Security Issues of WiMAX Networks with High Altitude Platforms

Ilija Basicevic, Miroslav Popovic
Faculty of Technical Sciences
University of Novi Sad
Novi Sad, Serbia
ilibas@uns.ac.rs, miroslav.popovic@rt-rk.com

***Abstract*—In this paper, we discuss the possibility of securing High Altitude Platform Networks (HAP) networks with intrusion detection systems (IDS). We assume that it is a 802.16 network, in point-to-multi point mode. An analysis of possible threats and attack sources is given. Based on that analysis and specific properties of HAP networks an IDS concept is proposed. The main idea of the concept is that a network-based IDS system is collocated with the base station (BS) software. The BS is on board the HAP. The extensions to the concept, in order to provide for prevention feature, are outlined. In that case, the correlation module is a publish/subscribe server for dissemination of events that are the results of alert correlation. Its subscribers are policy enforcement points in the HAP network.**

Keywords-high altitude platforms; IEEE 802.16; intrusion detection system; network security

I. INTRODUCTION

In the recent years, there has been a strong incentive in research of High Altitude Platform (HAP) networks. While in the first place they were envisioned as a means for rapid provisioning of connectivity in the case of disasters (because of the short time needed to launch a HAP vehicle and establish connectivity), soon other scenarios have been proposed as well. For example, in rural areas, with scarce or not existing ground infrastructure, HAPs can be used to provide broadband connectivity, see Fig 1. Another possible application is in mobile sites (e.g., trains). Applications in military communications are also considered. Researchers envisioned high-rate communications (up to 120 Mb/s) delivered directly to a user in line of site of a HAP within a coverage area up to 60 km wide [6]. There are three expected scenarios regarding the position of HAP in the end-to-end path [6]:

- Isolated from any core networks, providing connectivity for private networks
- Between core networks as point-to-point trunk connections
- In the access network, providing users with access to core networks

The significance of first-responder communications (e.g., Enhanced 911 service in US) during catastrophic events is utmost. Such services can be provided by dispatching HAP vehicle with telecommunications equipment in the affected area.

HAP is defined as a solar-powered unmanned airship or airplane, capable of long endurance on-station (several months or more) [7]. The HAP payload can be a complete base station. Besides up- and down-links to the user terminals, and backhaul links, links to satellites can be established as well. In some scenarios, where networks of HAPs are applied, there are also inter-HAP links.

The coverage region is determined by line-of-sight propagation and the minimum elevation angle at the ground terminal. The advantages of HAP communications are [7]:

1. Large area coverage (compared with terrestrial systems)
2. Flexibility to respond to traffic demands - flexible and responsive frequency reuse patterns and cell sizes, unconstrained by the physical location of base-stations.
3. Low cost - cheaper to launch than a geostationary satellite or a constellation of Low Earth Orbit (LEO) satellites, cheaper to deploy than a terrestrial network.
4. Incremental deployment - service may be provided initially with a single HAP and expanded gradually - in contrast to LEO satellites.
5. Rapid deployment - it is possible to design, implement and a deploy HAP service relatively quickly, especially when compared to satellites.
6. Platform and payload upgrading - can be relatively easily and safely brought down for payload upgrading.
7. Environmentally friendly

The backhaul link is realized using cellular scheme too, because a single link can not provide full backhaul capacity. Thus there are going to be a number of distributed backhaul ground stations, though this number can be fewer than the number of user cells served because of the higher order modulation schemes that would be used in backhaul links, which would provide greater capacity [7].

HAP-based services have been allocated frequencies by the ITU at 47/48 GHZ, also at 28 GHz in ITU Region 3 - Asia.

Most of the scenarios predict use of HAPs for 802.16 networks, although Universal Mobile Telecommunications System (UMTS) is present in application scenarios as well, albeit in much smaller extent. We assume that 802.16 network is in point-to-multi point (PMP) mode. With regard to physical characteristics of the network, HAP is usually positioned at an altitude of approximately 17-22 kilometers. It covers up to 256 cells.

 ISBN: 978-1-61208-176-2

Use of HAP platforms for different applications has been studied in the scope of several projects (HAPCOS – EU COST action 297, HELINET and CAPANINA EU Framework Programme projects), but to the best of our knowledge this is the first analysis of the possibilities for protection of HAP WiMAX networks with IDS systems.

Section 2 briefly presents security mechanisms that are used in 802.16 networks. Section 3 describes architecture of a network based intrusion detection system for 802.16 networks. It includes analysis of possible threats and possible improvements in order to realize prevention feature (besides detection). Section 4 contains concluding remarks.

II. SECURITY MECHANISMS IN 802.16 NETWORK TECHNOLOGY

Compared to IEEE 802.11, a serious effort has been undertaken in designing the security mechanisms in IEEE 802.16. The following description is based on [1].

IEEE 802.16 protocol stack contains Media Access Control (MAC) layer, which is divided into three sublayers (convergence sublayer, common part sublayer and privacy sublayer). Service specific convergence sublayer has two types, one that interfaces ATM as upper layer, and the other for TCP/IP. Common part sublayer is the core part of IEEE 802.16 MAC. It manages connections and bandwidth, among other functions. There are three types of connections: Primary, Basic and Secondary. Primary are used for authentication. Basic are used for time critical MAC control messages. Secondary are used for standards based management messages (e.g., SNMP [5]). MAC is connection oriented, and all data communications are in the context of connection. Connections are added, modified and deleted dynamically. Privacy sublayer is responsible for security functions:

- Encryption,
- Decryption,
- Authentication,
- Secure key exchange.

This sublayer contains two protocols: Encapsulation and the Privacy and Key Management Protocol (PKM).

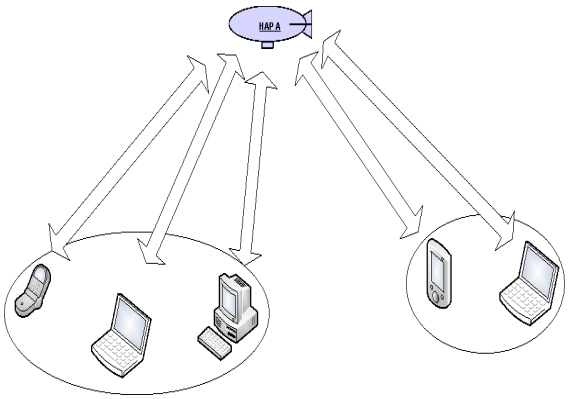

Figure 1. HAP network

Security protocols use Security Associations (SA). There are three types of SAs: primary, static and dynamic. Primary are established during initialization process. Static and dynamic can be shared between different subscriber stations (SS). Shared information may include traffic encryption key (TEK) and initialization vector (IV).

BS is responsible for maintaining keying information for all SAs. SA keying material has limited lifetime. When BS provides SS with a keying material, it includes information on remaining lifetime. Keying system is a two-tier one. The first tier is: using public keys, BS sends authorization key (AK) to SS. The second tier is that by using AK, the TEK exchange is protected.

PKM protocol is used for synchronization of keying information between BS and SS. PKM has two finite state machines: Authorization and TEK exchange. PKM authorization is realized as an exchange of three messages. In this exchange, SS provides BS with its certificates (certificate of the manufacturer and of the station itself) - BS authenticates SS, and BS provides SS with AK and with identification of SAs it is authorized to access. Key encryption key (KEK) and message authentication keys are derived from AK. Security components use X.509 Version 3 certificates. PKM TEK exchange is an exchange of two or three messages, in which BS sends TEK parameters for each requested SA. Three messages are exchanged. PKM is a client/server protocol where SS is a client. PKM uses RSA with SHA-1. IEEE 802.16 encryption uses DES CBC over payload. Generic MAC Header (GMH) and CRC fields are not encrypted.

New subscriber station enters the network in five steps:

1. SS scans for a BS downlink signal and uses it to establish channel parameters
2. Primary management connection established
3. SS authorized using PKM
4. SS sends a register request and BS responds with second management connection Id
5. Transport connections are created

The first phase is security capabilities negotiation during which SS informs BS which cryptographic suites it supports and BS tells SS which of those to use in the subsequent communication (this information is contained in the descriptor of the primary SA).

BS generates AKs and TEKs using random or pseudo-random generators. IVs are generated in such a manner as to be unpredictable.

III. NIDS FOR IEEE 802.16 - HAP CASE

Network-based IDS are an important class of contemporary IDS systems. In this class of systems, IDS processes the stream of packets that are transmitted over the network. In the typical wired environment IDS is usually placed in the network perimeter. In the HAP network, which is a 802.16 network in the point-to-multi point (PMP) mode, a logical place for NIDS is the base station. We propose architecture with a NIDS sensor in each cell, a NIDS sensor that monitors link to the gateway and a coordination and correlation module which has the following functions:

 ISBN: 978-1-61208-176-2

- It correlates alerts from NIDS sensors in 802.16 cells
- It sends the results of the correlation phase to the network operations center
- It downloads signature updates from public repository or vendor web site
- It uploads signature updates to NIDS sensors

Snort is a popular IDS system, significantly present both in everyday use, and in research. It is an IDS system for wired networks, but there are important common concepts that IDS systems for wired and wireless networks share. The Snort 3.0 architecture [8] promotes separation of the Snort Security Platform (SnortSP) from the Engines module which contains analytics modules. We propose that Snort 3.0 architecture can be used as IDS architecture for HAP systems. In the HAP case, the Dispatcher module connects not only to the local Data Source, but also receives alerts from the coordination module.

SNMP [5] is a de-facto standard for network management in Internet environment, thus we propose that in HAP IDS system the same protocol would be used. In case of HAP networks, it is usually assumed that the network operations center is placed on the ground, and that a wireless link is used for network management of the HAP network, for software updates and maintenance and also in some cases for the maneuvering of the HAP vehicle. The network operations center contains the Security Officer console, which allows for visual inspection of the state of HAP IDS, the list of most recent alerts and similar features.

A. Threats to the HAP network

As a primary attack venue, we see subscriber stations. We divide the attacks into three classes:

- Attacks at the physical layer,
- Attacks at the MAC layer,
- Attacks at higher layers.

Subscriber stations in the HAP cell can mount physical layer attacks. In the literature are often mentioned jamming and packet scrambling, belonging to this class. The jamming attack is mounted using information from UL-MAP message received from BS, and if it is a targeted attack, attacker has to map the CID from UL-MAP message to the station address. This attack can be realized with short transmissions and low radiated power, which protects the attacker [11].

At MAC layer, subscriber stations are capable of mounting Denial of Service (DOS) attacks. DOS attacks at MAC layer are realized as flooding of signalization requests (authentication, capabilities negotiation, key management frames, etc.). The primary means of those attacks are resource intensive cryptographic operations.

Some of messages in IEEE 802.16 are not authenticated (Traffic Indication Message, Neighbor Advertisement Message, Fast Power Control, Multicast Assignment Request, Downlink Burst Profile Change Request, Power Control Mode Change Request) [12] which leaves space for attacks.

At higher layers, a distributed variant of DOS (DDOS) attacks is possible. DOS attacks at application layer that disturb the normal application operation instead of depleting network resources as in classical DOS, are becoming more and more serious threat recently. At application layer, also are possible targeted attacks at users. Typical examples are different types of malware hidden in email attachments. Protective measures include application level filters at network servers. Those are outside the scope of this paper.

One often cited type of attack, which is possible in 802.16, although it is more difficult to realize than in 802.11 is the rogue base station attack. This type of attack belongs to the class of man-in-the middle attacks. In the attack, the rogue base station impersonates a legitimate one. A short description of the attack is given in [4]. Other attacks in this class are more probable in a mesh network, rather than in a network in PMP mode. The proposed IDS system at this moment does not include the detection feature for this type of attacks.

Besides subscriber stations, the source of attacks in higher layers of protocol stack can be in external networks - mounted over the link to the gateway. Those attacks are targeted at stations in the HAP network. As this is the last hop in the communication path between attacker and its target, DOS attacks are already amplified and easily detectable, but the possibility for reaction is limited.

The last is that although SNMPv3 includes authentication, it has to be noted that the link to operations center presents another attack venue. The privileges that are given to management personnel are wide: software updates, installation of software modules, restart, power on/off, maneuvering in case of HAP airplanes, etc. Since the operations that are realized over the management interface are of great security impact, the damage that an attacker who successfully impersonates the network operations center could make is critical.

B. Remarks on the construction of HAP IDS

The first phase of detection in a NIDS is the packet "sniffing". While relatively simple for realization in a wired network, in wireless networks the NIDS system has to scan traffic at a set of frequencies. Each of the frequencies is scanned in specific intervals of time. Typically not the same time interval is devoted to scanning of all frequencies in the set, and there is usually a heuristic algorithm (sometimes based on fuzzy logic) applied to determine how long to scan each of the frequencies. The integration of IDS sensor software with the BS protocol stack software would provide for the simple method of monitoring of the communication between subscriber stations and the base station. The concept of integration can be similar to the use of filter hooks [9] and filtering platform callout drivers [10] in Microsoft Windows OS in packet filtering applications for wired networks. Fig 2 presents the structure of HAP IDS/IPS at one BS, including the information flows.

Average traffic load on HAP BS can be estimated in the following way. A traffic stream from one mobile user to the HAP BS can be modeled as 4IPP [13] (traffic model for IEEE 802.16.3) . Number of terrestrial users is 240-256 per cell in published simulations [14]. Thus, the total traffic on

 ISBN: 978-1-61208-176-2

HAP BS coming from terrestrial users in one cell in average case can be modeled as 256 4IPP streams. The HAP IDS should be able to inspect such a stream, without losing packets. The 4IPP average rate is 3 pkts/unit-of-time. The bandwidth of SS-HAP link is 1 Mbps in simulations [15]. The packet size is 1500 Bytes. The packet rate is 1000000/(1500*8), which is 83 packets per sec. The parameters of the basic 4IPP model (see Table 1, the 4IPP Average Rate is calculated as a sum of IPP stream rates and equals to 3 pkts/unit-of-time) should be scaled by 83/3=27.8 unit-of-time per sec. The resulting parameters of IPP streams for model of communication in HAP network are given in Table 2.

TABLE 1. PARAMETERS OF IPP STREAMS IN BASIC 4IPP TRAFFIC MODEL

Source #i	λi IPP in ON state (pkts/unit-of-time)	Averaged over both ON and OFF states (pkts/unit-of-time)
IPP#1	2.679	1.1480
IPP#2	1.698	.7278
IPP#3	1.388	.5949
IPP#4	1.234	.5289

TABLE 2. PARAMETERS OF IPP STREAMS IN HAP WIMAX TRAFFIC MODEL

Source #	Averaged over both ON and OFF states (pkts/sec) – for 1 SS	Averaged over both ON and OFF states (pkts/sec) – for 256 SS
IPP#1	31.91	8168.96
IPP#2	20.23	5178.88
IPP#3	16.54	4234.24
IPP#4	14.7	3763.2

Since it aggregates events from several cells, in some cases, the correlation module can detect low volume DDOS attacks (at higher layers of protocol stack), that would otherwise (without the aggregation and correlation of alerts coming from different cells) pass unnoticed.

In case of multi-HAP network, operation of HAP IDS systems belonging to specific HAP networks can be coordinated in centralized manner (from the network operations center on the ground), or those can cooperate in a distributed manner. The realization of such a cooperative system is outside the scope of this paper.

Attacker location is an important feature in wireless security. Application of techniques such as triangulation for that purpose is outside the scope of this paper.

C. *Possible improvements*

Besides the aforementioned cooperation in case of multi-HAP networks, there are two directions in which the proposed concept can be improved and/or extended.

The first one is that the 802.16 network can be used in mesh mode. There are already some proposals for IDS systems for wireless mesh networks: OpenLIDS [2], WATCHERS, TIARA, CONFIDANT, MobIDS, RESANE, SCAN [3]. The change from PMP to mesh mode would require a substantial rework of the concept.

The other direction is that having provided the detection functionality, the next step is the reaction feature (intrusion prevention). Such architecture is based on the use of Policy Enforcement Point engine (PEP) at the base station. It is often implemented as a firewall. In that case the functionality of the correlation module would be extended with the following function: dispatching of new alerts that are the results of correlation phase back to NIDS sensors. In order to achieve efficient use of communication and processing resources, the correlation module should be able to filter the alerts that it sends to sensors. There are strict limitations with respect to the weight of the load that can be placed in the HAP that imply the efficient use of processing resources. For that reason we propose that the coordination and correlation module is a lightweight topic-based publish/subscribe system. There is a publish/subscribe association between this module and PEP engines. In this association, the correlation module is the publisher and PEP engines are subscribers. We remark that in this design the PEP engines are collocated with sensors.

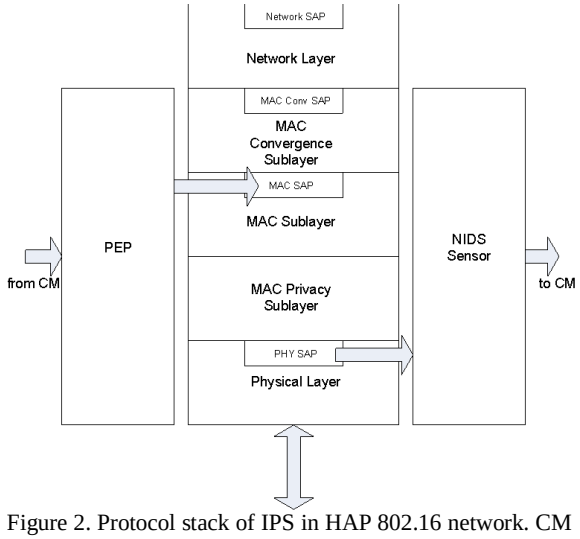

Figure 2. Protocol stack of IPS in HAP 802.16 network. CM is correlation module.

The proposed system is a good platform for realization of the reaction feature, because the communication stream from the correlation module to the PEP engines, which carries

results of correlation phase, in the average case contains enough information for decisions on reaction.

By implementing IDS/IPS as described, we allow for swift reaction in case of handovers of malicious subscriber stations. Once recognized as malicious, such a station can be disconnected and prevented from moving to the neighboring cell. This is especially of interest in overlapping areas, where mobile station can choose one of up to three cells (in average case) that it will use for communication.

IV. CONCLUSION AND FUTURE WORKS

This paper presents an approach to securing of HAP networks by using intrusion detection systems. The protected network is a 802.16 network in point-to-multi point mode. The proposed system is a distributed network-based IDS system with a NIDS sensor in each cell. IDS system is collocated with the base station software. The BS is on board the HAP. IDS sensors monitor communications links between base station and subscriber stations. The backhaul link to ground station is monitored as well. The IDS is collocated with the base station device, on board the HAP vehicle.

The system allows for detection of distributed DOS attacks in the HAP network. The paper describes the required modifications to the system in order to include reaction feature (intrusion prevention) in a straightforward manner. The correlation module in the extended system is the publish/subscribe server that publishes results of the correlation phase to the policy enforcement point engines in HAP cells.

The system could be further developed to include support for cooperation of IDS/IPS systems in multi-HAP networks.

ACKNOWLEDGMENT

This paper is a continuation of the research conducted in the scope of HAPCOS project (COST action 297). This work was partially supported by the Ministry of Education and Science of the Republic of Serbia under the project No. 32031 and 44009, year 2011.

REFERENCES

[1] IEEE Std 802.16™-2009, IEEE Standard for Local and metropolitan area networks, Part 16: Air Interface for Broadband Wireless Access Systems, IEEE-SA Standards Board, The Institute of Electrical and Electronics Engineers, Inc.

[2] F. Hugelshofer, P. Smith, D. Hutchison, and N.J.P. Race, OpenLIDS: A Lightweight Intrusion Detection System for Wireless Mesh Networks, Mobicom 09, Beijing, China, 2009, pp. 309-320

[3] T.M. Chen, G.S. Kuo, Z.P. Li, and G.M. Zhu, Intrusion Detection in Wireless Mesh Networks, chapter in Security in Wireless Mesh Networks, Auerbach Publications, 2008

[4] M. Barbeau, J. Hall, and E. Kranakis, Detecting Impersonation Attacks in Future Wireless and Mobile Networks, Workshop on Secure Mobile Ad-hoc Networks and Sensors, MADNES 2005

[5] U. Blumenthal and B. Wijnen, User-based Security Model (USM) for version 3 of the Simple Network Management Protocol (SNMPv3), RFC 3414, 2002, The Internet Society

[6] D. Grace, M. Mohorcic, M.H.Capstick, M. Bobbio Pallavicini, and M. Fitch, "Integrating Users into the Wider Broadband Network via High Altitude Platforms", IEEE Wireless Communications, Vol. 12, No. 5, pp. 98-105, October 2005

[7] T.C. Tozer and D. Grace, "High Altitude Platforms for Wireless Communications", IEE Electronics and Communications Engineering Jnl, Vol. 13, No. 3, June 2001, pp. 127-137

[8] Snort 3.0 Architecture Series Part 1: Overview, http://securitysauce.blogspot.com/2007/11/snort-30-architecture-series-part-1.html, retrieved: November, 2011.

[9] Filter-Hook Drivers, http://msdn.microsoft.com/en-us/library/windows/hardware/ff546489%28v=vs.85%29.aspx, retrieved: November, 2011.

[10] Introduction to Windows Filtering Platform Callout Drivers, http://msdn.microsoft.com/en-us/library/ff556954%28VS.85%29.aspx, retrieved: November, 2011.

[11] Security of IEEE 802.16, Arkoudi-Vafea Aikaterini, Master Thesis, Department of computer and Systems Science, Royal Institute of Technology, Stockholm, Sweden, 2006

[12] A. Deininger, S. Kiyomoto, J. Kurihara, and T. Tanaka, “Security Vulnerabilities and Solutions in Mobile WiMAX”, IJCSNS International Journal of Computer Science and Network Security, VOL.7 No.11, November 2007.

[13] C. R. Baugh, 4IPP Traffic Model for IEEE 802.16.3, IEEE 802.16.3c-00/51,

[14] Floriano De Rango, Mauro Tropea, and Salvatore Marano, Integrated Services on High Altitude Platform: Receiver Driven Smart Selection of HAP-Geo Satellite Wireless Access Segment and Performance Evaluation, International Journal of Wireless Information Networks, Vol. 13, No. 1, January 2006, pp. 77-94, DOI: 10.1007/s10776-005-0020-z

[15] C. E. Palazzi, C. Roseti, M. Luglio, M. Gerla, M. Y. Sanadidi, and J. Stepanek, Enhancing Transport Layer Capability in HAPS-Satellite Integrated Architecture, Wireless Personal Communications, Vol 32 Issue 3-4, February 2005

 ISBN: 978-1-61208-176-2