 minutes with different hopping rates, number of the subflows, and application layer message rates, i.e, 4ms (250 fps), 8ms (120 fps), 16s (60 fps). Subsequently, we find the ratio of the overhead messages to the whole traffic for each run. We conduct our experiments in the fix time period (5 min), since phasor measurement traffic acts as a continuous data stream unlike typical web applications. By doing so, we find the additional message overhead in the case of phasor measurement traffic.

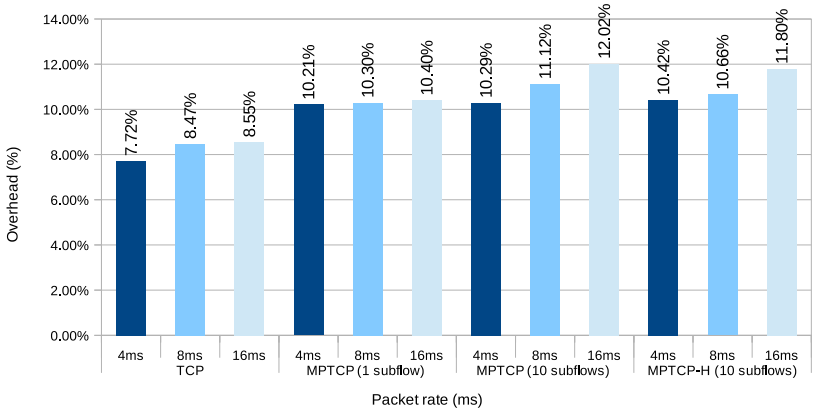


Figure 9: TCP, MPTCP vs MPTCP-H for message overhead

We first compare TCP, plain MPTCP, and MPTCP-H in terms of the additional message overhead, since TCP is recommended by IEEE standard C37.118.2 for phasor measurement traffic and is a reliable transportation protocol like MPTCP and MPTCP-H. Fig. 9 demonstrates that increasing the message rate causes a slight decrease in the message overhead ratio. The reason is that since the increase of application layer message rate does not lead to a linear raise in the message overhead of any protocols, the ratio of the overhead messages to all traffic decreases. In addition, we see that utilizing MPTCP (1 subflow) instead of TCP introduces around 2% of additional message overhead due to MPTCP's additional protocol messages. When we consider high capacity of contemporary network devices, this additional message overhead is reasonable for WAMS. Furthermore, we compare MPTCP (10 subflows) with MPTCP-H (10 subflows) to assess the message overhead caused by our mechanism. As seen in the Fig. 9, MPTCP-H does not introduce significant message overhead in comparison to the plain MPTCP. Moreover, it causes an additional 2% of message overhead compared to TCP, similar to plain MPTCP.

Fig. 10 shows that when the number of the subflows $s$ increases from 5 to 20, the message overhead also goes up to near 1%. The reason is that the increasing of the number of the subflows (sub-TCP connections) causes additional protocol-based message overhead. The results denote that the number of the subflows $s$ should be minimized due to the high overhead imposed by numerous PMUs in the network. On the other hand, involving a smaller number of subflows eases the discovery of the open ports as explained in Section 4.1. Therefore, $s$ should be adapted for different network topologies considering a probable adversary's attack coordination speediness and the trade-off between the $s$-related message overhead and the security consideration.

To show the effect of various hopping rates $t$ on the message overhead, we conduct experiments using 5 subflows in different hopping rates (time periods) $t$. The results indicate that reducing the time period of switching subflows slightly increases the message overhead, as illustrated in Fig. 11. However, the increase in message overhead is not as high as $s$. Therefore, we can select the shortest time period/hopping rate $t$ without considering the message overhead.

Lastly, we assess the effect of both different hopping rates and packet rates on the message overhead. The results demonstrate that when the message rate is high (4ms), the ratio of the overhead messages is much lower than the one in the low message rate (16ms), as shown in the Fig. 12. This implies that a higher message rate does not lead to a significant message overhead in MPTCP-H. Moreover, the effect of different hopping rates is clearly seen at the low message rate due to existence of less application layer messages in the whole traffic at a low message rate. Even in the worst case ($t$ = 5s), the increase of the ratio of the message overhead is less than 1%.

#### *7.1.3. Comparison between IEEE C37.118.2 and IEC 61850-90-5 standards*

Although the IEEE standards C37.118.1/2 [2] specify Synchrophasor measurements and data transmissions respectively, IEC 61850 is the de-facto standard for specifying the substation and utility automation [11]. IEC 61850-90-5, addressing the transmission of Synchrophasor measurements, defines Sample Values (SV) and Generic Object Oriented Substation Events (GOOSE) as an Ethernet layer based real time commu-

Table 1: Comparison between IEEE C37.118.2 and IEC 61850-90-5 standards [11].

| **Features** | **IEEE C37.118.2** | **IEC 61850-90-5** |
|---|---|---|
| Protocol Stack | TCP or UDP | TCP or UDP |
| Sampling Rate | 10-30 samples/sec (for 50 Hz) | 4000-12800 samples/sec (for 50 Hz) |
| Security features | Provides a limited security for intrusion and vulnerable to attack | Although exchanging cryptographic keys among devices enables a strong security mechanism, availability is still an serious concern. |
| Streaming protocol | Yes | Yes (R-SV) |
| Average data word size | 112 bytes | 305 bytes |

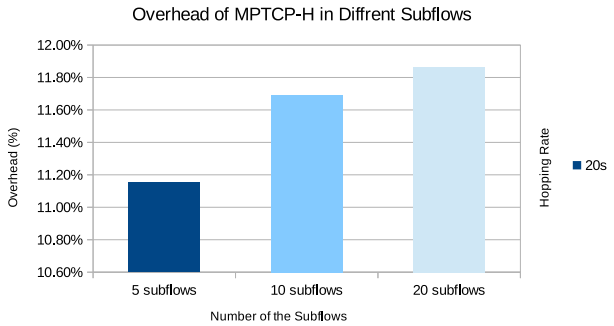


Figure 10: The effect of the number of subflows on the overhead

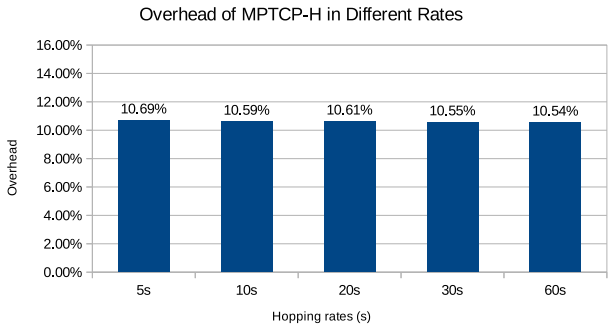


Figure 11: The effect of hopping rates on the overhead

nication services. For transmitting the PMU data over a wide area network (WAN) with SV and GOOSE, a transport layer routing service is required. As a result, the encapsulated routable SV and GOOSE messages transmitting over the network and transport layer are respectively termed as R-SV and R-GOOSE [11].

Although both the IEEE C37.118.2 and IEC 61850-90-5 standards recommend UDP or TCP for wide area measurements, UDP is usually preferred for WAMS due to its lightweight and unreliable mechanism. While the total packet size of a IEEE C37.118.2 is 112 bytes, the data word of IEC 61850-90-5 is found to be 305 bytes [11].

Whereas IEEE C37.118 does not address confidentiality issue, IEC 61850-90-5 achieves confidentiality by implementing the key distribution center (KDC), which provides the symmetric key coordination between the publishers and subscribers. Further, cyclic redundancy check (CRC) code used by IEEE C37.118 does not provide information authentication and integrity, whereas IEC 61850-90-5 uses digital signatures with asymmetric cryptography to provide the required security [11].

Availability is another very important security concern for WAMS, and enables uninterrupted communication between the publishers and subscribers. However, availability is not addressed in both IEEE C37.118.2 and IEC 61850-90-5 standards [11]. Table 1 demonstrates a comparison between IEEE C37.118.2 and IEC 61850-90-5 standards.

In Table 1, we can see that packet size of IEC 61850-90-5 is larger than packet size of IEEE C37.118.2, i.e., 112 bytes and 305 bytes respectively. However, since the packet size of IEC 61850-90-5 is not larger than the maximum Ethernet frame (1500 bytes), this issue does not introduce any problem our approach. Moreover, in Table 1, we can see that sampling rate of IEC 61850-90-5 is higher than sampling rate of IEEE C37.118.2, i.e., 10-30 samples/sec and 4000–12800 samples/sec respectively. In our all experiment, we see that when the date rate increases, our approach does not introduce any

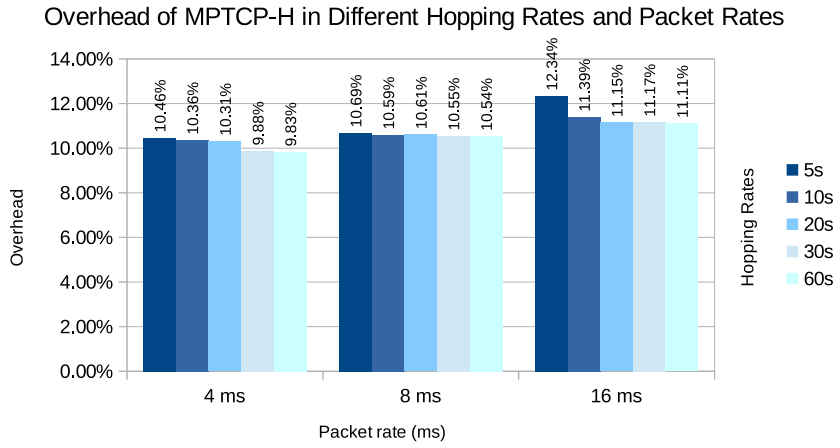


Figure 12: The effect of hopping rates and packet rates on the overhead

degradation. Therefore we do not expect any problem when IEC 61850-90-5 is used. However, to clarify this issue, we will implement IEC 61850-90-5 during the test of our approach against more complex DDoS attacks in our future work.

### 7.2. Under DoS attack conditions

In the following sections we assess our approach under DoS attack conditions. Since Nornet testbed does not allow us to launch DoS attack between nodes, we deploy our implementation scenario in our local network. To mount a DoS attack, we use Tcpkill tool.

#### 7.2.1. Assessment of the System Availability

We test the availability provided by MPTCP-H and TCP under the DoS attack. The availability refers to the successful delivery rate of the phasor measurements. The attack scenario in our evaluation is setup as follows: The attacker scans the all ports of the target (i.e., PDC or PMU) and then launches a SYN flooding attack against the ports for 5 minutes. We employ different phasor measurement rates, i.e., 250, 120 and 60 fps, while testing the availability of MPTCP-H and TCP under DoS attack.

Fig. 13 shows that under the DoS attack, MPTCP-H at a low data rate (60 fps) provides 100% availability. However, the provided availability degree decreases down to 92% with the increase of the data rates from 60 to 250 fps. The reason for this is that until the MPTCP-H switches subflows/ports under attack, mass amounts of data are transmitted in the high data rate scenarios, which can not be handled by the acknowledge mechanism of MPTCP-H. Alternatively, in Fig. 13 we see that TCP cannot provide more than 53% availability for any data rate when the PMU/PDC is under attack. Furthermore, with data rate increase, the provided availability degree sharply decreases around 10% like in the case of MPTCP-H.

#### 7.2.2. Evaluation the Additional Latency

As we target time-sensitive WAMS applications, we also assess our approach in terms of latency in both DoS attack and attack-free conditions. We run each experiment for the three phasor measurement rates.

Fig. 14 demonstrates that the DoS attack causes around 2 ms of additional latency for each data rate when the system uses MPTCP-H. However, as seen in Fig. 15, the DoS attack leads to more than 20 ms additional latency for TCP, which is not acceptable by most WAMS applications. Moreover, when we look at Fig. 15 and Fig. 14, it is clear that MPTCP-H does not cause any additional latency in attack-free cases in comparison to TCP.

*Summary*

The experiments for latency showed that MPTCP-H, with different network topologies, does not induce any additional latency for the phasor measurement traffic in WAMS in comparison to UDP, as recommended by the IEEE standard C37.118.2 and IEC 61850. Furthermore, using MPTCP instead of TCP introduces reasonable additional message overhead for the contemporary network devices. On the other hand, we test our approach under DoS attack conditions in terms of the system availability and latency. The results show that when the PMU/PDC is under DoS attack, whereas MPTCP-H

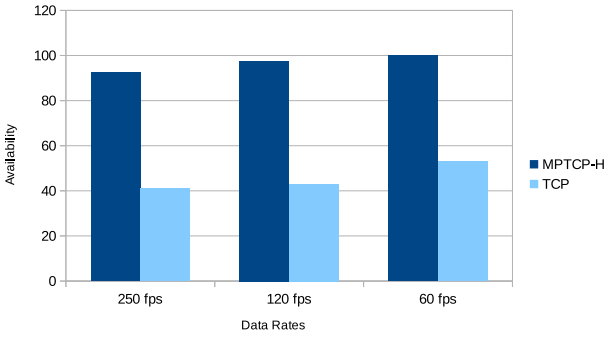


Figure 13: The system availability provided by MPTCP-H and TCP under DoS attack

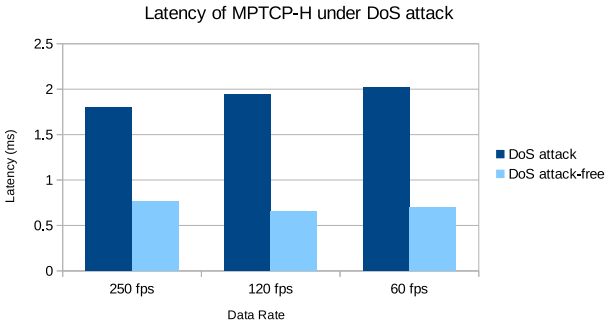


Figure 14: Latency of MPTCP-H under DoS attack

provides over 92% availability for each data rate, the availability provided by TCP is under 53%. In addition, while the DoS attack causes around 2 ms of additional latency for MPTCP-H, it leads to more than 20 ms of additional latency for TCP. Overall, we can see from the experiments that MPTCP-H provides a significant mitigation of the DoS/DDoS attack with a reasonable overhead.

## 8. Related Works

The authors in [18] proposed a random port hopping (RPH) technique where the server switches the UDP/TCP port numbers using two parameters (time and shared key) to a pseudo-random function. The authors in [19] highlights the operational difficulties from the clock drift problem, and proposes BiGWheel and HoPerAA algorithms to address the clock-drift issues for multiple servers and clients scenarios.

The alternate approaches [15, 16] based on port hopping do offer effective server-side protection against the application and transport layer DoS attacks. However, the emergent SG models require DoS attack protection on both server (PDC) and clients (PMUs) inside the substation network of the WAMS which is not possible using simplistic port hopping. Hence, based on the above considerations, we have proposed the MPTCP-H schema that achieves the protection for both server and clients by utilizing MPTCP's multipath function.

In addition, QUIC [27] is a reliable transport protocol that enables the communicating parties to combine multiple UDP-based sub-connections into a connection. Furthermore, QUIC allows changing the endpoint addresses (i.e., IP/Port) without breaking the connection. The proposed stream hopping approach can be adapted to make QUIC resilient against DoS attacks.

## 9. Conclusion

In this paper, we first surveyed the possible DoS attack threats against the WAMS (i.e., PMUs and PDCs). As a countermeasure against possible DoS attacks, we have proposed an MPTCP-extension, termed MPTCP-H, which basically switches the subflows by removing each subflow after a prescribed $t$ period and then by adding a new subflow with a new port. Thus, the proposed mechanism hides the session information from an attacker who is capable of scanning the ports.

As real-time delivery is a crucial requirement for the phasor measurement traffic, we evaluated the additional latency and message of our approach in comparison to

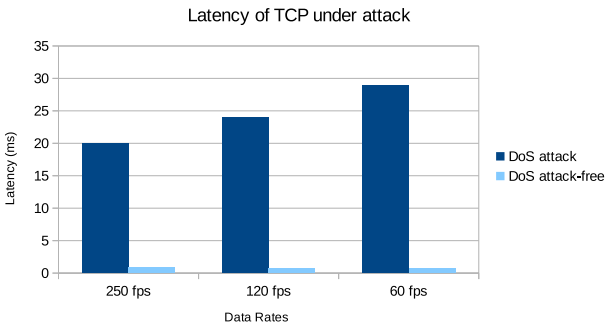


Figure 15: Latency of MPTCP-H under DoS attack

the standard UDP and TCP. The results show that our approach introduces a latency performance competitive even with the most lightweight transport protocol of UDP. In addition, MPTCP-H does not introduce any significant additional message overhead in comparison to plain MPTCP and TCP. Furthermore, the experiment results obtained under DoS attack scenario indicate that while MPTCP-H provides over 92% availability, TCP is not capable of providing an availability above 53%.

Moreover, we showed that MPTCP-H, with its lightweight mechanism, can significantly mitigate DoS attacks originating from inside the WAN. Overall, these results validate that MPTCP does not introduce significant additional overhead that can disturb the phasor measurement traffic whilst maintaining the protection against DoS attacks.

Moreover, we plan to test our approach under more sophisticated attacks where the attacker can continuously scan using powerful computers.

[1] D. M. Laverty, D. J. Morrow, R. Best, P. A. Crossley, Telecommunications for Smart Grid: Backhaul solutions for the distribution network, IEEE PES General Meeting (2010) 1–6.

[2] K. E. Martin, G. Brunello, M. G. Adamiak, G. Antonova, M. Begovic, G. Benmouyal, P. D. Bui, H. Falk, V. Gharpure, A. Goldstein, Y. Hu, C. Huntley, T. Kase, M. Kezunovic, A. Kulshrestha, Y. Lu, R. Midence, J. Murphy, M. Patel, F. Rahmatian, V. Skendzic, B. Vandiver, A. Zahid, An Overview of the IEEE Standard C37.118.2 Synchrophasor Data Transfer for Power Systems, IEEE Transactions on Smart Grid 5 (2014) 1980–1984.

[3] C. Raiciu, S. Barre, C. Pluntke, A. Greenhalgh, D. Wischik, M. Handley, C. Raiciu, S. Barre, C. Pluntke, A. Greenhalgh, D. Wischik, M. Handley, Improving datacenter performance and robustness with multipath TCP, Proc. of the ACM conference on SIGCOMM 41 (2011) 266.

[4] K. Demir, N. Suri, Towards DDoS Attack Resilient Wide Area Monitoring Systems, Proc. of the 12th International Conference on Availability, Reliability and Security (ARES ) (2017) 1–7.

[5] M. Kanabar, M. G. Adamiak, J. Rodrigues, Optimizing Wide Area Measurement System architectures with advancements in Phasor Data Concentrators (PDCs), Proc. of IEEE Power & Energy Society General Meeting (2013) 1–5.

[6] A. Ford, C. Raiciu, M. Handley, O. Bonaventure, TCP extensions for multipath operation with multiple addresses, IETF RFC 6824 (2013).

[7] M. Scharf, T. Banniza, MCTCP: A Multipath Transport Shim Layer, 2011 IEEE Global Telecommunications Conference - GLOBECOM 2011 (2011) 1–5.

[8] P. Amer, M. Becke, T. Dreibholz, N. Ekiz, J. Iyengar, P. Natarajan, R. Stewart, M. Tuexen, Load sharing for the stream control transmission protocol (sctp), IETF ID: draft-tuexen-tsvwg-sctp-multipath-06 (work in progress) (2013).

[9] L. Magalhaes, R. Kravets, Transport level mechanisms for bandwidth aggregation on mobile hosts, Proceedings Ninth International Conference on Network Protocols. ICNP 2001 (2001) 165–171.

[10] C. Paasch, S. Ferlin, O. Alay, O. Bonaventure, Experimental evaluation of multipath TCP schedulers, Proc. of the ACM SIGCOMM workshop on Capacity sharing workshop (CSWS ) (2014) 27–32.

[11] I. Ali, M. A. Aftab, S. M. S. Hussain, Performance comparison of IEC 61850-90-5 and IEEE C37.118.2 based wide area PMU communication networks, Journal of Modern Power Systems and Clean Energy 4 (2016) 487–495.

[12] R. Ahmad, A. Pathan, A Study on M2M (Machine to Machine) System and Communication: Its Security, Threats, and Intrusion Detection System, Security Solutions and Applied Cryptography in Smart Grid Communications (2017) 179–214.

[13] S. Paudel, P. Smith, T. Zseby, Attack Models for Advanced Persistent Threats in Smart Grid Wide Area Monitoring, Proc. of the 2nd Workshop on Cyber-Physical Security and Resilience in Smart Grids - CPSR-SG (2017) 61–66.

[14] T. Morris, S. Pan, J. Lewis, J. Moorhead, N. Younan, R. King, M. Freund, V. Madani, Cybersecurity risk testing of substation phasor measurement units and phasor data concentrators, Proc.of the Seventh Annual Workshop on Cyber Security and Information Intelligence Research (CSIIRW) (2011) 1–4.

[15] G. Badishi, A. Herzberg, I. Keidar, Keeping denial-of-service attackers in the dark, IEEE Transactions on Dependable and Secure Computing 4 (2007) 191–204.

[16] Y. Luo, B. Wang, G. Cai, Effectiveness of Port Hopping as a Moving Target Defense, Proc. of 7th International Conference on Security Technology (2014) 7–10.

[17] Z. Afzal, Towards Secure Multipath TCP Communication, Diss. Karlstads Universitet (2017).

[18] H. Lee, V. Thing, Port hopping for resilient networks, IEEE 60th Vehicular Technology Conference (VTC) (2004) 3291–3295.

[19] Z. Fu, M. Papatriantafilou, P. Tsigas, Mitigating distributed Denial of Service attacks in multiparty applications in the presence of clock drifts, IEEE Transactions on Dependable and Secure Computing 9 (2012) 401–413.

[20] C. Paasch, Multipath TCP in the Linux Kernel, http://www.multipath-tcp.org, Last visited on 23-04-2017 (2017).

[21] S. Zannettou, M. Sirivianos, F. Papadopoulos, Exploiting path diversity in datacenters using MPTCP-aware SDN, Proc. of IEEE Symposium on Computers and Communication (ISCC) (2016) 539–546.

[22] R. C. Dixon, Spread spectrum systems: with commercial applications, Wiley New York (1994).

[23] C. Paasch, O. Bonaventure, Securing the MultiPath TCP handshake with external keys, Work in Progress, draft-paasch-mptcp-ssl-00 (2012).

[24] B. Hesmans, A socket API to control Multipath TCP, https://tools.ietf.org/ html/draft-hesmans-mptcp-socket-00 Last accessed on 03-08-2017 (2017).

[25] G. Demaude, P. Ortegat, https://github.com/reirep/matcp-java.git, Last accessed on 03-08-2017 (2017).

[26] T. Dreibholz, The NorNet Testbed A Large-Scale Experiment Platform for Real-World Experiments with Multi-Homed Systems,, https://www.simula. no /research/projects/nornet (Last visited on 08-08-2017) (2015).

[27] R. Hamilton, J. Iyengar, I. Swett, A. Wilk, Quic: A udp-based secure and reliable transport for http/2, IETF, draft-tsvwg-quic-protocol-02 (2016).