A Security Architecture for Automated Social Engineering (ASE) Attacks over Fiber-Wireless (FiWi) Access Networks

Mohammad Zohirul Islam mzislam@kth.se
Department of Computer and Systems Sciences
Royal Institute of Technology-KTH
Stockholm, SE-100 44, Sweden

Sarwarul Chowdhury chowdsi@emt.inrs.ca
Department of Telecommunications
University of Quebec
Montréal, QC H5A 1K6, Canada

Abstract

Future communication networks will integrate `SSS' concepts such as social networking, social networking device, and social desktop. In this paper, we focus on applications over social networking sites (SNS). Due to emerging bandwidth-hungry applications over SNS, hybrid fiber-wireless (FiWi) access networks are a promising solution to mitigate the last mile bandwidth bottleneck. SNS are particularly vulnerable to Automated Social Engineering (ASE) attacks due to their powerful information gathering functionalities. We discuss how integrated FiWi access networks supporting SNS systems perform, and how they can deal with threats related to ASE. In addition, we explain how an ASE attack may be launched from different networking platforms and propose a security architecture for ASE attacks over FiWi access networks.

Keywords: Social Networking Sites (SNS), Automated Social Engineering (ASE), Hybrid Fiber-Wireless (FiWi) Access Networks, WiMAX BS, EPON (ONU, OLT), ONU-BS.

1. INTRODUCTION

Future communication networks will enrich our lives by supporting enormous data rates for end users. Home networking will allow end users to access online games, video on demand, high-definition television, radio, audio, web, phone, alarm systems, home automation, and health care anytime, anywhere, and in any format by assisting consumers in maintaining their independence as they evolve from the same platform [1].

Future broadband access networks will be bimodal, capitalizing on the respective strengths of optical and wireless technologies and smartly merging them in order to realize future-proof fiber-wireless (FiWi) networks in support of a plethora of services for subscribers [2]. FiWi access networks mitigate the first/last mile and backhaul bandwidth bottlenecks, increase network coverage, and provide user mobility. In most of today's greenfield network deployments fiber rather than copper cables are installed for broadband access. Due to applications such as file sharing, chatting, audio, video, gaming, online communities over social networking sites (SNS), e.g., Facebook, bandwidth demands keep increasing day by day. Hence, home and access networks must not only support high-speed, plug-n-play, mobility, and QoS, but must also be scalable up- and down-market, and retrofit in home network installations, small business to large enterprise campuses, and from rural to urban areas, thus enhancing the revenue for operators and vendors. Despite their optical transparency, high capacity, and cost-saving benefits, FiWi networks may face operators and enterprises be unwilling to embrace them because of incurring compromises with security and privacy which may put their business at risk and may result in significant financial losses.

In this paper, we focus on automated social engineering (ASE) attacks over FiWi access networks. Social engineering is the art of exploiting the weakest link of information security systems as well as human factors to manipulate a person or group of people for the purpose of gaining access to sensitive information or systems. Attacks may also involve various kinds of technology, e.g., malware, e-mails, or manipulation of software. Future FiWi broadband access networks will not only provide quad-play services but also integrate applications and services of social networking sites such as Facebook, LinkedIn, Twitter, YouTube, Amazon, and MySpace on the same infrastructure, including additional applications such as medical care, e-governance, e-learning, weather forecasting, and traffic monitoring. As a consequence, social engineering attacks can be automated through these networking sites by means of different communication tools and protocols. According to [3]:

“Much like the current botnets, which are threatening due to their size and network communicating possibilities, the automated social engineering (ASE) bots will be threatening due to the fact that they will know so many people and so much about them. Their threat will lie in abusing the social networks, and not the Internet traffic networks.”

As users put their personal data in SNS, social engineering attacks can be automated. An attacker can use the subscriber's information as well as Internet bots to gather information and perform sophisticated ASE attacks. ASE bots require no human involvement and are scalable, thereby rendering social engineering a cheap and appealing attack [4]. SNS are an attractive platform for ASE attacks as they provide seamless services for a large number of users with a wide range of applications and socio-demographic characteristics. The aim of this paper is to develop and a security architecture for future broadband FiWi access networks that helps secure end users from ASE attacks and transfer the entire security solution to the networking devices such that the security credentials are set automatically during communications.

The remainder of the paper is structured as follows. Section 2 briefly reviews the state-of-the-art of FiWi access networks and discusses their security issues with an emphasis on ASE attacks. Section 3 introduces a holistic approach of ASE attacks over FiWi access networks via SNS. In Section 4, we will describe our proposed security architecture for ASE over FiWi access networks. Section 5 concludes the paper.

2. FIWI ACCESS NETWORKS AND SECURITY ISSUES

The state-of-the-art of FiWi access networks has been recently surveyed in [5]. The survey provides an overview of enabling FiWi technologies and recently proposed FiWi network architectures. Most of the proposed FiWi networks make use of low-cost Ethernet technologies such as IEEE 802.3ah Ethernet passive optical network (EPON) and IEEE 802.11 wireless LAN (WLAN), with a few exceptions deploying also IEEE 802.16 WiMAX. The survey highlights previously addressed challenges and outlines open issues of emerging FiWi networks. Among others, different FiWi network architectures as well as advanced path diversity, wavelength channel assignment, performance monitoring, fault management, load balancing, and reconfiguration techniques to improve the bandwidth efficiency and resilience of FiWi networks have been studied in depth.

Apart from the aforementioned optical and wireless technologies, next-generation FiWi networks will also have to incorporate emerging long term evolution (LTE) cellular and long-reach PON (LR-PON) technologies. LTE is an enabling technology for wireless access networks which helps improve their network throughput, coverage, and operational costs significantly. In comparison with WiMAX, LTE is able to reduce the round-trip latency to 10 milliseconds for both unpaired time division duplexing (TDD) and paired frequency division duplexing (FDD) [6]. Conversely, LR-PON introduces hybrid dense wavelength division multiplexing (DWDM)/time division multiple access (TDMA) techniques accommodating up to 32 different TDMA PONs. A LR-PON aims at supporting up to 16,000 subscribers over distances of up to 100km from a single network service node with 10Gb/s symmetric data rates in both upstream and downstream directions [7].

2.1 Security Issues in FiWi Access Networks

Designing security in wireless networks is a challenge. Among others, key security issues in wireless networks are the shared wireless medium, severe resource constraints, dynamic network topology, reliable and trusted infrastructure, open peer-to-peer network architecture, roaming, handover as well as interference in co-channel and adjacent cells. These issues cause a range of vulnerabilities and threats in wireless networks such as Denial-of-Service (DoS), sniffing, snooping, masquerading, signal jamming, traffic analysis, network injection and partition, message modification, man-in-the-middle, and wardriving attacks [8], [9].

Security issues have also been studied in optical networks considering different scenarios such as in-band-jamming, out-of-band jamming, gain competition, tapping attacks, channel attacks, denial and theft of service, eavesdropping, and masquerading. For detecting and preventing these threats and security holes in optical networks, a variety of authentication and encryption protocols may be used, e.g., Rivest Shamir Algorithm (RSA), Advanced Encryption Standard (AES), and Elliptic Curve Cryptography (ECC) [10], [11].

Until now, security has been mostly studied separately either in wireless or optical networks. No profound research activities have been conducted on security in integrated FiWi networks so far. All aforementioned security issues also apply to FiWi networks. Note, however, that FiWi networks may suffer from a number of specific security threats which can be categorized into terminal security, network security, and channel security. To protect FiWi networks against different threats and provide secure access, a multilayer strategy spanning all network layers is required. Heterogeneous networks in general and FiWi networks in particular introduce security issues like mutual authentication, device identification, data integrity, access control, and denial-of-service. Moreover, other challenging issues like efficient call handover, session initiation, dynamic bandwidth allocation, and congestion control are also becoming considerably vital from a network management point of view for heterogeneous networks. Specific security issues that might arise in FiWi networks include first/last mile security (inter-domain security), managing secure moving application sessions, secure context transfer, zero-day vulnerabilities, buffer overflows, structured query language (SQL) injections, separate IP authenticity during each handover, validation of different data rates, and interception. In this paper, we will focus on ASE attacks over FiWi access networks which come in the following three flavors:

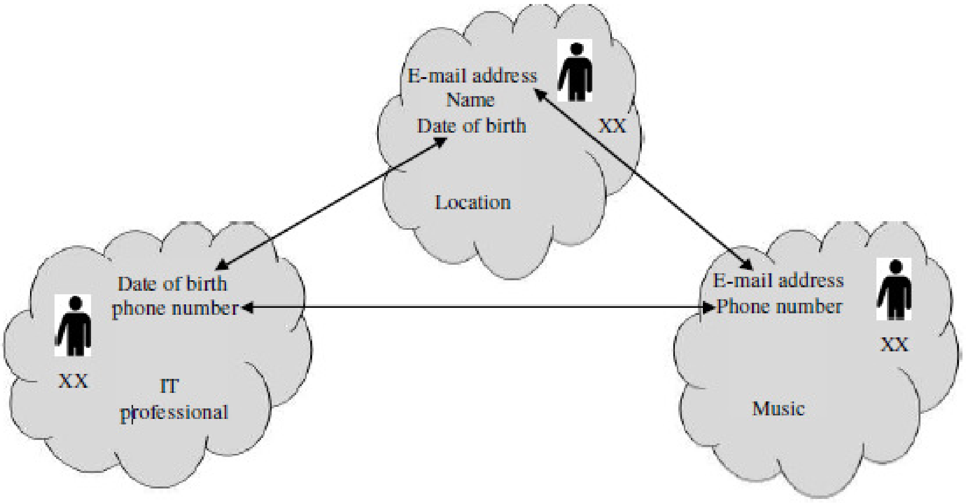


FIGURE 1: Cross-network information aggregation.

ASE attacks over SNS: SNS are becoming increasingly popular. They represent a promising platform for companies to advertise their products to a huge number of users. With the powerful development of search engine techniques, online communities, and user groups, personal information can be disclosed and modified by malicious users. Even though current SNS maintain a certain level of security, they fall short to protect each user's profile privacy. Due to out-of-context information disclosure, in- and cross-network information aggregation, and software bugs it is easy to gather personal information via chatting, spam, Internet bots, malware, data mining, and phishing from SNS. Hence, social engineering attacks may be done automatically through SNS [4]. ASE attacks over SNS may also occur through face recognition, social viruses and worms, and stalking (unwanted attention by individuals and sometimes groups of people to others for harassment and intimidation). Conversely, some other powerful techniques like cross-site scripting (code injection by malicious web users), cyber-bullying and grooming, corporate espionage, and infiltration of networks leading to information leakage, may be used for ASE attacks. For illustration, Figure 1 shows a cross-network information aggregation technique with a significant amount of member overlap across three different social networks based on location, IT professional, and music through common interest, choice, and hobbies. Users of multiple social networks may not want information of different contexts to be mixed up with each other. For instance, in Figure 1 user `XX' provides information such as his or her e-mail address, name, and date of birth in an SNS based on location, whereby the date of birth is shared with another SNS (IT professional). Similarly, the home phone number is available in SNS Music. Given the increasing use of SNS and powerful development of information retrieval processes (interconnection of SNS with Google) it is easy for an attacker to aggregate information from connected sources in order to acquire information related to the privacy of user `XX'.

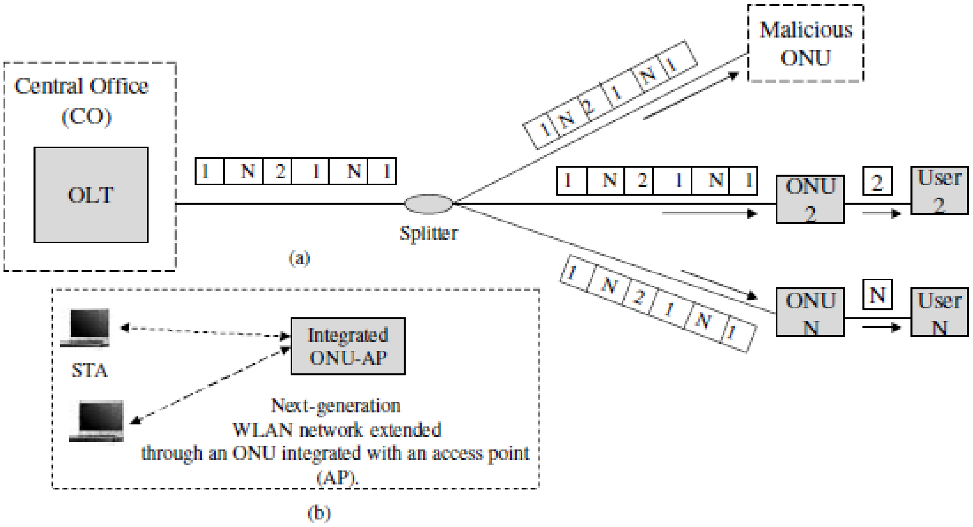


FIGURE 2: Malicious ONU monitors downstream transmissions from OLT to ONUs in a broadcast EPON.

ASE attacks over networking devices: A FiWi access network convergence different optical and wireless technologies. Due to the convergence of different technologies and dissimilar networking protocols, ASE attacks can be launched at FiWi networking devices such as EPON optical network units (ONUs) or WLAN access points (APs). As shown in Figure 2(a), a malicious ONU can analyze all downstream packets coming from the central optical line terminal (OLT) due to the broadcast nature of EPON. Hence, a malicious ONU may gather sensitive network information like logical link identifiers (LLIDs), medium access control (MAC) addresses, and device identities of APs, leading to serious ASE threats to networking devices. A malicious ONU or its attached users may inject malicious code to the networking devices and collect information about the network. Moreover, it may also set up an ASE bot in the network to collect information related to network resources like bandwidth allocation and transmission time. ONUs act as a packet filter to forward packets to authorized users. For example, in Figure 2(a), ONU 2 filters packets intended for user 2, though it receives all packets broadcast by the OLT. Figure 2(b) depicts a FiWi network based on an ONU integrated with a next-generation WLAN AP. Due to the broadcast transmission properties of the AP, the identity of wireless users and AP are vulnerable in an open network with wireless extensions. Moreover, communication channels between wireless station (STA) and integrated ONUs can also be hijacked by malicious users. Hence, network optimization, security credential, and a bandwidth management plan is required at the central office (CO) to eliminate sophisticated ASE attacks.

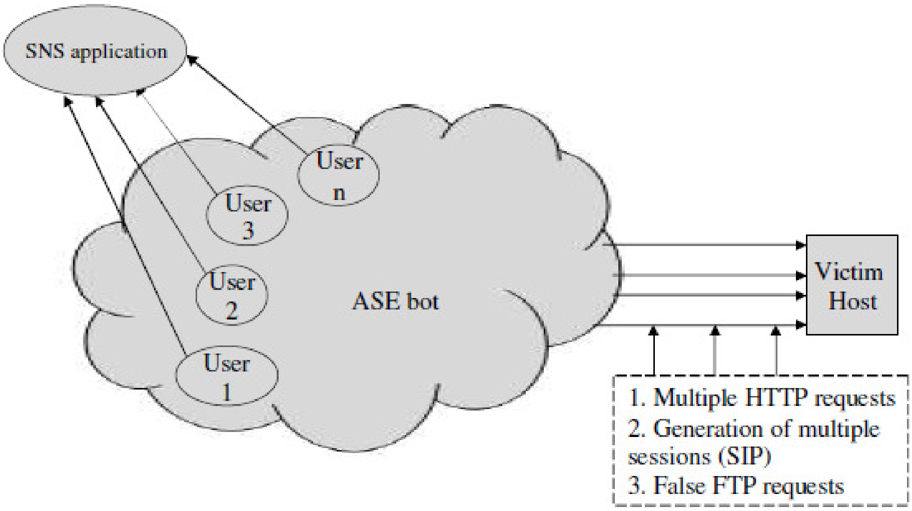


FIGURE 3: Users execute a malicious application in an SNS subsequently generate a series of different requests such as HTTP, FTP, and multiple sessions to target the victim host.

ASE attacks from end users: SNS provide all the essentials needed for the easy deployment of applications. It may happen that a group of malicious users can develop SNS applications such as a quiz, IQ test, or game, and add them to the account. A user who wants to use such a type of application causes a serious security threat. On the other hand, malicious users and groups may create several groups and invite people to join them in order to collect the information required for creating ASE attacks. Moreover, most of the SNS applications can be developed in personal home page (PHP) or Java. Developers may use information such as the name of the application, the IP address of the web server, and submit it to the server. Hackers may manipulate the communication between server and developers by introducing web bugs through this type of page submission. Basic tools for ASE attacks from end users in SNS include the following: (i) ignorance about IT security due to a very large and highly distributed user base; (ii) same application (developing the trust with each other), resource (asking for access to the same resource), or information (the same social interests); (iii) SNS platform attracts users to install unwanted applications; (iv) friendliness, showing confidence in an idea and impersonation; and (v) open gateway for hackers to develop applications to gather information through ASE bots. Figure 3 illustrates how an ASE bot may work in an SNS through multiple images, text files, session initiations, and HTML pages. When multiple users interact with the same applications, the victim host may receive unsolicited requests. These requests are triggered through the SNS. The SNS application used by the users (generated by the Web browser) and local devices execute the application. Hence, when multiple users act through the same application and generate multiple sessions or HTTP requests in the application, they create a malicious SNS application defined as an ASE bot. An AS E bot is depicted in Figure 3, where the cloud illustrates a collection of SNS users browsing a malicious application in the SNS. This causes a series of requests to be generated and directed towards the victim [12].

2.2 ASE over FiWi Access Networks

Figure 4 illustrates the convergence of next-generation EPON with WiMAX/LTE BS for different scenarios [13]. The most intuitive way to integrate EPON and WiMAX/LTE is to use independent architectures where EPON and WiMAX/LTE systems are operated independently by considering a WiMAX/LTE BS a generic user attached to an ONU. The two devices may be interconnected via a common standard interface, e.g., Ethernet. The hybrid ONU-BS architecture is an enhanced approach to integrate an ONU and a WiMAX/LTE BS in a single box (ONU-BS), as illustrated in the lower ONU of Figure 4. The connection-oriented architecture is a more complex convergence approach due to the different transmission properties of WiMAX and LTE. WiMAX is a connection-oriented transmission technology where each service flow is allocated a unique connection ID (CID). In contrast, EPON does not support connections and bandwidth requests are queue-oriented. The OLT allocates bandwidth to each ONU, and then the latter one makes a local allocation of the granted bandwidth to up to eight different priority queues.

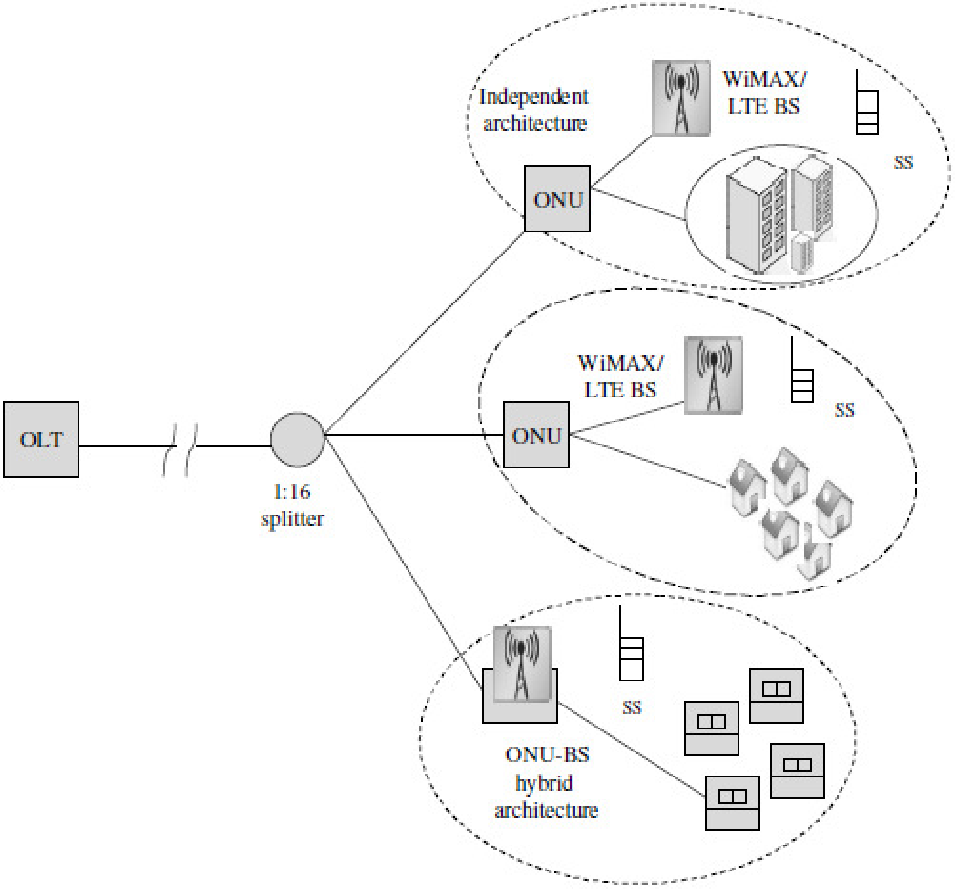
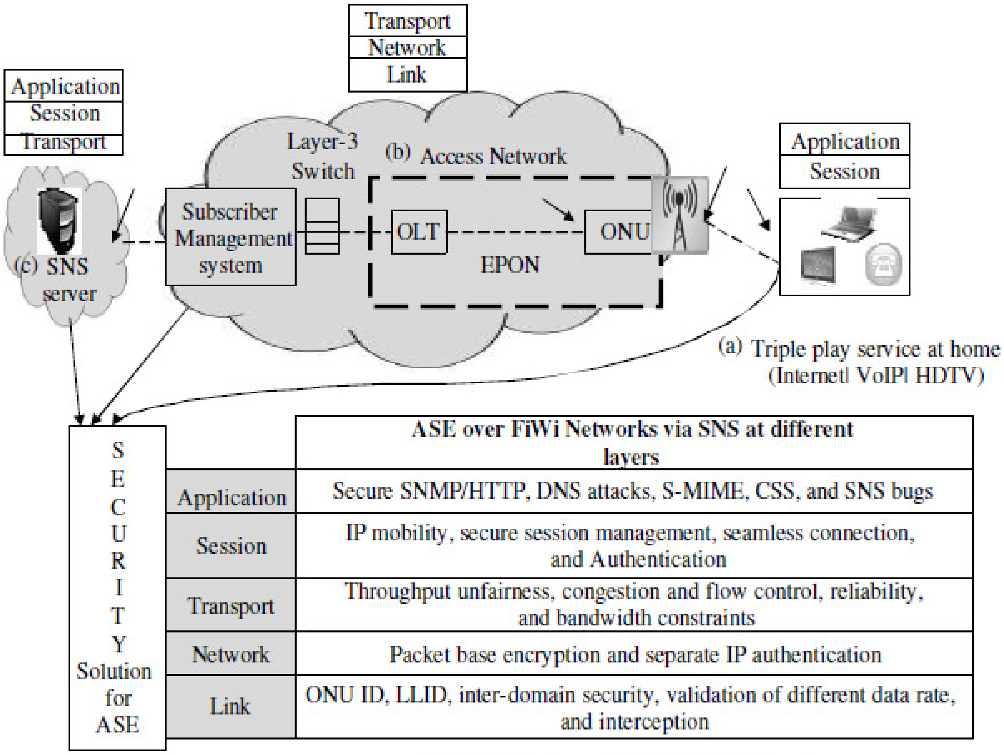


FIGURE 4: Convergence of next-generation EPON and WiMAX/LTE base station (BS) [13].

There are vulnerabilities of ASE attacks for all aforementioned integration processes. In WiMAX/LTE networks, identity theft is a severe threat to unlicensed services supported by WiMAX/LTE. A fake device can use the hardware address of another registered device by intercepting management messages over the air. Once succeeded, an attacker can turn a BS into a malicious BS. A malicious BS can imitate a legitimate BS by hijacking the associated SSs and gather the information about the entire network which poses a serious threat of ASE attacks. In integrated systems, each SS uses the dynamic host configuration protocol (DHCP) to obtain an IP address from the DHCP server, which can be attached to the central OLT or a remote ONU-BS.

The following two packet/frame forwarding techniques have been proposed for integrated EPON-WiMAX/LTE networks [13]: (i) network-layer IP packet routing and (ii) link-layer Ethernet frame switching. There is a range of security threats related to ASE attacks for the two aforementioned packet/frame forwarding techniques. First, the DHCP server should not be located at an insecure location such as the OLT. Usually, the CO maintains the IP addresses of all SSs. An ASE bot (through a malicious ONU) can control the DHCP server due to the lack of authentication of ONUs. Hence, end-to-end security solutions are required to assign IP addresses to SSs from the CO. Moreover, IP packets are sent by the user without encryption to the access router. Hence, other SSs can falsify the identity of SSs, resulting in a serious threat of ASE attacks to the entire network. Similarly, due to the loop-back fashion of the network-layer solution, time constraints of accessing networking resources are an important factor for SSs to eliminate the attacks related to ASE.



	ASE over FiWi Networks via SNS at different layers
Application	Secure SNMP/HTTP, DNS attacks, S-MIME, CSS, and SNS bugs
Session	IP mobility, secure session management, seamless connection, and Authentication
Transport	Throughput unfairness, congestion and flow control, reliability, and bandwidth constraints
Network	Packet base encryption and separate IP authentication
Link	ONU ID, LLID, inter-domain security, validation of different data rate, and interception

(d) A holistic view of ASE in FiWi Networks.

FIGURE 5: A holistic view of ASE attacks over FiWi networks via SNS.

Conversely, in the link-layer solution, Ethernet frame and IP packet downstream transmissions without encryption cause a security threat to SSs and integrated ONU-BSs. In this solution, Ethernet frames are switched based on MAC addresses. Therefore, the coherence and synchronization between two access routers (associated with OLT and ONU-BS) are required, otherwise MAC addresses may be falsified. Due to the different traffic patterns (in-microcell/out-microcell) of SSs, ONU-BSs need to prioritize traffic instantly to allow an access router to provide access to network recourses. Consequently, a malicious SS/ONU-BS can hijack the traffic pattern in order to access the network. Moreover, in both scenarios, IP and MAC addresses are sent across a public network, causing insecure communication for networking devices (Ethernet bridge and access router) to maintain an appropriate routing table (IP addresses and MAC addresses), to manage network resources, and to ensure security credentials for authorized users, ONUs, and BSs.

3. A HOLISTIC VIEW OF ASE ATTACKS OVER FIWI ACCESS NETWORKS VIA SNS

A holistic approach against ASE attacks over FiWi access networks carried out through SNS is shown in Figure 5. This approach aims at improving the performance of FiWi access networks with respect to security, longevity, optimization, and connectivity. Figure 5 (d) depicts a variety of security holes and vulnerabilities in FiWi networks occurring at from different networking layers. Security has to be ensured at all the layers of the protocol stack while the cost for ensuring security should not surpass the assessed security risk. A holistic network are shown in Figure 5: (a) home network for end users and mobile subscribers, (b) access network (convergence of EPON with WiMAX/LTE BS), and (c) SNS platform. The failure of inter-domain security and link-level identification may seriously affect the entire network to gather the information, possibly resulting in sophisticated ASE attacks.

Usually, these failures occur at network gateways. Hence, four main gateways (home users, ONU-BSs, transmission between OLT and ONU-BSs, and SNS) have been marked with an arrow. Let us assume that a traffic stream, shown by dotted lines, is generated by the SNS server, traverses core and EPON networks, and finally reaches the end users. In FiWi networks, per-flow QoS cannot be maintained in the core. This function must be performed at the edge of the network near the end users, e.g., EPON. We propose a layer-3 switch to carry best-effort web access traffic originating from SNS. It will ensure the per-flow serv ice level agreement (SLA) enforcement and prioritizing (high-bandwidth flows, traffic type, and congestions) the tr affic of the subscriber management system.

In Figure 5, the SNS server uses hypertext transfer protocol (HTTP) cookies and hidden form fields to maintain the authentication, access control, and authorization state after successful login to an SNS. The HTTP cookies contain session information while the hidden form fields ensure that forms are submitted by users and are protected against cross-site request forgery attacks. Since the hidden form values are partly created by JavaScript, this authentication method also blocks bots that are not JavaScript compatible. Third-party applications represent an additional attack which could be exploited by an ASE bot for malicious actions, e.g., to launch distributed DoS attacks or to gather personal information about future victims [12], [14], involving security issues like authorization, access control, and confidentiality for ASE attacks over SNS.

Figure 5 also shows various attacks at different networking layers related to ASE over FiWi networks. For example, at the application layer, in DNS attacks related to ASE an attacker exploits cross-site request forgery (CSRF) vulnerability by triggering a victim to visit a malicious page (SNS). The page will consist of specially crafted `xslt' requests designed to perform some action on the attacker's behalf. An attacker can exploit this to perform DNS poisoning attacks through the `NAME' and `ADD' parameters. Similarly, at the link layer, LLIDs need to be protected in all frames from being listened or attacked by a malicious user at an EPON downstream link. Moreover, separate IP authentication in the upstream direction (from end users to integrated ONU-BS) will also necessary to be protected.

Most of the SNS have implemented automated mechanisms to detect abusive behavior during communications. However, these mechanisms are not enough to provide security. Therefore, the subscriber management system needs to report about abusive behavior to the layer-3 switch in order to block traffic immediately. Once a possible abuse of an SNS feature is detected users are warned and if they don't adapt their using habits their accounts get permanently disabled. Security metrics that might detect an ASE bot are as follows: (i) fake names in profile, e.g., nicknames, (ii) exceeded rate limits to join or invite people in groups, messages on walls and groups, messages sent to other users, new friends, and accessed profiles, (iii) duplicate t ext in multiple messages to detect spam messages, and (iv) web scraping such as browsing speed [4].

4. SECURITY ARCHITECTURE FOR ASE

We propose a new security architecture for FiWi networks, in order to guarantee secure communications in access networks and avoid ASE attacks. This architecture is proposed only for the access network (OLT to ONU-BS) of Figure 5. The architecture ensures secure communication in both upstream and downstream for each frame sent and received by the OLT and ONU-BS, respectively. Figure 6 depicts the four different modules of our proposed architecture: (a) Encryption Module, (b) Packet, Frame, and Secure payload (PFS) Module, (c) Traffic Analyzer and Confidentiality, Integrity, and Authentication (CIA) Module, and (d) Controlling Module. Figure 6 illustrates in greater detail how frames are managed within the access network in a secure way. The functionalities of each module are as follows:

Encryption Module: The encryption module consists of a parameter set, key management & generation, and link management interface (LMI). The parameter set and key management & generation will set the parameters, e.g., initiation vector (IV), AUTH code, and keys for insecure frames. The AUTH code will be generated by the LMI, including negotiation of the parameter set and key generation for each frame. A statistical report will be stored to compare the transmission time between upstream and downstream traffic for future authentication. *PFS Module*: The PFS module is a combination of payload, frame framer, and packet multiplexer/de-multiplexer (MUX/DMUX). A frame framer encapsulates data received from the advanced encryption standard in counter-mode (AES-CTR) with a MAC header. Subsequently, every frame will be checked for its identity using the CIA module and is scheduled by the downlink (DL) scheduler for transmission to avoid congestion in the network. *Traffic Analyzer & CIA Module* : The traffic analyzer & CIA module is an integration of different modules such as traffic auditing & management module, fault and alarm management module, authentication and access control module. The traffic auditing module monitors the transmission of different frames between OLT and ONU-BS. If any abusive traffic travels across the access network, it will be immediately report to the fault management module in order to discard the frame. The authentication and access control module checks the fundamental security parameters like confidentiality, integrity, authentication, and access control on a per-frame basis in both upstream and downstream directions. *Controlling Module:* The controlling module is a combination of OLT& ONU-BS controller, CPU, and mapping unit. This module is responsible for blocking abusive traffic, checking the security credentials of users, traffic going to encoder or coming from decoder, man aging the functionalities of other modules, and monitoring the control messages generated by ONU-BS and OLT.

Beside this, the frame encoder/decoder delivers/receives the payload to/from the advanced encryption standard AES-CTR module. AES-CTR generates a unique per-frame value for each payload and communicates this value to the frame MUX/DMUX for upstream or downstream transmissions. It checks the identity of each ONU-BS or subscriber's transmission through the identity check module. The same IV and key combination must not be used more than once. The IV used here is 64 bits long (8-octets) with a key size of 128 bits (10 rounds). It also receives an instruction for AES-CTR from the parameter set in order to perform authenticated encryption. This approach can protect against eavesdropping attacks by deploying encrypted LLID header for each logical link, whereby the header is encrypted separately with a different IV for each encrypted packet prior to upstream transmission. Hence, attackers are unable to obtain the MAC address or LLID and to masquerade as another ONU.

Upon the reception of frames, the frame analyzer examines them, and forwards insecure fames for encryption on the basis of their LLID. The transmission time, AUTH code value, and key parameters are stored as a statistical report, thus guaranteeing secure transmission.

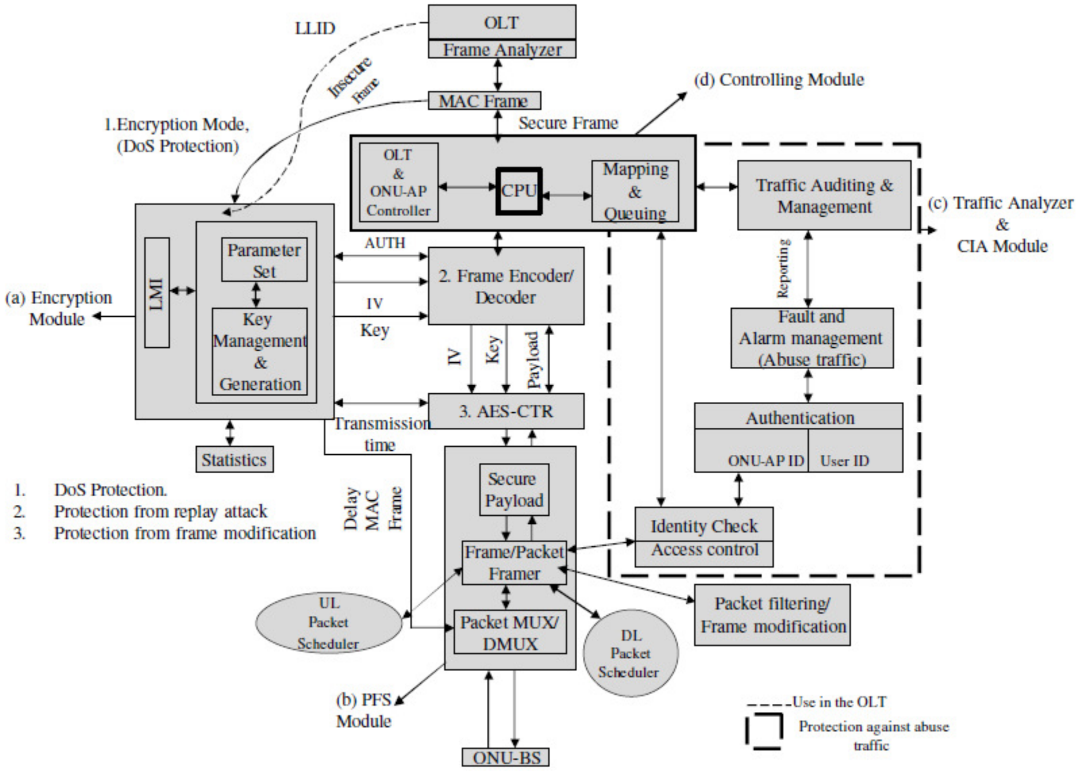


FIGURE 6: Security architecture for ASE over FiWi networks.

Our proposed security architecture ensure protection against ASE attacks in the following way: 1) The architecture protects against eavesdropping attacks by using an encrypted LLID header for each logical link. Hence, attackers cannot obtain the MAC address or LLID. 2) During transmission, each transmission window will be checked through the AUTH code of the previous statistical report. As a result, primary resources (transmission time and bandwidth) are protected from DoS attacks, which in turn reduces the risk of ASE attacks. Moreover, attackers cannot inject automatic malicious code in upstream transmission due to the use of a separate AUTH code, IV, and transmission time for each window. 3) Attackers cannot set up an ASE bot in the access network due to the link level identity and per-frame based access control. Furthermore, all traffic in upstream and downstream direction will be audited to reduce the vulnerabilities of abusive communications. Hence, the controlling module obtains a complete traffic scenario from the traffic management system in order to take action immediately. 4) The IP addresses from the DHCP sever (associated with the CO) are transmitted separately after assigning an LLID to each ONU. This mitigates the risk of IP spoofing. Moreover, all the packets undergo a filtering process in the downstream direction to assure the subscriber's identity.

5. CONCLUSION

FiWi access networks hold great promise to support future broadband services and applications on the same infrastructure. Similarly, SNS are a promising approach to merge end-user applications. However, security is a severe obstacle in FiWi networks and SNS because of automatic engineering and powerful information retrieving tools in today's networks. We discussed ASE attacks over FiWi networks and explained how they may occur at different networking layers. We proposed a security architecture following a multi-layer strategy that examines the traffic in both directions and extracts abusive traffic of applications run over SNS. Several fundamental security issues like CIA and access control are addressed by our proposed security architecture for FiWi access networks.

6. REFERENCES

[1] J. Prat, “Next-Generation FTTH Passive Optical Network s: Research towards Unlimited Bandwidth Access,” *Springer* , 2008.

[2] M. Maier, N. Ghazisaidi, and M. Reisslein, “The Audacity of Fiber-Wireless (FiWi) Networks (Invited Paper),” *in Proc., ICST ACCESSNETS,* Las Vegas, NV, USA, Oct. 2008.

[3] M. Nohlberg, S. Kowalski, and M. Huber, “Measuring Readi ness for Automated Social Engineering,” *in Proc., 7th Security Conference,* pp. 20.1-20.13, Las Vegas, NV, USA, June 2008.

[4] M. Huber, “Automated Social Engineering Proof Of Concept,” *Technical Report, SecLab, KTH,* Stockholm, Sweden, March 2009.

[5] N. Ghazisaidi, M. Maier, and C. M. Assi, “Fiber-Wireless (FiWi) Access Networks: A Survey,” *IEEE Communications Magazine*, vol. 47, no. 2, pp. 160-167, Feb. 2009.

[6] E. Dahlman, S. Parkvall, J. Skold, and P. Beming, “3G Evolution: HSPA and LTE for Mobile Broadband,” *Second Edition, Academic Press*, Oct. 2008.

[7] P. D. Townsend, G. Talli, E. K. MacHale, and C. Antony, “Long-reach PONs,” *in Proc., 7th International Conference on Optical Internet,* pp. 1-2, Tokyo, Japan, Oct. 2008.

[8] S. K. Miller, “Facing the Challenge of Wireless Security ,” *IEEE Computer*, vol. 34, no. 7, pp. 16-18, July 2001.

[9] B. Potter, “Wireless Security's Future,” *IEEE Security and Privacy Magazine,* vol. 1, no. 4 , pp. 68-72, July/Aug. 2003.

[10] M. M´edard, D. Marquis, R. A. Barry, and S. G. Finn, “Security Issues in All-Optical Networks,” *IEEE Network,* vol. 11, no. 3, pp. 42-48, May/June 1997.

[11] M. Hajduczenia, P. R. M. Inacio, H. J. A. Da Silva, M. M. Freire, and P. P. Monteiro, “On EPON Security Issues,” *IEEE Communications Surveys and Tutorials,* vol. 9, no. 1, pp. 68-83, 1st Quarter 2007.

[12] E. Athanasopoulos, A. Makridakis, S. Antonatos, D. Antoniades, S. Ioannidis, K. G. Anagnostakis, and E. P. Markatos, “Antisocial Networks: Turning a Social Network into a Botnet,” *in Proc., 11th International Conference on Information Security,* pp. 146-160, Taipei, Taiwan, Sept. 2008.

[13] S. Gangxiang, R. S. Tucker, and C. Chang-Joon, “Fixed Mo bile Convergence Architectures for Broadband Access: Integration of EPON and WiMAX,” *IEEE Communications Magazine,* vol. 45, no. 8, pp. 44-50, Aug. 2007.

[14] S. M. Devine, “Anti-social networking: exploiting the trusting environment of Web 2.0,” *Network Security,* vol. 2008, no. 11, pp. 4-7, Nov. 2008.