Assessing the Overhead of Authentication during SDN-Enabled Restoration of Smart Grid Inter-substation Communications

Abdullah Aydeger, Nico Saputro, Kemal Akkaya, and Selcuk Uluagac
Dept. of Electrical & Computer Engineering, Florida International University, Miami, FL, 33174 USA
{aayde001, nsapu002, kakkaya, suluagac}@fiu.edu

***Abstract*—Since real-time and resilient recovery of link failures is crucial for power grid infrastructure to continue its services, emerging technologies such as Software Defined Networking (SDN) has started to be employed for such purposes. SDN switches can be remotely controlled to change their configurations by exploiting the wireless communication options. However, when wireless is to be used in Smart Grid communications, security and reliability become important issues due to the specific characteristics of wireless communications. This paper investigates the overhead of providing such services on wireless links when SDN is utilized. Specifically, we consider the establishment of authentication services when wireless back-up links (i.e., WiFi or LTE) are employed as a result of a reactive link failure detection mechanism. To the best of our knowledge, this work is the first to consider authentication of such an SDN-enabled Smart Grid inter-substation communication with WiFi and LTE. To be able to effectively evaluate the performance of this proposed SDN-enabled framework, we developed it in Mininet emulator. Since Mininet does not support the authentication services for WiFi or LTE, we proposed several novel extensions to Mininet by integrating it with ns-3 simulator that supports the LTE/WiFi protocol stacks. We conducted extensive experiments by considering a general application using Smart Grid Manufacturing Message Specification (MMS) standard to assess the recovery performance of the proposed secure SDN-enabled recovery system. The results show that when authentication and reliable protocols such as TCP are to be employed, the proposed framework can still meet the deadlines of 100 ms with WiFi while LTE misses only a few packets.**

I. Introduction

Power Grid in the US is going through major changes by enjoying the advancements in information and communication technologies. In addition to employing more intelligent electronic devices, the data communication infrastructure is also being upgraded with new standards and wireless communication options to pave the way for a much Smart(er) Grid. For instance, advanced metering infrastructure (AMI) mostly exploits wireless mesh networking among smart meters while substation communications rely on WiFi. LTE-based communications are also being considered for inter-substation or Phasor Measurement Units (PMUs) communications.

One very recent advancement in Smart Grid communication infrastructure is to employ Software Defined Networking (SDN), a promising technology that brings efficient management, flexibility, and control [1]. The main idea of SDN is to separate the data and control planes in networking by employing OpenFlow protocol and thereby giving control to a central manager to flexibility update the traffic, software, and configurations whenever needed. It has been recommended to be used in many components of Smart Grid such as microgrids, SCADA networks, inter-substation communications and PMU networks [2]–[7]. In this paper, we are particularly focusing on the inter-substation communication applications where SDN was deemed as an effective mechanism to quickly recover from link failures due to an attack or a disaster [7]. Specifically, via SDN, the switches can start using the backup wireless links to resume data (or control data) communications with almost negligible switching time delays [7] while also sustaining similar performance when wireless links are used.

However, the previous studies do not take into account the security threats that might be relevant when a wireless link is established for inter-substation communications. For instance, a malicious user may impersonate an SDN switch and can connect to the source substation via wireless links. Additionally, if a cellular link is to be established, there might be rogue base-stations that may act as a man-in-the-middle attacker between two substations. For such cases, authentication is necessary before any data can be allowed to resume its transmissions. However, when authentication is employed, it will bring additional delay for the data in transmission. SDN switches should be capable of handling the delay incurred in such authentication depending on the used wireless protocol. Additionally, once the connection is authenticated, one needs to ensure that the time-sensitive smart grid packets are not lost due to the wireless channel.

In this paper, we propose novel mechanisms to mutually authenticate SDN switches during a link failure recovery and assess their delay overhead on the recovery time. We argue that as opposed to proactive approaches that are being championed by the latest version of OpenFlow, reactive approach is needed to be able to employ authentication on time. We consider both IEEE 802.11 and LTE standards and integrate them with the SDN-based recovery schemes.

In order to evaluate efficiency of the proposed framework, we utilized Mininet [8]. Since Mininet does not support authentication protocols, we integrate them with Mininet by simulating the link behavior on a network simulator, namely ns-3. Specifically, we implemented mutual authentication in ns-3 among two IEEE 802.11 nodes and two LTE user end devices (UEs) that connect via an LTE base-station (a.k.a

978-1-5386-4790-5/18/$31.00 ©2018 IEEE
Authorized licensed use limited to: FLORIDA INTERNATIONAL UNIVERSITY. Downloaded on May 07,2023 at 18:53:41 UTC from IEEE Xplore. Restrictions apply.

eNodeB). We then integrated these authentication protocols within the SDN-based recovery frame in Mininet.

In the experiments, we evaluated the performance of both IEEE 802.11 and LTE-based recovery by using Manufacturing Message Specification (MMS) standard data with both UDP and TCP protocols for reliability purposes. MMS is the core communication protocol of IEC61850 system [9] and can support real-time communications. We tested whether MMS data could be reliably transmitted when authentication is also involved. The results indicate that despite the overhead of authentication and slowness of reactive-based link failure detection approach (as opposed to a proactive one), IEEE 802.11 can still meet the end-to-end delays required by Smart Grid infrastructure (i.e., 100ms), which can be safely used in control communications and in MMS data transfers. LTE also performs similarly and misses only a few packets that cannot make the deadline. Additionally, TCP guarantees reliability while UDP shows a few packet losses.

II. Related Work

There are a number of SDN-based Smart Grid resilience studies that are published recently for different Smart Grid networks and applications such as link failure recovery based on the rate of packet losses for PMU networks [2], network delay guarantee and traffic prioritization for microgrid operations [3], and eavesdropping prevention in SCADA network [4]. Our work is different from these since we are targeting the inter-substation communications. Moreoever, in [5] and [6], the authors used SDN for failure detection and rerouting the traffic using the available redundant links. Our work is different as well since we introduce wireless or cellular link as the backup link. Moreover, all these works do not consider the authentication overhead.

LTE has been considered for different kinds of Smart Grid applications. For instance, the first experimental results were provided for LTE integration of automation of Smart Grid in [10]. The authors observed the Round Trip Time (RTT) is usually below 100 ms that will make LTE usage possible in most of the grid automation communications. In [11], the authors proposed usage of LTE networks for Smart Grid distribution networks. They considered smart metering and remote control communications applications by using MMS protocol stack. Their simulation results show that LTE can support requirements of these applications by exchanging mix background traffic. Different from these works, our paper considers the impact of authentication process when LTE is used in inter-substation communications.

III. Secure SDN-based Inter-substation Network

Smart Grid has three main components: the power generation, power transmission, and power distribution. For transmission and distribution, substations at different geographical locations are used. There are applications which may necessitate intra- or inter-substation communications and thus the communication architecture supports such needs via usually wired or wireless links.

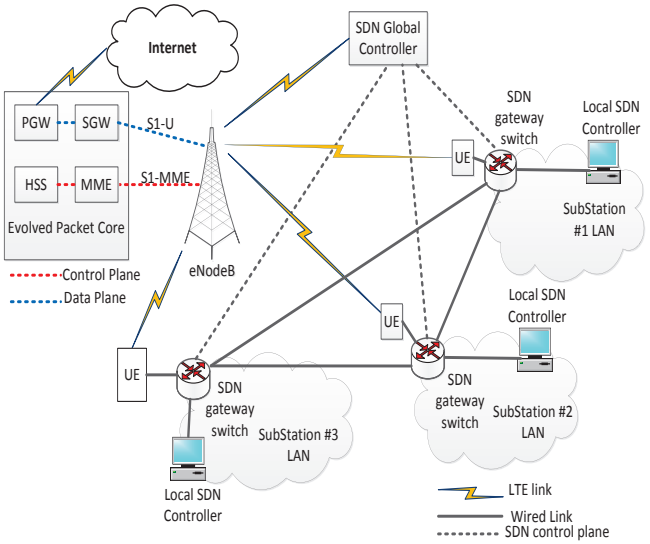


Fig. 1: Proposed SDN-based LTE redundant links model for substation communications.

In this section, we describe our SDN-based redundant wireless link model that includes the mutual authentication to ensure that only legitimate devices are able to access to the substation network after any link failures. Our model discussed is an extension from our proposed SDN-model for resilient inter-substation communications [7] which did not cover authentication features. We describe these authentication features next under two wireless links options: LTE and IEEE 802.11.

A. Proposed LTE redundant link Model

Fig. 1 shows the proposed LTE redundant link model. We consider each substation with an SDN switch that will be connected to SDN controller in a control center. Every SDN switch is connected to a UE (User Equipment) as the redundant link that will be used whenever the wired link goes down. To ensure that legitimate devices are connected, they need to do a mutual authentication with the public LTE network.

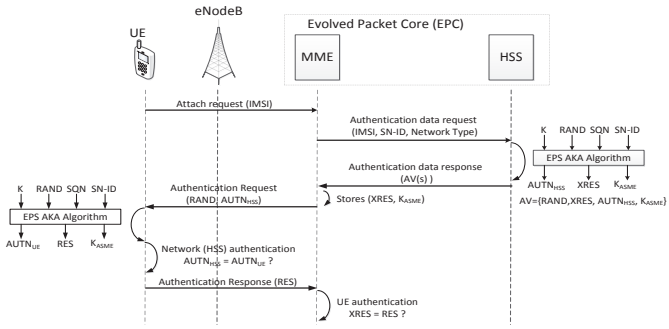


Fig. 2: LTE mutual authentication

The mutual authentication process from a UE and an LTE public network are depicted in Fig. 2. Typically, a SIM card stores a pre-shared master key K and a unique International Mobile Subscriber Identity (IMSI). Mutual authentication between a UE and an LTE public network is performed through

Authorized licensed use limited to: FLORIDA INTERNATIONAL UNIVERSITY. Downloaded on May 07,2023 at 18:53:41 UTC from IEEE Xplore. Restrictions apply.

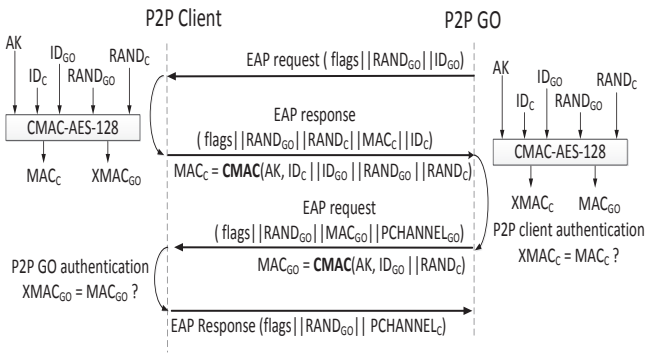


Fig. 3: IEEE 802.11 peer-to-peer mutual authentication. Note that the figure only shows the mutual authentication cryptographic operations and does not show the cryptographic operations of the protected channel.

an Evolved Packet System Authentication and Key Agreement (EPS AKA) mechanism [12] with the Milenage algorithm set [13]. This mechanism is basically a challenge response mechanism with an additional security using a pre-shared master key K on top of it. The mutual authentication is performed through three-message exchanges between a UE and an Evolved Packet Core (EPC) network as follows:

1) An attach request, which contains an International Mobile Subscriber Identity (IMSI) of the UE, is sent from the UE to the Mobility Management Entity (MME) in the EPC network;
2) An Authentication request (i.e., a challenge message) is sent from MME to UE;
3) An Authentication response is sent from UE to MME.

B. LTE Base-station Authentication

The disaster situations may damage the LTE base-station and thus we also consider the situation where the LTE provider must provide a temporary LTE base-station such as using a drone to restore the eNodeB base station functionality. For this case, the base-station must be pre-authenticated first by the LTE provider before it can be used. The authentication is performed as part of IP Security (IPsec) [14], the IP network security protocol for LTE control plane that provides a set of security services (e.g., access control, data integrity, anti-replay protection, data origin authentication, and confidentiality). These security services require the use of cryptographic keys that can be manually or automatically distributed using Internet Key Exchange version 2 (IKEv2) [15]. One option for the creation and maintenance of keys is to use public key infrastructure (PKI). However, if PKI is used and a new temporary base-station (i.e., drone) is deployed as defined in 3GPP TS 33.310 [16], certificate enrollment to Registration Authority/Certificate Authority (RA/CA) is needed. This may not be available in emergent cases and thus, we opt to use a pre-shared secret key that is pre-loaded before the drone flies.

C. Proposed IEEE 802.11 redundant link Model

We consider each SDN switch has a Wi-Fi Direct-enabled device [17] that supports single-hop direct device-to-device communications. Each device has the same disaster recovery key (i.e., a pre-shared key). When the wired link is down, both end WiFi Direct devices must form a peer-to-peer (P2P) group, which is functionally the same as an IEEE 802.11 infrastructure mode, and negotiating their roles, as a P2P group owner (P2P GO) that has the Access Point (AP)-like functionality, or as a P2P client through a three-way handshake. Note that this process is a one-time process and can be done in advance to save time for the applications which require meeting certain end-to-end delay times. After each role is determined, they perform mutual authentication using the Extensible Authentication Protocol - Pre-Shared Key (EAP-PSK) protocol [18] as depicted in Fig 3. Four messages exchanged for the proposed mutual authentication are as follows:

1) The P2P GO sends an EAP request message that includes its identity ID_{GO} to a P2P client;
2) The P2P client replies with an EAP response message that consists of a 16-byte random challenge $RAND_C$ created by the P2P client, the client identity ID_C, and a message authentication code MAC_C;
3) The P2P GO sends another EAP request message that consists of a MAC_{GO} and a protected channel $PCHANNEL_{GO}$ setup;
4) The P2P client replies an EAP response message with $PCHANNEL_C$ to finish the setup.

The mutual authentication is successful if the P2P client can present the correct MAC_C to the P2P GO and the P2P GO can present the correct MAC_{GO} to the P2P client.

D. Proposed Link Failure Detection

An important mechanism that is part of the entire recovery process is how to detect the failures in the links promptly so that SDN switch can take immediate actions. Two types of approaches are possible: (1) the reactive solution (also known as the restoration approach) and the proactive solution (also known as the protection approach) without any SDN controller intervention.

In the reactive solution, the SDN controller sends Link Layer Discovery Protocol (LLDP) packets periodically and update the flow tables if any of the link states has changed from the previous state. Thus, the recovery time will consist of LLDP packet transmission from Controller to switches, getting replies back, comparing the topology with the previous state, and updating the flows if necessary.

For the proactive solution, we can use the OpenFlow fast-failover groups that are supported after OpenFlow 1.1 . Specifically, a fast-failover group with watch ports is installed in all SDN switches before a failure occurs. Failure is detected by an SDN switch . Bidirectional Forward Detection (BFD) can be employed for the link failure detection in each switch. BFD is based on reception of hello messages between switches. If three consecutive messages are not received, then the switch will assume the link is down. Whenever a failure is detected, the SDN switch just uses the next available port for the next packets it receives.

Authorized licensed use limited to: FLORIDA INTERNATIONAL UNIVERSITY. Downloaded on May 07,2023 at 18:53:41 UTC from IEEE Xplore. Restrictions apply.

When authentication is also considered, the failure detection approach to be picked becomes an issue. Specifically, a proactive approach is not suitable for authentication since SDN controller will not immediately learn about the failure and during this time the packets will be forwarded through the wireless backup links without waiting for the authentication process. This is an important issue that has never been considered in the previous works. We argue that the reactive approach should be used in order to enable authentication services before any packets are transmitted. Thus, we followed this approach and conducted experiments as discussed in the next section.

IV. Experimental Evaluation

A. Experiment Setup

To assess the overhead of authentication on our proposed SDN-based recovery mechanisms, we extended our previous work on the integration between Mininet and ns-3 for the wireless redundant link in [7] to support the LTE link between SDN switches. We also integrated the authentication protocols discussed in Section III. We used FloodLight as the SDN controller. We assumed to substations communicating to each other. For a fair comparison, we set the same distance of 100m for both the IEEE 802.11n link and between the UE and the base station. We used MMS data sent from one substation to the other. MMS works above the IP layer and thus both UDP and TCP can be used as a transport layer protocol. Thus, we tested both UDP and TCP as the transport protocols.

As a benchmark, we used a topology whose backup link is assumed to be wired. In other cases, the backup link is assumed to be the proposed IEEE 802.11n or LTE. We labeled these three type of links as **Wired**, **Wireless**, and **LTE**, respectively.

We implemented both reactive and proactive link failure detections for comparison. LLDP transmission rate was 25ms in the reactive case and BFD session was set to 1ms in the proactive case. We used 4ms packet frequency with 30secs simulation time and the link failure is assumed at the 15th second of the simulation. We repeated the experiment 50 times for statistical significance.

B. Performance Metrics

As for performance metrics, we considered the following:

1) *End-to-end Delay (ETE Delay)*: This is the main delay each packet is experiencing in the network from one substation to another.
2) *Switching Delay*: It consists of the *Recovery Time*, the time spent for failure detection and updating the flow rules; and the *Authentication Time*, the time it takes to perform mutual authentication between two substations.
3) *Packet Loss*: This metric is to assess the number of lost packets if any.

TABLE I: Performance Results (in ms)

Link Type	***Recovery Time***		***Authentication Time***	***ETE delay***	
	Reactive	***Proactive***		TCP	UDP
Wired	50	4	N/A	0.18	0.15
Wireless	65	13	6	0.48	0.46
LTE	78	37	43	0.91	0.72

C. Performance Results

1) End-to-end Delay: From Table I, we observe that **Wireless** and **LTE** have longer ETE delays than the **Wired**. This is expected as wireless can support limited bandwidth compared to Ethernet. However, we see a major difference between **Wireless** and **LTE**. This can be attributed to the fact that IEEE 802.11n can support up to 600MB/s within shorter distances (e.g., 100m) while **LTE** supports 300Mbps downlink and 75Mbps uplink but with longer distances (possibly about 100 kilometers) [19].

As these presented values are average, we also analyzed the worst-case scenarios for the end-to-end delay in order to understand the behavior of the network under TCP and UDP protocols. Thus, we collected data during the time of the link failure. Using this data, we basically displayed the end-to-end delay values for both **Wireless** and **LTE** approach for each packet under TCP and UDP between 13-17 seconds of the experiment in Figures 4 and 5. We see from these figures that end-to-end delay value jumps at the link switching moment since packets require waiting for the connection to be set.

Such waiting time depends on the underlying transport protocols. As UDP and TCP have different behaviors in terms of establishing connections, we further analyzed the status of TCP packets at the switching time by using Wireshark to investigate how TCP treats the connection when the links fail. Sample TCP packet retransmissions were shown in Fig. 6. As can be seen in Fig. 6, TCP packets are retransmitted in case they cannot reach the destination. Specifically, what happens is that if a TCP packet does not get a reply within its round trip time (RTT), it will be retransmitted by the source. Furthermore, for the next packets, the waiting time will be doubled per TCP protocol guidelines.

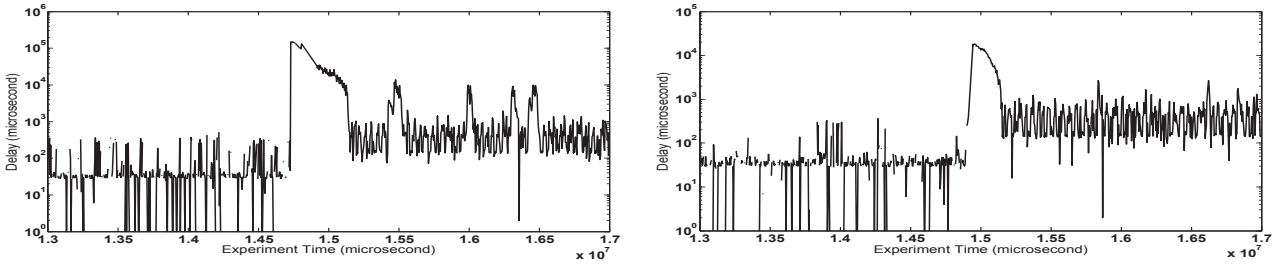
2) Switching Delay: Next, we analyzed the switching delay by separately measuring the recovery and authentication delays. Our results are shown in Table I. We presented the average recovery delay according to different times of periods and the **Wireless/LTE** switching delays by considering authentication times in Table I.

The results for overall switching times for reactive link failure detection experiments can support message type 3 of Smart Grid even in cases of a disaster according to [20]. While LTE authentication delay is much more than IEEE 802.11n authentication, on average it is still within the boundaries of 100ms delays for MMS applications, which is promising.

Note that for the proactive case, the authentication time overhead is assumed to be none as it cannot support authentication. Its recovery time is much better and thus can be considered for more time-constrained applications such as Generic object oriented substation events (GOOSE) [9]. However, in such cases, there need to be some sort of pre-authentication or trust mechanisms among the substations.

3) Packet Loss: The packet loss results are shown in Table II only when UDP is used since there is no packet loss in TCP case. We showed our packet loss results in Table II whenever we use LTE connection between the substation

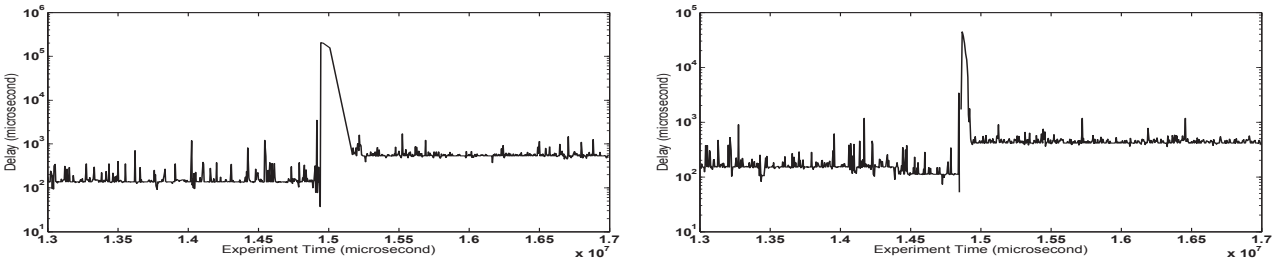
Authorized licensed use limited to: FLORIDA INTERNATIONAL UNIVERSITY. Downloaded on May 07,2023 at 18:53:41 UTC from IEEE Xplore. Restrictions apply.



(a) TCP protocol, controller checks every 25 ms

(b) UDP protocol,controller checks every 25 ms

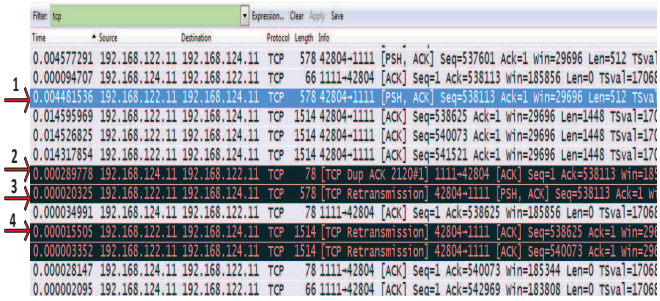
Fig. 4: End-to-end Delay packet distribution when LTE redundant link is used between the 13th and 17th seconds of the simulation, data rate is 4ms



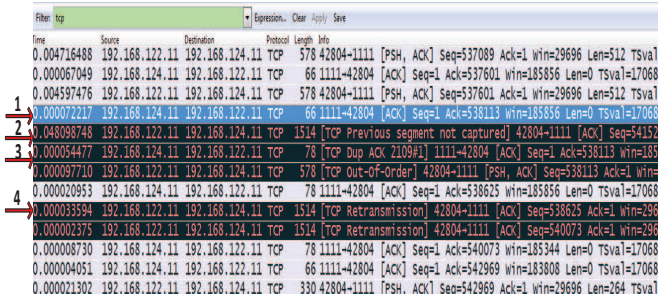
(a) TCP protocol, controller checks every 25 ms

(b) UDP protocol,controller checks every 25 ms

Fig. 5: End-to-end Delay packet distribution when IEEE 802.11n redundant link is used between the 13th and 17th seconds of the simulation, data rate is 4ms



(a) Switch 2 - eth1, connected to client. The controller checks every 25 ms. The 1st arrow is pointing to packet with sequence #538113 that can reach the destination and receive ACK properly. But it receives a duplicate ACK afterward as pointed by the 2nd arrow. Thus, the packet is retransmitted as shown by the 3rd arrow. Similarly, the packets shown by the 4th arrow are retransmitted as well since they have bigger sequence numbers (i.e., problem occurred before they were sent).



(b) Switch 3 - eth1 connected to server. The controller checks every 25 ms. The packet shown with the 1st arrow has a sequence #538113 but the packet with sequence #541521 shown with the 2nd arrow is not the next expected packet. Thus, the server sends duplicate ACK for the packet with sequence #538113 as shown with the 3rd arrow. After that, we can see the TCP retransmission packets sent from the client are arriving at the switch connected to the server.

Fig. 6: Wireshark Observations for TCP packets at the switches during the link failures.

switches. While we see 6-19 packet loss in Wireless and 8-23 in LTE for reactive approach, in proactive approach, we can see only 0 (75% of the experiments) or 1 (25% of the experiments) packet loss for both cases in our experiments.

TABLE II: UDP Number of Packet Loss

Approach	*Wireless*	*LTE*
Reactive	6-19	8-23
Proactive	0-1	0-1

The proactive approach has the advantage of taking local action immediately without consulting with the SDN controller and thus it immediately switches to the wireless links. This is not the case for reactive which needs SDN controller involvement and this causes some packet losses. However, as mentioned before, the involvement of SDN controller is needed anyway to perform the authentication.

4) Further Traffic Analysis: In this subsection, we analyzed the behavior of the network more closely during the failure time under a variety of conditions and metrics. We discuss potential trade offs and present some suggestions.

First, we start by comparing UDP and TCP performance for handling the link failures. Fig. 4a and 4b show the end-to-end delay of each packet that is sent during the time frame of 13-17 secs where we have the link failure happening at time 15 sec. In Fig. 4a, we show the case where the Controller application checks the network every 25 milliseconds, the data rate of client is 4 millisecond and packets are sent by TCP sockets. On the other hand, in Fig. 4b the same configuration with UDP protocol is shown. Even though it is easily recognizable that the UDP case does not have large values of delays as in the TCP case, it still cannot transmit

Authorized licensed use limited to: FLORIDA INTERNATIONAL UNIVERSITY. Downloaded on May 07,2023 at 18:53:41 UTC from IEEE Xplore. Restrictions apply.

the packets for a few milliseconds. This can be explained by the fact that UDP has packet losses due to the link failure. These packets are not retransmitted as in the case of TCP and thus the only delay is associated with the waiting time of the link restoration. In the case of TCP, this is not the case. Some of the packets will be lost and thus the source will re-transmit them after the timeouts. This takes more time (e.g., comparing the transmission from the source after timeouts vs. transmission on the link after the links is restored). Additionally, the retransmission timeout (RTO) value will be doubled when packets do not arrive at the destination. This will further increase the waiting times for the source, which adds to the end-to-end delay value.

Next, we analyzed the cases with the used underlying wireless links and observed the behavior of Wireless 802.11n and LTE. The delay results are shown in Fig. 4 and 5. In Fig. 4a, we have Controller application period as 25 milliseconds with LTE back-up link, data rate of client is 4 millisecond and the protocol is TCP whereas it has the IEEE 802.11n backup link in Fig. 5a. In both cases, we can see that for about 50 milliseconds, the packets cannot be sent which we consider as recovery delay caused by the link failure. One of the big difference between LTE and IEEE 802.11n experiments is that LTE exhibits having more fluctuation. We believe this occurs mostly because there is a base station involved in LTE network. Therefore, there are two hops in the communication physically although logically there seems to be a single link. The packets need to travel different protocol stacks within ns-3, LTE, and Mininet logical nodes. Depending on the traffic and CPU availability, the waiting and processing times at these nodes may differ each time a packet is sent. Such a situation does not happen when IEEE 802.11n is used since the stations communicate via a single physical link and only ns-3 protocol stack is involved. Another possible reason is the way LTE provides access to the links. This is different from the random access used in IEEE 802.11n and may be different in case of downlink and uplinks. The wireless link does not make any differentiation between down and uplinks.

V. Conclusion

In this paper, we studied the impact of authentication on SDN-based recovery in Smart Grid communications. Specifically, we proposed two novel authenticated IEEE 802.11 or LTE back-up links which can be activated from the SDN Controller in a Smart Grid infrastructure whenever the failure occurs.

The extensive evaluation results indicate that SDN can provide seamless resiliency in case of the availability of redundant wireless IEEE 802.11 or LTE links for protocols such as MMS. Authentication can safely be supported when reactive detection mechanism is used with IEEE 802.11. Despite a minor delay increase and a few packet losses in UDP, the maximum packet delays are still within the bounds of monitoring applications. For TCP, we observed that there is a higher delay to restart transmissions due to packet retransmission feature of TCP.

VI. Acknowledgement

This material is based upon work supported by the Department of Energy under Award Number DE-OE0000779 and Florida Cybersecurity Center.

References

[1] F. Hu, Q. Hao, and K. Bao, "A survey on software-defined network and openflow: From concept to implementation," *IEEE Communications Surveys & Tutorials*, vol. 16, no. 4, pp. 2181–2206, 2014.

[2] D. Gyllstrom, N. Braga, and J. Kurose, "Recovery from link failures in a smart grid communication network using openflow," in *Smart Grid Communications (SmartGridComm), IEEE International Conference on*. IEEE, 2014, pp. 254–259.

[3] L. Ren, Y. Qin, B. Wang, P. Zhang, P. B. Luh, and R. Jin, "Enabling resilient microgrid through programmable network," *IEEE Transactions on Smart Grid*, 2016.

[4] E. G. da Silva, L. A. D. Knob, J. A. Wickboldt, L. P. Gaspary, L. Z. Granville, and A. Schaeffer-Filho, "Capitalizing on SDN-based SCADA systems: An anti-eavesdropping case-study," in *IFIP/IEEE International Symposium on Integrated Network Management (IM)*, May 2015, pp. 165–173.

[5] N. Dorsch, F. Kurtz, H. Georg, C. Hgerling, and C. Wietfeld, "Software-defined networking for smart grid communications: Applications, challenges and advantages," in *Smart Grid Communications (SmartGridComm), IEEE International Conference on*, Nov 2014, pp. 422–427.

[6] N. Dorsch, F. Kurtz, F. Girke, and C. Wietfeld, "Enhanced fast failover for software-defined smart grid communication networks," in *Global Communications Conference (GLOBECOM), IEEE*, 2016, pp. 1–6.

[7] A. Aydeger, K. Akkaya, M. H. Cintuglu, A. S. Uluagac, and O. Mohammed, "Software defined networking for resilient communications in smart grid active distribution networks," in *2016 IEEE International Conference on Communications (ICC)*, May 2016, pp. 1–6.

[8] B. Lantz, B. Heller, and N. McKeown, "A network in a laptop: rapid prototyping for software-defined networks," in *Proceedings of the 9th ACM SIGCOMM Workshop on Hot Topics in Networks*, 2010, p. 19.

[9] R. Mackiewicz, "Overview of iec 61850 and benefits," in *Power Systems Conference and Exposition. IEEE PES*. IEEE, 2006, pp. 623–630.

[10] P. Ferrari, A. Flammini, M. Loda, S. Rinaldi, D. Pagnoncelli, and E. Ragaini, "First experimental characterization of lte for automation of smart grid," in *Applied Measurements for Power Systems (AMPS), IEEE International Workshop on*, 2015, pp. 108–113.

[11] G. Karagiannis, G. T. Pham, A. D. Nguyen, G. J. Heijenk, B. R. Haverkort, and F. Campfens, "Performance of lte for smart grid communications." in *MMB/DFT*. Springer, 2014, pp. 225–239.

[12] 3GPP. 3GPP System Architecture Evolution (SAE); Security architecture (3GPP TS 33.401 version 14.2.0 Release 14) .

[13] ——. Specification of the MILENAGE algorithm set: An example algorithm set for the 3GPP authentication and key generation functions f1, f1*, f2, f3, f4, f5 and f5*; Document 2: Algorithm specification (3GPP TS 35.206 version 12.0.0 Release 12) .

[14] ——. Network Domain Security (NDS); IP network layer security (3GPP TS 33.210 version 13.0.0 Release 13).

[15] C. Kaufman, P. Hoffman, Y. Nir, and P. Eronen, "RFC 5996: Internet Key Exchange Protocol Version 2 (IKEv2)." [Online]. Available: http://www.rfc-editor.org/info/rfc5996

[16] 3GPP. Network Domain Security (NDS) Authentication Framework (AF) (3GPP TS 33.310 version 13.2.0 Release 13).

[17] D. Camps-Mur, A. Garcia-Saavedra, and P. Serrano, "Device-to-device communications with Wi-Fi Direct: overview and experimentation," *IEEE Wireless Communications*, vol. 20, no. 3, pp. 96–104, June 2013.

[18] "EAP-PSK protocol." [Online]. Available: https://tools.ietf.org/html/rfc4764

[19] M. J. Chang, Z. Abichar, and C.-Y. Hsu, "Wimax or lte: Who will lead the broadband mobile internet?" *IT professional*, vol. 12, no. 3, pp. 26–32, 2010.

[20] I. E. Commission *et al.*, *IEC 61850-5: Communication Networks and Systems for Power Utility Automation. Communication Requirements for Functions and Device Models. Exigences de Communication Pour Les Modèles de Fonctions Et D'appareils*. IEC, 2013.

Authorized licensed use limited to: FLORIDA INTERNATIONAL UNIVERSITY. Downloaded on May 07,2023 at 18:53:41 UTC from IEEE Xplore. Restrictions apply.