Article

New Traceback Approach Deployment in Smart Mesh Microgrids against DoS Attacks

Mouna Gassara* and Bilel Gassara

[1] Digital Research Center of Sfax, University of Sfax, Tunisia; gas.bilel@yahoo.fr
*Corresponding author: gas.mouna@gmail.com

Abstract: Today's major challenge for smart Microgrids is to ensure the security of communications in a large number of changing data sets that are vulnerable to attacks by denial of services in constant evolution. The Internet Protocol Traceback defines a set of methods that help identify the source of an attack with minimal requirements for memory and processing. However, the concept of Traceback is not yet being used in smart Microgrids.
As a result, the main challenge of this article is to incorporate a new Traceback approach into the cybernetic system of a smart mesh Microgrid, which can be tested using a network simulator (NS-3) based on delay, debit, and packet loss rate parameters. In fact, the simulation results show the efficacy of this approach compared to others existing in the literature. Furthermore, using the proposed Traceback technique and the mesh nodes, we were able to create a smart meshed Microgrid. Moreover, using the Traceback approach given for merging Intel Galileo Gen.1 nodes with the Compex WLE200NX.11a/b/g/n to establish a secure test bench, which is deployed as a prototype at the Sfax Digital Research Center in Tunisia, we were able to create an intelligent Microgrid. In fact, by identifying all attack vectors and revealing their origins, we could boost the efficiency of our operation by 100%.

Keywords: IP traceback; smart mesh Microgrid; NS-3; real secure testbed

1. Introduction

The recent Smart Microgrids differ from the traditional power grids by their great flexibility to integrate increasing Distributed Energy Resources (DERs) [1], artificial intelligence and communications and information technologies evolving to cyber-physical systems.

However, through the exhaustion of communicational and computational resources, the Denial of Service (DoS) assaults in these systems prevents measurement availability and controls signals. As a result, numerous academics have looked into how to defend Microgrids against the DoS assaults [2]. In fact, Jianzhe Liu et al. [3] advocated that the disturbance effects of the DoS be linked to variations of pure physical model parameters with the development of a sufficient condition to assure a system power balance in the cyber layer. For their part, Jiahong Dai et al. [4] proposed a cyber-resilience strategy based on dynamic priority scheduling and a side-channel detector for detecting and mitigating DoS assaults in Microgrids. Another solution against cyber-attacks was proposed by Ahmad Saad et al [5]; it offers a digital twin (DT) based IoT interacting with the control system to guarantee its proper operation. However, any IP Traceback [6] solution in smart Microgrid has been proposed in the literature until now [2]. In this paper, the proposed approach is the first one that integrates the Traceback field in smart Microgrids. However, through the exhaustion of communicational and computational resources, the Denial of Service (DoS) assaults in these systems prevents measurement availability and controls signals. As a result, numerous academics have looked into how to defend Microgrids against the DoS assaults [2]. In fact, Jianzhe Liu et al. [3] advocated that the disturbance effects of the DoS be linked to variations of pure physical model parameters with the development of a sufficient condition to assure a system power balance in the cyber layer. For their part, Jiahong Dai et al [4] proposed a cyber-resilience strategy based on dynamic priority scheduling and a side-channel detector for detecting and mitigating DoS assaults in Microgrids. Wireless Mesh Network (WMN) [7] describes a radio nodes-based communications network structured in a mesh topology. Ahmad Almadhor [8] suggested a mesh communication architecture for monitoring and controlling Microgrid. Another previous work proposed by M. Ben Belgacem et. al [9] developed a demand-side management algorithm for energy consumption scheduler capacity. It offers optimal energy sharing, counting on adequate multi-source installation and suitable energy cost parameters. This work manipulates low Microgrid layers. However, our contribution adds a new security layer to the mesh Microgrid. On the other hand, the wireless mesh network (WMN) [7], is a radio node-based communications network with a mesh topology. To monitor and regulate Microgrids, Ahmad Almadhor [8] proposed a mesh communication architecture. Furthermore, M. Ben Belgacem et al. [9] introduced a demand-side management algorithm for energy consumption scheduler capacity, which provides optimal energy sharing by relying on adequate multi-source installation and appropriate energy cost parameters, as well as manipulating low Microgrid layers. Therefore, in this research, our contribution to the mesh Microgrid consists in adding a new security layer. More specifically, we will describe the fundamentals of our technique used in this paper and validate it using the network simulator 3 (NS-3) [10]. As a result, this section is critical in ensuring the security of our mesh Microgrid technology. A second section explains our hardware implementation and describes our real-world smart mesh Microgrid implementation in an accessible commercial deployment.

The rest of the paper is organized as follows: Section II outlines our smart mesh Microgrid Traceback approach with a theoretical presentation of our simulation results. Then, the proposed Traceback approach is used to create our smart mesh Microgrid implementation in section III. Finally, section IV concludes this paper.

2. The Proposed Traceback approach for Smart Mesh microgrid

Our contribution consists in inventing a novel Traceback approach based on PREP messages of HWMP protocol [11] for smart mesh Microgrid.

We use the trigger-based on-demand traceback to launch the process of our proposed IP traceback solution. Indeed, two conditions are required to trigger a traceback process:

1. The traceback starts when a suspicious flow is identified by an Intrusion Detection System (IDS) [12] or if a network analysis is required [13, 14].
2. In fact, when routers detect the flows of interest, they probabilistically perform a traceback (with a probability $\boldsymbol{p} = \frac{1}{1000}$).

Due to the progress in Software-Defined Networking (SDN) for mesh Microgrid [15], the trigger-based traceback is implementable on SDN-enabled mesh routers.

In this paper, we are concerned with the flow of interest which can be generally identified by a pair of (source, destination) or a five-tuple flow ID (srcIP, dstIP, srcPort, dstPort, and protocol) [16].

To explain our novel approach, we will describe the PREP message protocol of communication by illustrating the intermediate router behavior. After that, an example of our solution will be illustrated. Finally, some security issues in the proposed approach will be discussed.

2.1. PREP message protocol of communication

HWMP [11] uses the PREQ and PREP beacons only in the path discovery process. Therefore, these messages are not needed when packets are transmitted. From this principle, we have the idea to conceive a novel IP traceback approach that uses the PREP message format to transfer the traceback information. We can confirm in our approach that MAC addresses are not spoofed since every spoof in a MAC address induces a perturbation in the routing issue based on the HWMP protocol. Indeed, the choice of PREP comes from the idea that it is a unicast message while the PREQ is a broadcast message. Every router, which joins the wireless mesh Microgrid, must perform authentication to use the proposed scheme. Once, the attacker sends a malicious packet, every authenticated router in the path produces a PREP message after receiving the packet and sends it to the victim. As a consequence, the victim can reconstruct the whole attack path. Figure 1 explains step by step the whole procedure.

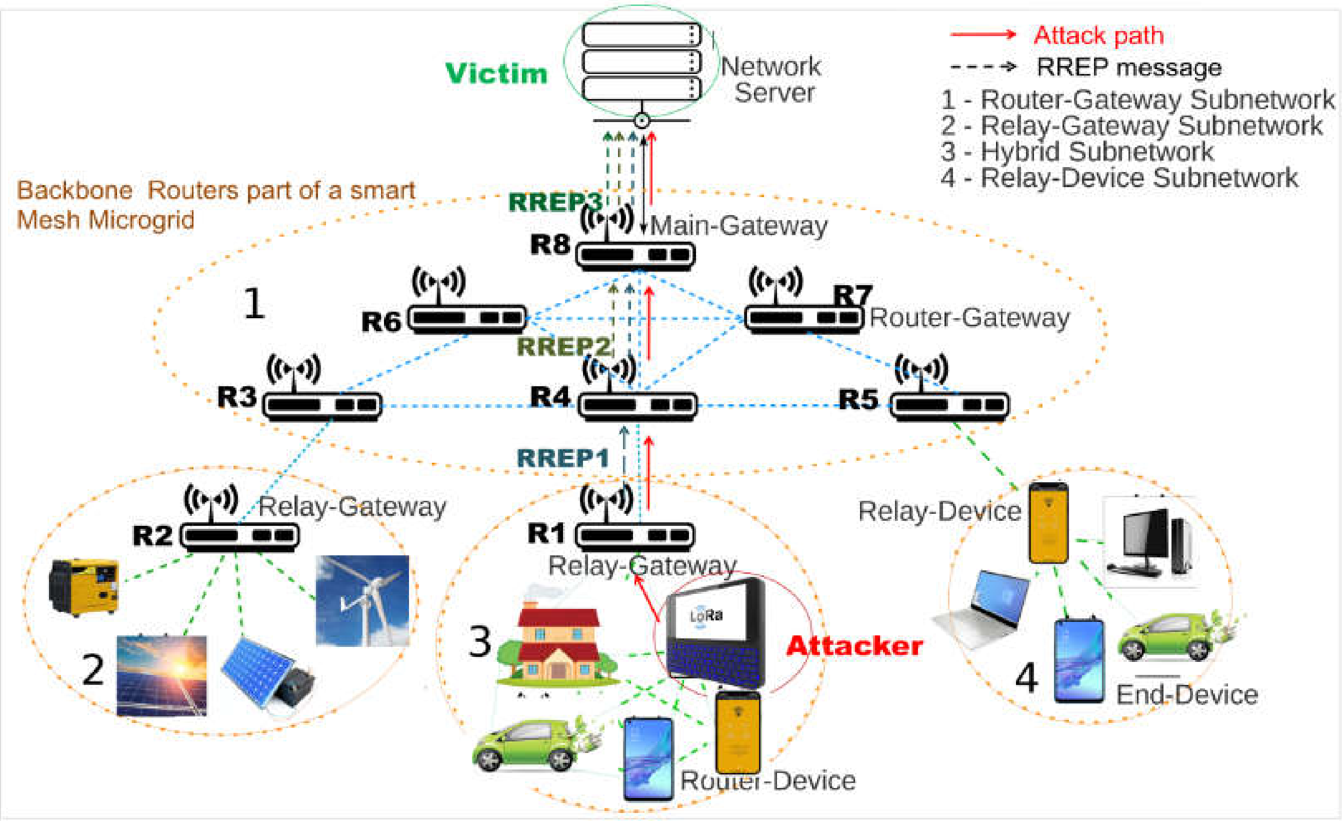


Figure 1. The proposed Traceback procedure against DoS attack for smart mesh Microgrid.

As shown in Figure 2, every PREP message is composed of *Mutable Field* (*MF*; blue color) and *Non-Mutable Field* (*NMF*; white color) [11]. As the PREP message has no effect after the path discovery process, MF and NMF can be used. Thus, we choose to put the decimal form of the attacker's IP address in the ***Originator Sequence Number*** MF field (this field is unused since we have just one message) to inform the victim about the real attacker's address. We propose to assign the current router MAC address to the ***Originator Address*** MF field for allowing the destination to reconstruct the attack path and giving a concrete originator address for HWMP protocol. We assign zero to the ***Metric*** NMF field for giving this message the priority to be treated by HWMP and signaling that it is a traceback message. The identification of the related packet is performed using the ***Lifetime*** and ***Target Sequence Number*** MF fields to match each packet with associated PREP messages. We also propose to assign the MAC address of the victim (extracted from the related packet at data link layer level) to the ***Target External Address*** MF field for sending correctly the current message and the MAC address of the next router to the ***Target Address*** MF field to properly use HWMP. PREP format includes ***Flags*** MF field having B0-B5 and B7 bits reserved in the path discovery process to authenticate NMFs and MFs. To guarantee the message integrity here, we suggest using this field to put the hash value of the related packet identification. The function "mod" by a prime, 127 is the largest 7-bit prime, is used to generate the hash value. Every value is carefully chosen by respecting the maximum size in bits allocated to each field. We suppose that our authentication system can be hacked and a PREP message is spoofed by an intermediate malicious router. Then, the MAC addresses are not spoofed since every MAC spoof changes the real HWMP route. As a consequence, the MAC address trace deducted in the victim part reflects the real attack trace and it is possible to locate the attacker.

Figure 2. schematically summarizes the way to assign the traceback information in the PREP message fields. .

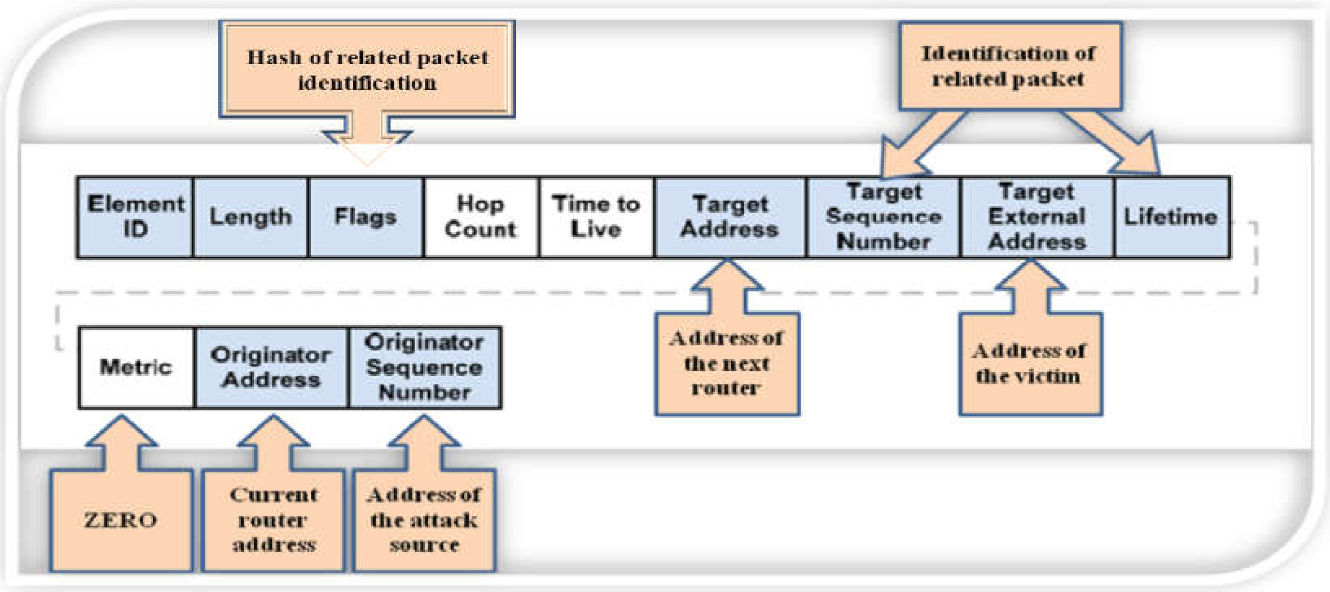


Figure 2. Traceback information used in the PREP message format.

2.2. First router behavior

After receiving an attack packet, the first router in the attack path can determine the real attacker's MAC address from the data link layer. This address cannot be spoofed since any MAC address spoof induces HWMP routing modification. Therefore, this router transforms the real attacker MAC address to the real attacker's IP address using the Reverse Address Resolution Protocol (RARP) mechanism. This router generates the first PREP message. Then, the Traceback algorithm running in the first router is illustrated:

Algorithm 1 The first router Traceback algorithm

```
Initialize no received packet
While true do
    Receive packet P
    if P ϵ attack flow then
        Determine the attacker's MAC address
        Deduce the attacker's IP address using RARP
        Generate the first PREP message
    Forward P
```

2.3. Intermediate router behavior

When the packet attains a router designated by "R", it checks if the related PREP messages exist. If so, the router R forwards old PREP messages to the next router existing in the attack path, which in turn generates a new message then sends it to the next hop before forwarding the related packet.

Our solution can circulate just one PREP message generated by the first router to give information about the real attacker. However, it can also circulate many PREP messages to draw the whole attack trace then avoid man-in-the-middle attack effects at the routing issue. Hence, we do not need in our approach any additional queue since PREP beacons are submitted before the related packet, so every router in the attack path will receive and process them before the packet. In fact, algorithm 2 details the behavior of an intermediate router in the attack path after receiving an attack packet.

Then, after using the trigger-based on-demand traceback, every intermediate router can receive many PREP messages and many packets coming from previous routers existing in different attack paths. Hence, thanks to our traceback scheme, it can match every packet with its PREP messages based on a comparison between the identifiers of packets and the combination of the target sequence number and lifetime fields in every PREP message format. Subsequently, the intermediate router can identify the previous attack path.

Algorithm 2 The intermediate router Traceback algorithm

```
Initialize no received packet
While true do
    Receive packet P
    if P ϵ attack flow then
        While PREP messages related to P exist do
            Forward old PREP messages related to P
        Generate new PREP message with current @MAC
        Forward new PREP message to the next router
    Forward P
```

2.4. PREP message traceback technique

The attack packet attains the last closest router to the victim after its related PREP messages. Therefore, it becomes possible to extract the packet identifier (ID) from this packet as well as the ***Target Sequence Number*** and ***Lifetime*** fields from each message. Then, this router compares the value of ID with the combined value of two fields. Consequently, it can match the packet with its messages ordered chronologically and discover the whole attack path.

Moreover, the victim can block the source of attack just using the first PREP message since the originator sequence number field of this message contains the attacker's IP address. In fact, algorithm 3 illustrates the PREP message traceback technique.

Algorithm 3 The last router Traceback algorithm

```
Initialize no received packet, Attack Path to ϕ
While true do
    Receive packet P
    if P ϵ attack flow then
        Extract ID of P
        While PREP message exists and prior do
            Extract Target Sequence Number and Lifetime
            if ID = concatenate (Target Sequence Number, Lifetime) then
                Add Originator Address to Attack path
        Forward the whole attack path to the victim
    Forward packet P
```

2.5. PREP message IP traceback example

As shown in Figure 1, when the attack packet attains the first router (R1), it generates a PREP message that contains the decimal form of the real attacker's IP address, the MAC address of the current router since HWMP uses MAC addresses, the MAC address of the next-hop (R4) and the MAC address of the victim as the destination address (equals to the destination address of HWMP packet). Then, router R4 forwards the first PREP message received by R1 and generates a second PREP message based on the first message traceback information after receiving the attack packet. This generated PREP message is similar to the first one except that it contains the MAC address of R4 (current router). In the same way, Router R4 forwards the first and second PREP messages and generates another PREP message based on the old ones after receiving the attack packet.

At the destination level, PREP beacons arrive chronologically ordered based on the hop count field. After the reception of an attack packet, the victim can extract the packet identifier and consequently deduces the set of related PREP messages. In this example, the deduced attack path is **R1 --> R4 --> R8**. Consequently, the attacker having the real IP address, extracted from PREP messages, belongs to route R1 LAN.

2.6. Implementation considerations

Using the PREP message protocol of communication, only authenticated routers can participate in the PREP message approach. Subsequently, an attacker who desires to behave as an intermediate router cannot join our mesh Microgrid. In the case of a network congestion, successive messages may overload the mesh network. Consequently, our approach allows discovering the real IP address of the attacker even with a unique PREP message using the ***Original Sequence Number*** field. Thus, the victim can block the source of the attack (e.g. using filtering methods) based only on the first message or optionally wait for all PREP messages to conclude the whole attack path.

For deploying our PREP message approach, we implement two procedures; a generation procedure in the first and intermediate authenticated routers and a reconstruction procedure on the last closest router to the victim. Initially, to execute our Traceback solution, it is essential to establish a PREP generation procedure at the router level. Secondly, it is important to reconstruct the path of the attack packet using the PREP messages. Moreover, to deploy our scheme, we need to neither to add a new message format nor to replace the existing routers with a higher-performance ones.

In fact, only one attack packet is needed by our scheme to perform a traceback since the generated PREP beacons contain all the useful information to reconstruct the path when achieving the destination.

In our approach, the authenticated router creates a new PREP message. Therefore, the sent PREP beacons cause small overheads in the bandwidth. Moreover, the generation procedure is too simple as it does not involve any significant change to the hardware of the router. Furthermore, our scheme needs a limited quantity of extra memory on all the participated routers. Finally, it can defend against major DDoS attacks and can reveal any attack packet source before reaching the network border.

2.7. Performance analysis by resorting to some related works

It is essential to evaluate the proposed Traceback approach by means of ones existing in the litterature. In this case, several IP Traceback solutions [17] are proposed to overcome DoS attacks. In fact, two Traceback techniques resemble our approach concept; the first one is ITrace, which is a traditional *Probabilistic Packet Marking* scheme [18]. Therefore, we can realize a theoretical probabilistic comparison which is sufficient since the ITrace method is old. Then, the second Traceback solution is the OBTA, which is a new *Deterministic Packet Marking* scheme [19]. Moreover, we will compare our proposed approach with OBTA throughout simulations results.

2.7.1. Probabilistic comparison

To perform the first probabilistic comparison with the ITrace method, we need the following performance metrics:

- The number of the required Traceback messages
- The number of the packets needed for the reconstruction of the whole path.
- The bandwidth overhead
- Accuracy

a) The number of required Traceback messages

The ITrace method proposed by Thing et al. [19] produces a message with forwarding or backwarding link permitting to determine 2 routers in an attack path. Moreover, another message with both links is produced to allow the victim to determine 3 routers in an attack path. Hence, for an attack path of 'h' hops, at least 'h/2' ITrace messages (one link) are needed to determine one attacker. Similarly, 'h/3' ITrace messages (both links) are needed to recognize one attacker. In fact, equations (1) and (2) denote respectively the minimum number of ITrace messages with one link and ITrace messages with two links, which are needed to trace 'n' attackers.

$$N_{ITrace} \quad \sum_{i=1}^{n} \frac{h_i}{2} \tag{1}$$

$$N_{ITrace} \quad \sum_{i=1}^{n} \frac{h_i}{3} \tag{2}$$

Therefore, our proposed approach requires 'h' PREP beacons for an attack path of 'h' hops. These beacons, which would be exchanged between routers in the background, are generated at the data link layer level without disturbing the flow of normal data compared to the ICMP, which considers an IP packet circulating with data packets.

$$N \quad \sum_{i=1}^{n} h_i \tag{3}$$

Furthermore, the number of PREP messages needed for the proposed approach is larger than the one needed in the ITrace. However, these messages are beacons circulating between the routers at the routing stage so they are faster than other message types. Besides, these beacons do not globally affect the normal flow transmission.

b) The number of packets needed for the whole path reconstruction

This metric defines the required number of packets that arrived at the last closest router to the victim to reconstruct the entire attack path. Then, the needed data and the Traceback packets are considered in the computing of this metric. Accordingly, the The increase of the required packets needed for the attack path reconstruction delays the Traceback. The Traceback message deduced from multiple hops in the attack path is required by the ITrace. In fact, the probability (P_s) [20] of recreating the whole attack path with 'n' IP packets based on the proposed and the ITrace solutions is given in Table I. On the other hand, in our approach, the probability (P_s) depends on the one generating the first PREP message, and all PREP messages are consequently produced. Therefore, this probability is independent of the path length. However, our solution uses just one normal data packet to establish the traceback process.

Table 1. Probability of the Itrace and the Proposed IP Traceback Solution.

IP Traceback solution	Probability (P_s) of reconstruction of the whole attack path	
Itrace (forward or backward link)	$P_s = (1-(1-p)^n)^{\frac{h}{2}}$	(4)
Itrace (both links)	$P_s = (1-(1-p)^n)^{\frac{h}{3}}$	(5)
PMIT	$P_s = 1-(1-p)^n$	(6)

where p is the probability of generating the traceback message and h is the number of hops in the attack path.

Moreover, the majority of the network paths do not exceed 32 hops [21]. In fact, Figure 3 illustrates the probability of the attack path reconstruction of 20 and 32 hops of path length on receiving ‘n’ packets based on the ITrace (one link), the ITrace (both Links), and the proposed approach sent at a probability of 1/1000.

Fig. 3 demonstrates that our solution needs a smaller number of packets compared to the ITrace methods.

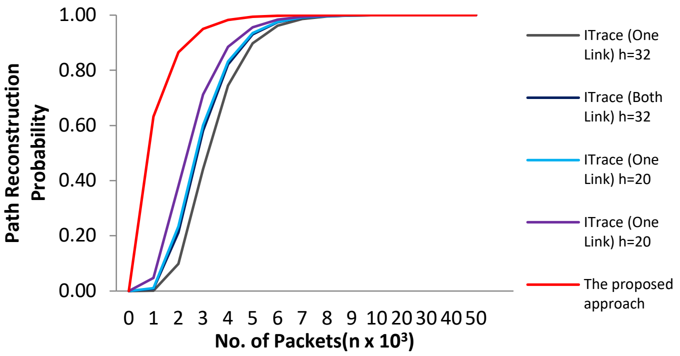


Figure 3. Path reconstruction probability of the ITrace methods, and the proposed Traceback solution.

c) Bandwidth overhead

It is essential to define the bandwidth overhead cost introduced by the proposed IP approach. It doesn’t generate any packet to trace an attack since it uses PREP messages considered as beacons. Therefore, an additional bandwidth is negligible. On the other hand, a traceback message from every hop is needed by the ITrace, whereas our solution requires some traceback beacons to trace the attack path. In fact, Figure 4 illustrates the bandwidth overhead for different attack path lengths using the probability of 1/1000. Then, the ITrace net increase in traffic is dependent on the path length while the proposed approach needs a uniform bandwidth depending on the number of attacks and not on the path length.

The ITrace bandwidth overhead is smaller than the one introduced by our solution with a path length inferior to 20 hops. As for paths having a length exceeding 20 hops, the proposed approach introduces an additional bandwidth smaller than the one produced by the ITrace.

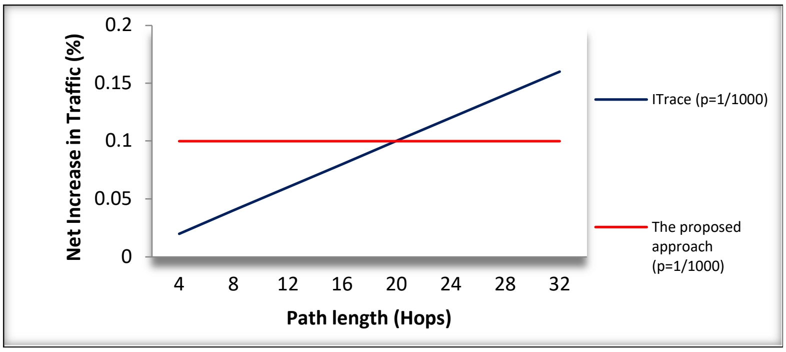


Figure 4. The bandwidth overhead of the ITrace, and the proposed approach.

d) Accuracy

An IP Traceback scheme must be evaluated based on the metric accuracy as a false positive one defines the fact that a border router is falsely considered as an attacker. Therefore, the legal users would be unreasonably punished. The false-negative defines the inability to identify an attacker's border router. In fact, Figure 5 demonstrates the number of false-negative nodes in the function of the number of attackers.

On the other hand, the ITrace solution can reconstruct the attack path only after gathering all the ITrace messages related to that path. In fact, the number of the Itrace messages increases with the rise in the number of attacks. Therefore, if an ITrace message fails to be sent by a router, this will result in an incomplete path and consequently, in false negatives. On the other hand, the ITrace-CP needs multiple ICMP packets to create the attack tree by generating false negatives, mainly when a router fails to send an ICMP packet.

Moreover, the proposed approach uses fast successive beacons for a single data normal packet. As this solution does not depend on multiple data packets or logged data, no possibility of an incomplete path exists. Therefore, it generates zero false positives and false negatives unless the path information element is corrupted by an intruder.

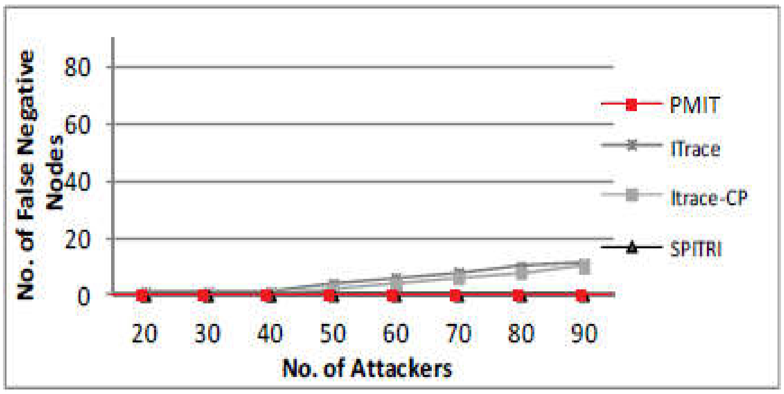


Figure 5. The number of false-positive nodes in the function of the number of attackers.

2.7.2. Simulation results

a) Description of simulation scenario

To validate our approach, we used the discrete simulator NS-3 [22] whose duration is 1000 seconds. On the other hand, the mesh Microgrid simulation model is based on a structure that contains 9 wireless *Mesh Access Points* (MAPs) organized in a square grid topology, as illustrated in Figure 6. Actually, the efficiency of this topology has been proved in previous research [23]. Our MAPs are established according to IEEE 802.11s stack with HWMP protocol and peering management. We choose the MAPs that can incorporate a software, (such as Ettercap [24]). Then to insert the traffic, we used the UdpClientApplication. In fact, the simulation parameters are illustrated in Table II.

doi:10.20944/preprints202208.0382.v1

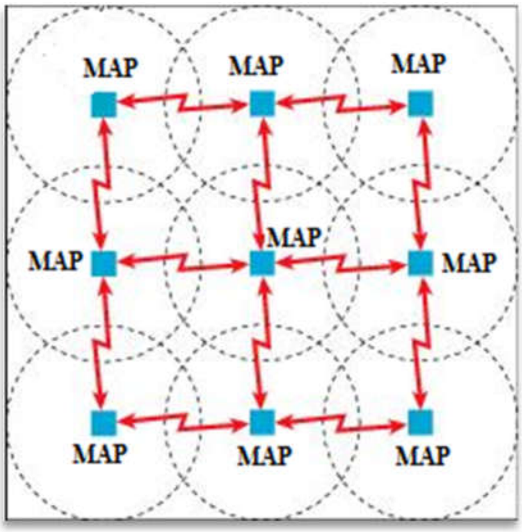


Figure 6. Simulation scenario topology.

Table 2. Simulation parameters.

Parameter	*Value*
Packet size	1024 bytes
Traffic Type	UdpClientApplication
Simulation duration	1000 seconds
Simulation zone	300 m x 300 m
Nodes number	9
Network protocol	IPv4
Routing protocol	HWMP
MAC protocol	MAC/802.11s

b) Performance metrics

Three performance parameters are used in this paper to evaluate the proposed Traceback approach, such as *Delays*, *Throughput*, and the Packet Loss Ratio (*PLR*) of each flow. Theoretically, the end-to-end delay represents the difference between the packet generation time and the time of the packet achieving destination. In our performance evaluation, the *Delays* represent an expressed function of all the end-to-end delays for all the received packets of the flow while the *Throughput* represents the average number of bits per second reaching the destination node. On the other hand, the *PLR* represents the number of overall lost transmitted packets for the flow. We rely on the existed variables related to the Flow Monitor module in the NS-3 to calculate the following three parameters:

- *rxPackets*: the total number of received packets for the flow.
- *txPackets*: the total number of transmitted packets for the flow;
- *delaySum*: the sum of all the end-to-end delays for all the received packets of the flow;

$$delaySum = \sum_{i=1}^{rxPackets} d_{P_i} \tag{7}$$

where P_i is the received packet at instant $i \epsilon [1, n]$, and d_{P_i} is the end-to-end delay of P_i.

- *rxBytes*: the total number of received bytes;

$$rxBytes = rxPackets \times nb \tag{8}$$

then, *nb* is the number of bytes per one received packet.

- *timeLastRxPacket*: when the last packet in the flow is received;

- *timeFirstTxPacket*: when the first packet in the flow is transmitted;

$$Delays = delaySum\ (s) \tag{9}$$

$$Throughput = \frac{\frac{\frac{rxBytes \times 8.0}{timeLastRxPacket\ (s) - timeFirstTxPacket\ (s)}}{1024}}{1024} \tag{10}$$

$$PLR = float\left(\frac{100*(\boldsymbol{txPackets - rxPackets})}{float(rxPackets)}\right) \tag{11}$$

(7), (8), (9), (10), and (11) permit to deduce the *Delays*, the *Throughput*, and the *PLR* values.

In fact, the first scenario contains three legal users associated with three defined MAPs (see Figure 7) for observing the normal simulator function. Then, we inject a UDP flooding attack in the border user as shown in Figure 8; we progressively measure the end-to-end delay per-flow without any attack or Traceback scheme. We choose in our experiments three flows to highlight our solution effect on the attack flow and other normal ones in the network. Then, we implement the proposed solution in the data link layer and monitor the metric variations.

On the other hand, the UDP flooding attack generates a red curve as shown in Figure 9. This curve is associated with the *Delays* value of the attacker’s flow growing linearly. This is due to the attacker's monopolization of the Mesh Microgrid. Practically, by adding our algorithms to the HWMP protocol in the mesh module within the NS3 core, we can observe an amelioration of the attack flow *Delays* with the implemented Traceback solution. Therefore, the *Delays* values become close to the normal simulator function.

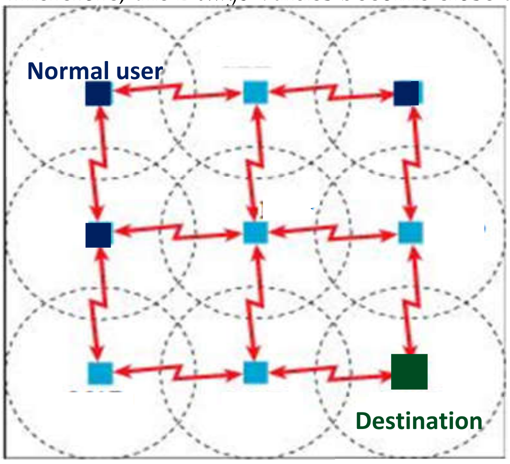


Figure 7. The normal simulation scenario.

doi:10.20944/preprints202208.0382.v1

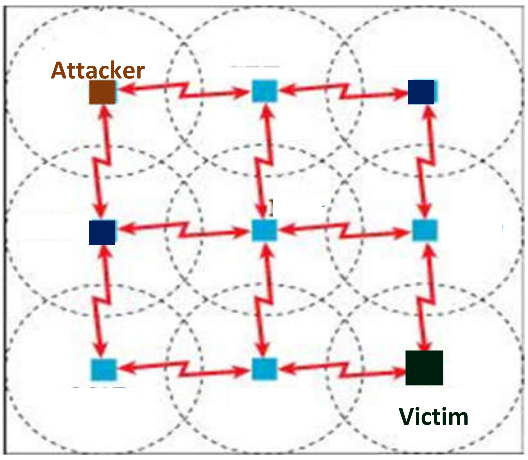


Figure 8. The UDP Flooding attack injection.

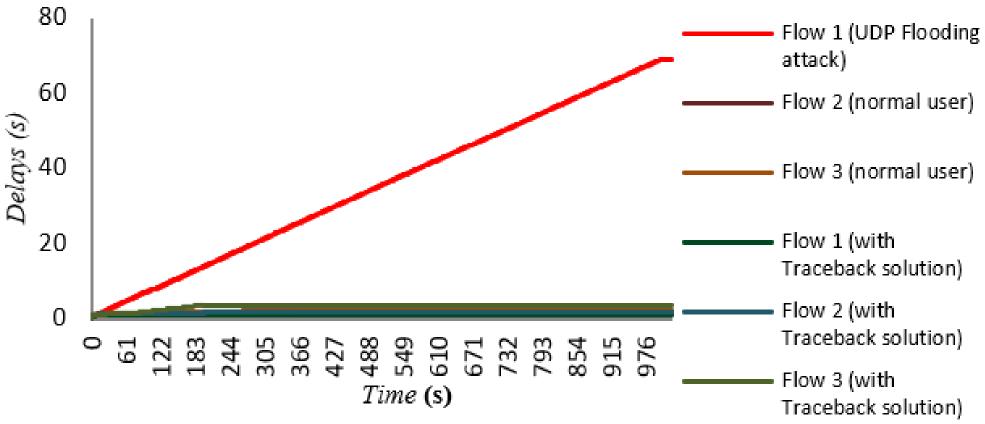


Figure 9. Amelioration of the Delays values with the proposed Traceback solution against the UDP Flooding attack.

In fact, the proposed solution brings an additional communication overhead in terms of *Delays* (Figure 10), which achieves a maximum of *1,125 seconds* better than the OBTA induced one *(2 seconds)*. This delay is added by the PREP message generation processes. Moreover, it is acceptable to secure the submitted packets in a mesh Microgrid. The enhancement in Delays, compared to OBTA, is equal to *875 ms*. We compare our approach with the OBTA because the two solutions operate in the data link layer. Therefore, OBTA seems the best for making the comparison.

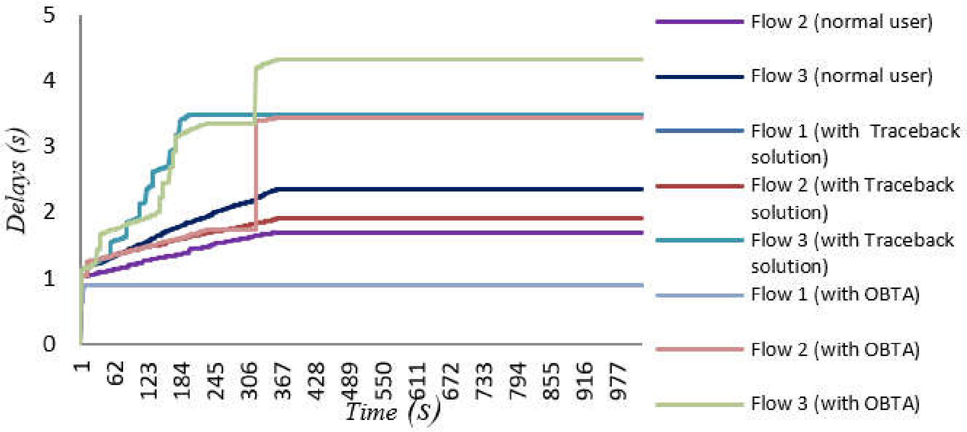


Figure 10. Delays overhead of the proposed approach and the OBTA.

Figure 11 illustrates the *Throughput* values under the attack controlled by the proposed Traceback scheme and the OBTA solution for the two considered flows. Since the PREP message is a beacon, the throughput remained approximately the same even after implementing the proposed solution. On the other hand, flows 2 and 3 are used here to highlight our approach capacity to conserve the Throughput (≃3.10^{-3} Mbps) compared to the OBTA, which reduces it (≃ 2.10^{-3} Mbps). Therefore, our solution outperforms the OBTA in terms of *Throughput*.

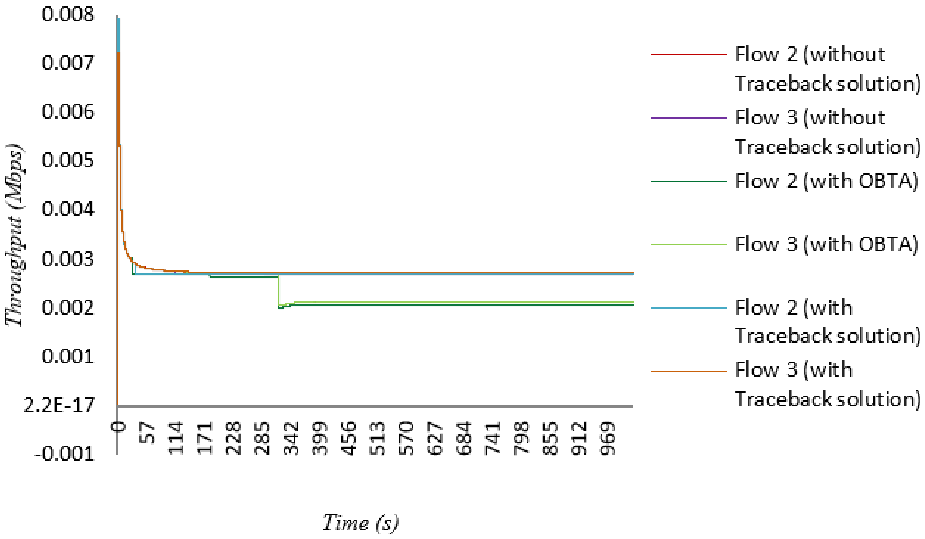


Figure 11. *Throughput* values controlled by the proposed approach and the OBTA.

Figure 12 represents the Packet Loss Ratio (*PLR*) of the three considered flows controlled by the proposed approach and the OBTA. On the other hand, flow 1 curves are practically constant (~2,8 %) since the traceback approaches stop the attack at the data link layer level, so the *PLR* has a constant value based on the application layer. Then, the difference between the proposed approach and the OBTA can be shown through flow 2 and 3 curves. Therefore, with the OBTA approach, the *PLR* attains approximately 30% since a separate radio module is used at the data link layer level for traceback purposes, which induces packets loss. In fact, with our solution, an enhancement in the *PLR* values compared to those of OBTA is illustrated in Table III. However, our approach increases this value by 2%, which is considered acceptable foor attaining the traceback goal.

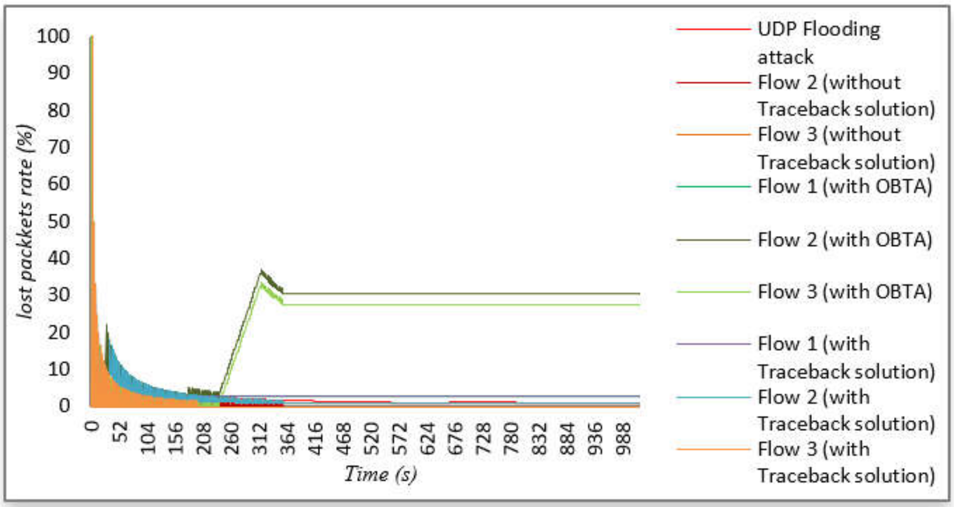


Figure 12. *PLR* values under the UDP Flooding attack controlled by the OBTA and the proposed approach.

Table 3. The PLR stationary value comparison between the OBTA and the proposed approach.

	Without attack	*Attack without Traceback*	*OBTA*	*Proposed solution*
Flow 1	0,299401	0,88	2,8169	2,8169
Flow 2	0,299401	0	30,4348	0,840336
Flow 3	0,299401	0,833	27,6596	0

Figure 13 represents the Throughput function of the number of attacks. We progressively insert a new UDP flooding attack to the simulation scenario to evaluate the proposed approach in the case of Distributed Denial of Service (DDoS) attacks. Then, the bandwidth is partitioned with the emergence of a new attack. In fact, in more than two attacks, each flow takes a constant bandwidth value without a bandwidth division. Besides, the Throughput overhead of the different attack numbers is approximately *0,001Mbps*, which is considered negligible in a mesh Microgrid. Therefore, by increasing the number of attacks, we notice that the attack throughput is practically similar to what is in our solution, OBTA, and HWMP standard. Consequently, the number of attacks metric has not a significant influence on the throughput value whatever the used traceback solution is.

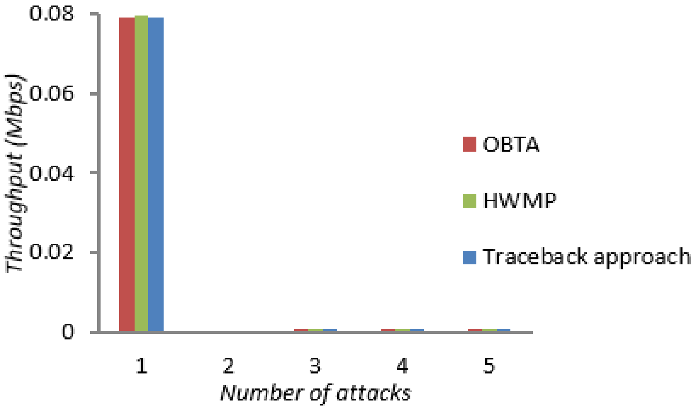


Figure 13. The *Throughput* value function of attacks number for the OBTA, the HWMP, sand the proposed Traceback solution.

doi:10.20944/preprints202208.0382.v1

The distance metric is the distance between nodes in the mesh Microgrid. To better asses the routing issues and the effect of using PREP messages, we need to add an auxiliary non-Traceback solution named HWMP-WATCHDOG [25] working with the HWMP protocol in the security field. In fact, Figure 14 shows the proposed approach and OBTA *Throughput* values closer to the HWMP standard ones than to the HWMP-WATCHDOG ones. Consequently, OBTA and our solution outperform HWMP-WATCHDOG in terms of the *Throughput* function of the distance.

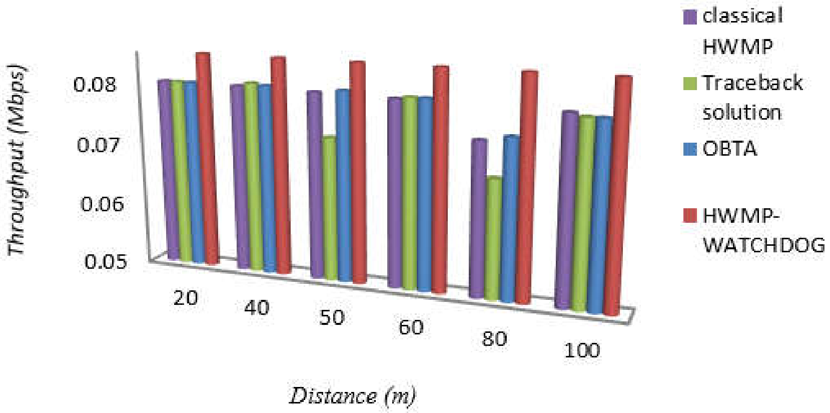


Figure 14. The *Throughput* values for the OBTA, the HWMP-WATCHDOG, the classical HWMP, and the proposed approach.

Figure 15 demonstrates that the OBTA and the proposed approach *PLR* values are closer to the classical HWMP values than the HWMP-WATCHDOG ones; which means that when the distance augments, a variation augments in a short-range between 4% and 8%. Then, the OBTA and our solution have approximately the same *PLR* variations as both use a special message to transfer traceback information, so both outperform the HWMP-WATCHDOG in terms of the *PLR* function of the distance.

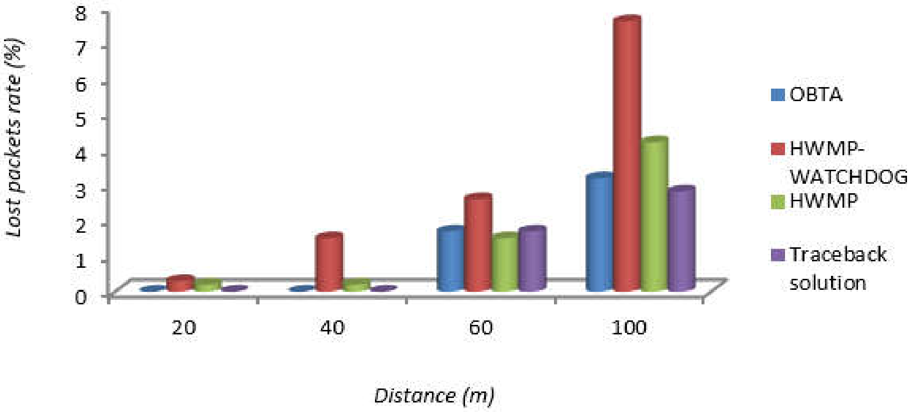


Figure 15. The *PLR* function of the distance for the OBTA, the HWMP-WATCHDOG, the classical HWMP, and the proposed approach.

3. Hardware deployment

3.1. Description of the smart microgrid installation and application

This paper deals with the multi-source solution [9] within the mesh Microgrid and proves that even with a reduced renewable energies installation, an excellent energy sharing system with an installed security layer can offer important results. As a consequence, the suggested system can be useful for all smart Microgrid users who share it. In the ain important assumption shows the common interests of all users in efficiently sharing energies by participating in the installation costs and also sharing the same space (building roof or common garden …), energy demand, etc. Moreover, the collaborative installation provides many advantages, such as the users encouragement to use renewable energy sources although these sources are relatively expensive or insufficient for covering the whole demand of the load. Therefore, integrating an optimal sharing system with a security layer is thought to be the main goal. Figure 16 describes the topology of collaborative energy sharing installation. Generally, which integrates:

- The users in the shared zone.
- The sources: in this application context, a multi-source solution is presented. The utility company (the public company of electricity (PC)) is the non-renewable source to cover, if necessary, the renewable energy insufficiency. In fact, the renewable energy is produced by wind turbines attached to photovoltaic panels (PV).
- The sharing station: It is a crucial part in the process as it receives the data from the users and sources. Besides, it is responsible deciding the convenient source to be used. As a result, the user will both switch or keep the source.
- Data channel: As shown in figure 16, in the suggested architecture, the data communication is designed to use Wireless Sensors Mesh Network.

In this application, an energy consumption scheduler (ECS) capacity is integrated.

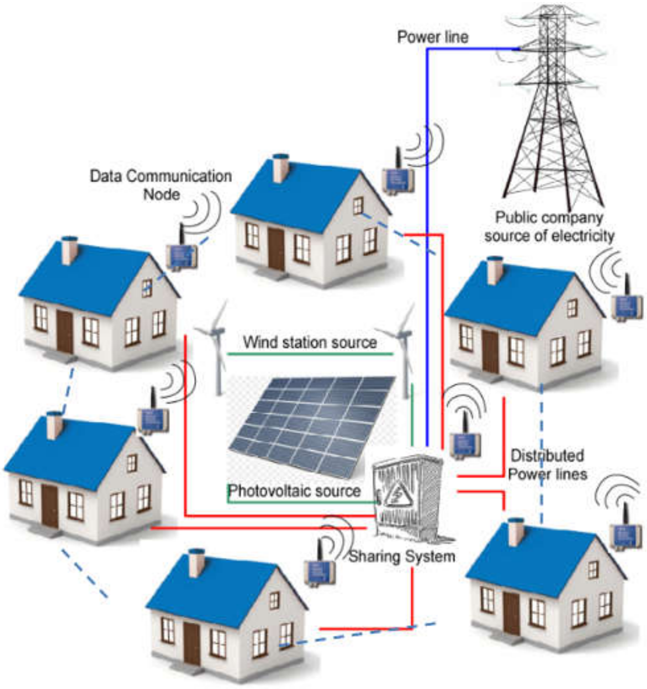


Figure 16. The energy sharing topology and strategy for smart Microgrid.

doi:10.20944/preprints202208.0382.v1

3.2. Hypothesis and test conditions

We are based on the Mini-Mesh Testbed [26] in the conception of our mesh Microgrid deployed as a prototype at the Sfax Digital Research Center in Tunisia. To design our mesh Microgrid we applied a testbed, which includes 9 Intel Galileo single-board computers [27]. In fact, these boards execute a full-featured Linux by providing a mPCIe interface, which is essential for equipping the nodes with .11 NIC from the Atheros product family, propped by the ath9k driver. Currently, it is the most versatile and configurable .11 driver.

Table 4. configurating the Test-bed.

Parameter	*Value*
Device	Intel Galileo Board (Gen.1)
CPU	Quark X1000 (Single-Core 400 MHz)
RAM	256 MB DDR3
OS	Debian 8 (Linux Kernel v4.9)
.11 NIC	Compex WLE200NX .11a/b/g/n (mPCIe)
NIC Chipset	Atheros AR9280 (ath9k driver)
Antennas	2 x 5 dBi Dual-Band Omni-Direct.
Antenna Cables	2 x 20 cm U.FL-RP-SMA
Attenuators	2 x Mini-Circuits VAT-30+ (30 dB)
Channel	149 (5745 MHz, HT20, Long GI)

In fact, Table IV shows the software and hardware configuration of the mesh nodes in the Microgrid. It can be seen that all the devices have a Debian 8 OS based on the Linux kernel v4.9, incorporating the .11(s) software MAC layer where each mesh node has a .11n capable Atheros NIC, which applies two TX and RX chains and up to two spatial streams that can operate in various and spatial multiplexing MIMO modes. Then, the NIC is attached to two dual-band omnidirectional antennas (6 cm inter-antenna distance, 5 dBi gain) through 20 cm pigtail cables. At each antenna connector, we add fixed 30 dB RF attenuators [28] for indoor scaling purposes.

Furthermore, to prevent an external interference in the testbed as possible as it can, we make all the nodes work on the practically unused 5 GHz channel 149. Although channels 149–165 are investigated for regular .11a running mode, their use in North America and other countries, is permitted only with a maximum TX power of 25mW for European regulations. Therefore, to ensure a fine-grained control of range within the technical and regulatory limits of our testbed, we configure the TX power in 1 dBm steps from 0 (1mW) to 14 dBm (25mW) per TX chain. In fact, this consists in inducing a dual-antenna configuration between a minimum of 3 dBm (2mW) and a maximum of 17 dBm (50mW).

As a consequence, our implemented mesh Microgrid, which requires an indoor area of 40 cm^2, consists of a 3x3-node regular grid setup to enable multi-hop scenarios. Figure 17 illustrates the current testbed geometry. Based on the result of the dual-antenna design, we place the adjacent nodes at a 26 cm distance, vertically, 20 cm horizontally, and 33 cm diagonally. However, only physical grid neighbors can directly transmit the data thanks to the communication range, which is limited to 33 cm<d<40 cm. This is performed by adding fixed RF attenuators and TX power diminution. Then, the 802.11s mesh routing protocol HWMP is responsible for automatically forming on-demand multi-hop paths between non-neighboring nodes.

3.3. Implementation stratigies

The energy acquisition part consists of three Energy Analyzers Carlo Gavazzi DIN14 connected to Intel Galileo Gen.1 with the Compex WLE200NX .11a/b/g/n. The first is designed to monitor Wind Station flow while the second is applied for the PV Station flow. Then, the last one controls Public Company's flow.

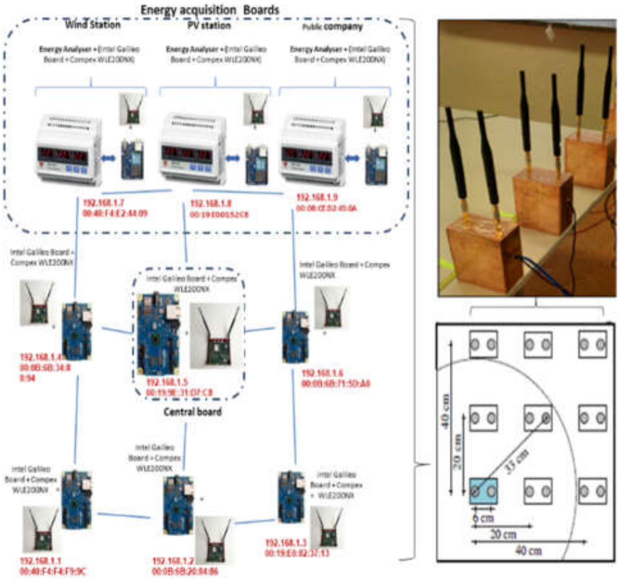
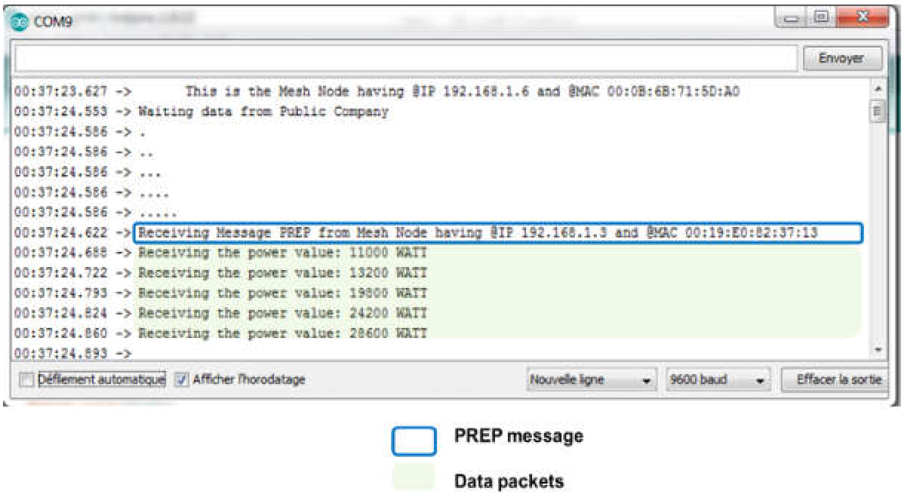

Energy acquisition Boards
Wind Station
PV station
Public company
Energy Analyser + (Intel Galileo Board + Compex WLE200NX)
Energy Analyser + (Intel Galileo Board + Compex WLE200NX)
Energy Analyser + (Intel Galileo Board + Compex WLE200NX)
192.168.1.7
00:40:F4:E2:44:09
192.168.1.8
00:19:E00552C8
192.168.1.9
00:08:CF:02:45:0A
Intel Galileo Board + Compex WLE200NX
Intel Galileo Board + Compex WLE200NX
Intel Galileo Board + Compex WLE200NX
192.168.1.4
00:0B:6B:34:8
8:94
192.168.1.5
00:19:9E:31:D7:C8
192.168.1.6
00:0B:6B:71:5D:A0
Central board
Intel Galileo Board + Compex WLE200NX
Intel Galileo Board + Compex WLE200NX
Intel Galileo Board + Compex + WLE200NX
192.168.1.1
00:40:F4:F4:F9:9C
192.168.1.2
00:0B:6B:20:84:86
192.168.1.3
00:19:E0:82:37:13
40 cm
20 cm
33 cm
6 cm
20 cm
40 cm

Figure 17. Our deployed Mesh Microgrid.

Furthermore, after preparing the mesh Microgrid testbed, we implement the Traceback solution in the data link layer by adding Traceback procedures to the HWMP implementation of the open sources open80211s [29] where each Intel Galileo Board can be held through Arduino 1.8.12 software. We suppose that there is a Distributed Denial of Services attack (DDoS) composed of three attackers having 192.168.1.1, 192.168.1.2, and 192.168.1.3 as IP addresses. These attackers usurp Wind station, PV station, and Public Companies' identities to send false information about the entire energy available for Microgrid consumption. Therefore, we control the Monitor output of each mesh node to control the three attackers' flows which behave as Wind station, PV station, and Public Company.

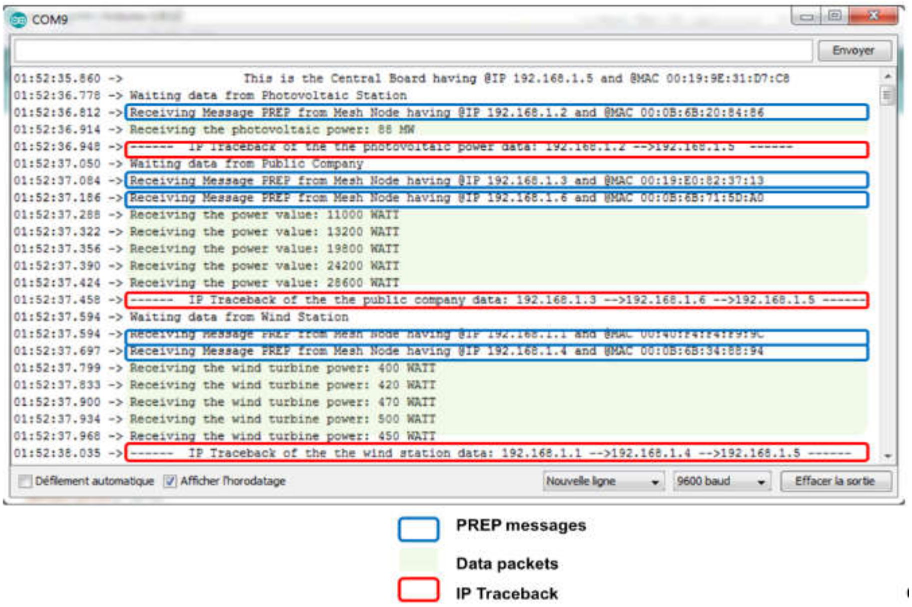
3.4. Results

Figure 18 describes the Monitor output of the mesh node having 192.168.1.6 as IP address and 00:0B:6B:71:5D: A0 as MAC address. This intermediate Mesh node receives the first PREP message associated with data packets of the attack flow.



```
00:37:23.627 ->       This is the Mesh Node having @IP 192.168.1.6 and @MAC 00:0B:6B:71:5D:A0
00:37:24.553 -> Waiting data from Public Company
00:37:24.586 -> .
00:37:24.586 -> ..
00:37:24.586 -> ...
00:37:24.586 -> ....
00:37:24.586 -> .....
00:37:24.622 -> Receiving Message PREP from Mesh Node having @IP 192.168.1.3 and @MAC 00:19:E0:82:37:13
00:37:24.688 -> Receiving the power value: 11000 WATT
00:37:24.722 -> Receiving the power value: 13200 WATT
00:37:24.793 -> Receiving the power value: 19800 WATT
00:37:24.824 -> Receiving the power value: 24200 WATT
00:37:24.860 -> Receiving the power value: 28600 WATT
00:37:24.893 ->
```

Figure 19. The Monitor output of the mesh node has @IP 192.168.1.4.



```
01:52:35.860 ->                  This is the Central Board having @IP 192.168.1.5 and @MAC 00:19:9E:31:D7:C8
01:52:36.778 -> Waiting data from Photovoltaic Station
01:52:36.812 -> Receiving Message PREP from Mesh Node having @IP 192.168.1.2 and @MAC 00:0B:6B:20:84:86
01:52:36.914 -> Receiving the photovoltaic power: 88 MW
01:52:36.948 -> ------  IP Traceback of the the photovoltaic power data: 192.168.1.2 -->192.168.1.5  ------
01:52:37.050 -> Waiting data from Public Company
01:52:37.084 -> Receiving Message PREP from Mesh Node having @IP 192.168.1.3 and @MAC 00:19:E0:82:37:13
01:52:37.186 -> Receiving Message PREP from Mesh Node having @IP 192.168.1.6 and @MAC 00:0B:6B:71:5D:A0
01:52:37.288 -> Receiving the power value: 11000 WATT
01:52:37.322 -> Receiving the power value: 13200 WATT
01:52:37.356 -> Receiving the power value: 19800 WATT
01:52:37.390 -> Receiving the power value: 24200 WATT
01:52:37.424 -> Receiving the power value: 28600 WATT
01:52:37.458 -> ------  IP Traceback of the the public company data: 192.168.1.3 -->192.168.1.6 -->192.168.1.5 ------
01:52:37.594 -> Waiting data from Wind Station
01:52:37.594 -> Receiving Message PREP from Mesh Node having @IP 192.168.1.1 and @MAC 00:40:F4:F4:F9:9C
01:52:37.697 -> Receiving Message PREP from Mesh Node having @IP 192.168.1.4 and @MAC 00:0B:6B:34:88:94
01:52:37.799 -> Receiving the wind turbine power: 400 WATT
01:52:37.833 -> Receiving the wind turbine power: 420 WATT
01:52:37.900 -> Receiving the wind turbine power: 470 WATT
01:52:37.934 -> Receiving the wind turbine power: 500 WATT
01:52:37.968 -> Receiving the wind turbine power: 450 WATT
01:52:38.035 -> ------  IP Traceback of the the wind station data: 192.168.1.1 -->192.168.1.4 -->192.168.1.5 ------
```

Figure 20. The Monitor output of the central board.

4. Conclusion

To conclude, we can say that this paper is the first to have adopted an IP Traceback field in the mesh Microgrid. In fact, we designed a novel Traceback method based on the unused PREP messages after the path discovery process of the IEEE 802.11s HWMP protocol. These messages are exchanged between intermediate mesh routers in the attack path to determine the attack originator. We validated our solution through NS-3 simulations by performing a concrete comparison with some Traceback solutions of the Literature. Our solution reduces approximately 29% of the *PLR* value compared to the OBTA solution. Finally, we performed a Mini-Mesh Microgrid as an accessible commercial deployment at the Sfax Digital Research Center in Tunisia to examine the efficacy of the proposed method. On the other hand, the Monitor outputs of the intermediate mesh nodes and the central board show the good solution function and its 100% capacity of tracing back the attack source and deducing the whole attack trace.

References

[1] Q. Yang, J. A. Barria, and T. C. Green, “Advanced power electronic conversion and control system for universal and flexible power management,” IEEE Trans. Smart Grid, vol. 2, pp. 231–243, Jun. 2011.

[2] B. Canaan, B. Colicchio, D. Ould Abdeslam, “Microgrid Cyber-Security: Review and Challenges toward Resilience”. *Appl. Sci.* Vol. *10*, no. 16, pp. 5649, 2020. https://doi.org/10.3390/app10165649.

[3] J. Liu, Y. Du, S. Yim, X. Lu, B. Chen and F. Qiu, "Steady-State Analysis of Microgrid Distributed Control under Denial of Service Attacks," in IEEE Journal of Emerging and Selected Topics in Power Electronics, doi: 10.1109/JESTPE.2020.2990879.

[4] J. Dai, Y. Xu, Y. Wang, T. -L. Nguyen and S. Dasgupta, "A Cyber-Resilience Enhancement Method for Network Controlled Microgrid against Denial of Service Attack," IECON 2020 The 46th Annual Conference of the IEEE Industrial Electronics Society, Singapore, 2020, pp. 3511-3516, doi: 10.1109/IECON43393.2020.9254876.

[5] A. Saad, S. Faddel, T. Youssef and O. A. Mohammed, "On the Implementation of IoT-Based Digital Twin for Networked Microgrids Resiliency Against Cyber Attacks," in IEEE Transactions on Smart Grid, vol. 11, no. 6, pp. 5138-5150, Nov. 2020, doi: 10.1109/TSG.2020.3000958.

[6] S.M. Bellovin , “IP Traceback”. In: van Tilborg H.C.A., Jajodia S. (eds) Encyclopedia of Cryptography and Security. Springer, Boston, MA, 2011. https://doi.org/10.1007/978-1-4419-5906-5_268.

[7] G. R. Hiertz, D. Denteneer, S. Max, R. Taori, J. Cardona, L. Berlemann, and B. Walke, “IEEE 802.11s: the WLAN mesh standard,” IEEE Wireless Communications, vol. 17, no. 1, 2010.

[8] A. Almadhor, “Feedback-Oriented Intelligent Monitoring of a Storage-Based Solar Photovoltaic (PV)-Powered Microgrid with Mesh Networks”. Energies. Vol. 11, no. 6, pp. 1446, 2018. https://doi.org/10.3390/en11061446.

[9] M. Ben Belgacem, B. Gassara , A. Fakhfakh."Design and implementation of multi-source and multi-consumer energy sharing system in collaborative smart microgrid installation". Sensors, Vol. 13, No. 9, September 2013, pp. 11553-11585.

[10] NS-3 Consortium, “NS-3 is a discrete-event network simulator,” 2017. [Online]. Available: {https://www.nsnam.org}.
[11] Tan. Whye K, Lee.Sang-Gon, Lam. Jun H and Yoo. Seong-Moo."A Security Analysis of the 802.11s Wireless Mesh Network Routing Protocol and Its Secure Routing Protocols". Sensors, Vol. 13, No. 9, September 2013, pp. 11553-11585.
[12] Q. Dong, S. Banerjee, M. Adler, and K. Hirata, “Efficient probabilistic packet marking,” The 13th IEEE International Conference on Network Protocols (ICNP'05), Boston, MA, USA, November 2005.
[13] L. Lu, M. C. Chan, and E.-C. Chang, “A general model of probabilistic packet marking for IP traceback,” Proceedings of the ACM Symposium on Information, Computer and Communications Security (ASIACCS’08), Tokyo, Japan, March 2008, pp. 179–188.
[14] P. Patil, A. Hakiri, Y. Barve, A. Gokhale, "Enabling software-defined networking for wireless mesh networks in smart environments", The 15th International Symposium on Network Computing and Applications (NCA), Cambridge, MA, USA, October 2016, pp. 153-157.
[15] D. Jin et al., "Toward a Cyber Resilient and Secure Microgrid Using Software-Defined Networking," in IEEE Transactions on Smart Grid, vol. 8, no. 5, pp. 2494-2504, Sept. 2017, doi: 10.1109/TSG.2017.2703911.
[16] M. Avula, S. –G. Lee. S-M. Yoo, "Security Framework for Hybrid Wireless Mesh Protocol in Wireless Mesh Networks ", KSII Transactions on Internet and Information Systems, Vol. 8, No. 6, June 2014, pp. 1986.
[17] K. Singh, P. Singh, K. Kumar, “A systematic review of IP traceback schemes for denial of service attacks” Computers & Security, Vol. 56, pp. 111-139, 2016. https://doi.org/10.1016/j.cose.2015.06.007.
[18] V. L. L. Thing, H. C. J. Lee, M. Sloman and J. Zhou. “Enhanced ICMP Traceback with Cumulative Path”, Proceedings of the 61st IEEE Vehicular Technology Conference, Stockholm, Sweden, May 2005.
[19] M. Gassara, I. Bouabidi, F. Zarai, M. S. Obaidat, Fellow of IEEE and Fellow of SCS, and Hsiao K-F. “Deployment and validation of Out of Band IP Traceback Approach (OBTA) in Wireless Mesh Network". International Journal of Communication Systems, Vol. 31, No. 10, pages e3580, 2018. https://doi.org/10.1002/dac.3580.
[20] M. Vijayalakshmi and S. Mercy Shaline, “Single Packet ICMP Traceback Technique using Router Interface”. Journal of Information Science and Engineering. vol. 31, 2015, pp. 1757-1778.
[21] B. Cheswick, H. Burch, and S. Branigan. “Mapping and Visualizing the Internet.” in Proc. of USENIX Annual Technical Conference 2000, San Diego, CA, June 2000.
[22] Network Simulator, https://www.nsnam.org/, last visited in April 2021.
[23] M. Sanni, A. Hashim, F. Anwar, G. Ahmed, S. Ali. "How to model wireless mesh networks topology", IOP Conference Series: Materials Science and Engineering, Vol. 53, No. 1, pp. 12-37, November 2013.
[24] [Online]. Available: https://null-byte.wonderhowto.com/how-to/spy-web-traffic-for-any-computers-your-network-intro-arp-poisoning-0131785/.
[25] J. Ben-Othman. J.-P. Claude and Y.I.S. Benitez, “A Novel Mechanism to Secure Internal Attacks in HWMP Routing Protocol”, Proceedings of the IEEE International Conference on Communications (ICC) Technical Symposium on Ad-Hoc And Sensor Networks, Ottawa, Canada, June 2012.
[26] M. Rethfeldt, B. Beichler, H. Raddatz, F. Uster, P. Danielis, C. Haubelt, D. Timmermann, "Mini-Mesh: Practical assessment of a miniaturized IEEE 802.11n/s mesh testbed," IEEE Wireless Communications and Networking Conference (WCNC), 2018, pp. 1-6, doi: 10.1109/WCNC.2018.8377247.
[27] Intel Galileo Gen1, 2017. [Online]. Available:http://ark.intel.com/products/78919/Intel-Galileo-Board
[28] Mini-Circuits, “VAT-30+ Signal Attenuators,” 2017. [Online]. Available:http://www.minicircuits.com/pdfs/VAT-30.pdf.
[29] open80211s, 2020. [Online]. Available: http://www.o11s.org/.