Int. J. Communications, Network and System Sciences, 2017, 10, 43-53
http://www.scirp.org/journal/ijcns
ISSN Online: 1913-3723
ISSN Print: 1913-3715

MAC Frame Resolution and PHY Protocol Type Detection of IEEE 802.11

Ling Li[1], Shi Peng[1], June Li[2,3*], Kai Yuan[3], Zhihao Wang[3], Yinbin Liu[3], Ping Chen[3], Xianbing Wang[3]

[1]China Electric Power Research Institute, Beijing, China
[2]Key Laboratory of Aerospace Information Security and Trusted Computing of Ministry of Education, Wuhan, China
[3]Wuhan University, Wuhan, China
Email: *jeli@whu.edu.cn

How to cite this paper: Li, L., Peng, S., Li, J., Yuan, K., Wang, Z.H., Liu, Y.B., Chen, P. and Wang, X.B. (2017) MAC Frame Resolution and PHY Protocol Type Detection of IEEE 802.11. *Int. J. Communications, Network and System Sciences*, **10**, 43-53.
https://doi.org/10.4236/ijcns.2017.105B005

Received: March 6, 2017
Accepted: May 23, 2017
Published: May 26, 2017

Abstract

Frame resolution and physical layer (PHY) protocol type detection are the basis of research and development of intrusion prevention systems for IEEE 802.11 wireless network. Aiming at the problems which cannot be solved by the specifications export, this paper proposed a MAC frame analytical method and a PHY protocol type detection algorithm based on parsing the IEEE 802.11packets captured by the library Libpcap. The packet structure and the length of the frame preamble (18 or 26 bytes) are presented. Then the methods of transforming byte-order and resolving sub-fields are given. A detection algorithm of PHY protocol type is proposed based on the experiments and examples are given to verify these methods. This work can be a reference for the R & D related to link layer frame analysis.

Keywords

IEEE 802.11, MAC Frame, Resolution, PHY Protocols, Detection

1. Introduction

IEEE 802.11 Wireless LAN (WLAN) plays an important role in personal Internet access as well as industrial applications [1] [2] [3] [4], because of its convenient deployment, lower cost and mobility. Compared to the wired network, WLAN is more vulnerable [5] [6] [7]. It is very easy to capture and analyze the transmitting message, because the medium of WLAN is shared. Therefore, it is particularly important to research the security technologies for WLAN.

The research on the technology for WLAN security mostly focused on intrusion detection systems [6] [7] [8] [9] [10] in the past, but is still at an initial stage. Mature commercial products are also inadequate.

Real-time monitoring and analysis of the WLAN environment is an effective

way to find potential risks, such as vulnerabilities, suspicious devices or behavior. At a WLAN-forbidden location, unauthorized APs and STAs can be detected by the real-time monitoring system to avoid an exposure of the private network.

Capturing and resolving the MAC frames are the technical basis of a real-time monitoring and analysis system, vulnerability scanning system and intrusion detection system for WLAN [6] [7] [8] [9] [10]. IEEE 802.11 MAC frames are categorized into three types: control frames, management frames, and data frames. Control frames and management frames contain a lot of useful information and are transmitted in plain text. Although the body of data frame is encrypted when a security measure is enabled, the frame header is still in plaintext. Therefore, we can parse the captured MAC frames to get the information and use the appropriate detection algorithm to identify the potential risks in a WLAN.

However, there are some practical problems, for which no literature presents solutions about frame capture and analysis. For example, the length of frame preamble is not the same when different STAs capture MAC frames from a same AP or STA. There are bytes and bits order converting problems when analyzing the captured data. The research of packet capture and analysis focused on the PDU (protocol data unit) encapsulated in TCP or UDP rather than that in link layer frame in the past.

Detection of PHY protocol types is basic content of the WLAN environment analysis and further development. Network managers can analyze the behaviors of APs or STAs on the basis of their real-time PHY protocol type and other information to identify suspicious devices in a WLAN.

However, the specification of some information elements in the standard is not detailed enough, so the detection algorithm of PHY protocol types cannot be designed based on the standard. And, no literature proposes the detection algorithm.

Aiming at the problems above, this paper proposes a MAC frame resolution method and a PHY protocol type detection algorithm of IEEE 802.11, on the basis of a large number of experiments for frame capturing and analyzing. The packet capturing is based on the library of Linux Libpcap.

2. Method of MAC Frame Resolution

2.1. Structure of Captured Data and Length of Frame Preamble

The length of frame preamble is not the same when different STAs capture MAC frames from a same AP or STA. The captured data are represented by the structure shown in **Figure 1**. The MAC frame consists of a header, a body and the FCS. The frame preamble is related to network interface card.

There are two kinds of length of the frame preamble. One is 26 bytes and the other is 18 bytes. The length can be calculated from the value of third byte of the captured data. An example of the captured binary data of a beacon frame is shown in **Figure 2**. The third byte of the example shown in **Figure 2** is 0x1A,

which indicates that the frame preamble is 26 bytes. If the third byte of the captured data is 0 × 12, it represents that the frame preamble is 18 bytes (shown in **Figures 9-13**).

2.2. Method of Frame Resolution

To analyze the information contained in the frame, we need to identify the value

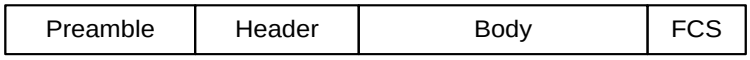

Figure 1. Structure of the captured data.

00	00	1A	00	2F	48	00	00	C0	DA	2E	00	00	00	00	00	10	02	6C	09
A0	00	D8	01	00	00	80	00	00	00	FF	FF	FF	FF	FF	FF	6C	E8	73	9E
E5	36	6C	E8	73	9E	E5	36	40	62	63	C9	EA	C0	A2	00	00	00	64	00
31	04	00	07	49	4D	49	54	31	31	34	01	08	82	84	8B	96	0C	12	18
24	03	01	01	05	04	00	01	00	04	2A	01	00	30	18	01	00	00	0F	AC
02	02	00	00	0F	AC	04	00	0F	AC	02	01	00	00	0F	AC	02	00	00	32
04	30	48	60	2D	2D	1A	6E	10	03	FF	00	00	00	00	00	00	00	00	00
00	00	00	00	00	00	00	00	00	00	00	00	00	3D	16	01	05	11	00	00
00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	DD	1A	00
50	F2	01	01	00	00	50	F2	02	02	00	00	50	F2	04	00	50	F2	02	01
00	00	50	F2	02	DD	18	00	50	F2	02	01	01	03	00	03	A4	00	00	27
A4	00	00	42	43	5E	00	62	32	2F	00	DD	09	00	03	7F	01	01	00	00
FF	7F	DD	DE	00	50	F2	04	10	4A	00	01	10	10	44	00	01	02	EE	EC
39	B6																		

Figure 2. A captured beacon frame data.

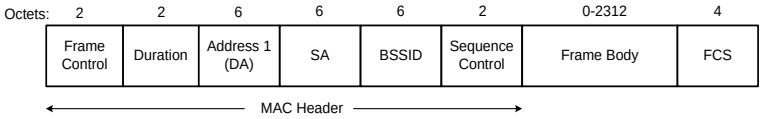

Figure 3. Management frame format.

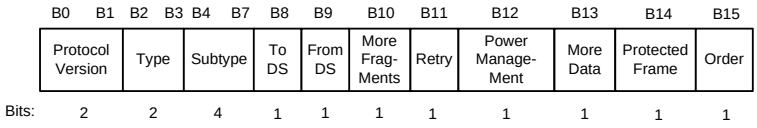

Figure 4. Frame Control field.

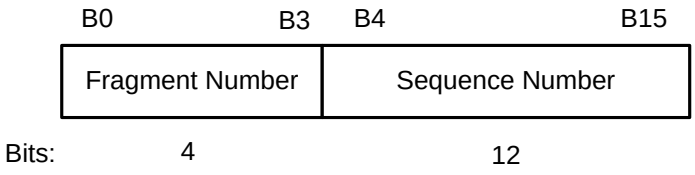

Figure 5. Sequence Control field.

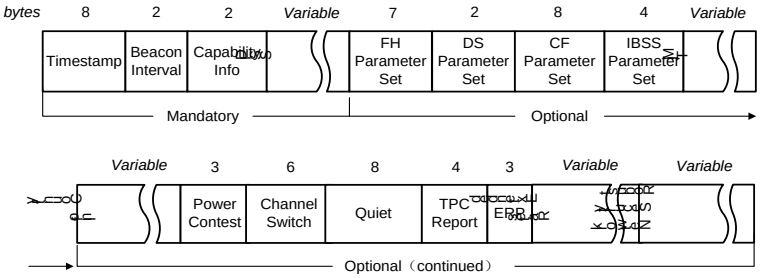

Figure 6. Beacon frame body.

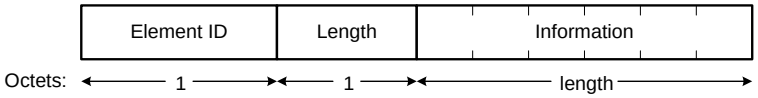

Figure 7. Common general format of information element.

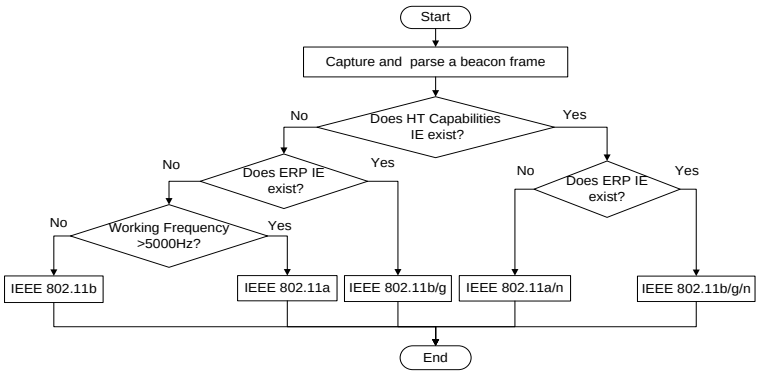

Figure 8. Algorithm flowchart of PHY protocol type's detection.

00	00	12	00	2E	48	00	00	00	02	6C	09	A0	00	DE	03	00	00	80	00
00	00	FF	FF	FF	FF	FF	FF	00	07	26	19	94	08	00	07	26	19	94	08
B0	39	73	F1	EC	04	00	00	00	00	64	00	11	00	00	0E	44	2D	4C	69
6E	6B	5F	44	49	52	2D	38	30	35	01	04	82	84	8B	96	03	01	01	05
04	00	03	00	00	30	14	01	00	00	0F	AC	04	01	00	00	0F	AC	04	01
00	00	0F	AC	02	00	00	DD	18	00	50	F2	02	01	01	00	00	03	A4	00
00	27	A4	00	00	42	43	BC	00	62	32	66	00	DD	06	00	E0	4C	02	01
60																			

Figure 9. The captured data of a beacon frame from an AP set into IEEE 802.11b.

in each field. The frame resolution must be corresponding to the frame format. The information for security detection comes mainly from management frames. This section will illustrate an analytical method of IEEE 802.11 MAC Frame in three examples, which are adopting this method in analyzing1) a management frame's header, 2) Control Frame field of the management frame and 3) Control Sequence field of the management frame. Their structures are shown in **Figures 3**-**5** respectively [11]. The information contained in these fields is the most basic information for analyzing 802.11 wireless network environment. This informa-

00	00	12	00	2E	48	00	00	00	0C	71	16	40	01	C5	03	00	00	80	00
00	00	FF	FF	FF	FF	FF	FF	00	07	26	19	94	04	00	07	26	19	94	04
E0	DD	1B	00	B4	14	00	00	00	00	64	00	11	00	00	11	44	2D	4C	69
6E	6B	5F	44	49	52	2D	38	30	35	2D	35	47	01	08	8C	12	98	24	B0
48	60	6C	05	04	00	01	00	00	30	14	01	00	00	0F	AC	04	01	00	00
0F	AC	04	01	00	00	0F	AC	02	00	00	DD	18	00	50	F2	02	01	01	00
00	03	A4	00	00	27	A4	00	00	42	43	5E	00	62	32	2F	00	DD	06	00
E0	4C	02	01	60															

Figure 10. The captured data of a beacon frame from an AP set into IEEE 802.11a.

00	00	12	00	2E	48	00	00	00	02	6C	09	A0	00	A7	03	00	00	80	00
00	00	FF	FF	FF	FF	FF	FF	00	07	26	19	94	08	00	07	26	19	94	08
F0	16	73	41	32	01	00	00	00	00	64	00	11	04	00	0E	44	2D	4C	69
6E	6B	5F	44	49	52	2D	38	30	35	01	08	82	84	8B	96	0C	12	18	24
03	01	01	05	04	00	03	01	00	2A	01	04	32	04	30	48	60	6c	30	14
01	00	00	0F	AC	04	01	00	00	0F	AC	04	01	00	00	0F	AC	02	00	00
DD	18	00	50	F2	02	01	01	00	00	03	A4	00	00	27	A4	00	00	42	43
5E	00	62	32	2F	00	DD	06	00	E0	4C	02	01	60						

Figure 11. The captured data of a beacon frame from an AP set into IEEE 802.11b/g.

00	00	12	00	2E	48	00	00	00	0C	71	16	40	01	C9	03	00	00	80	00
00	00	FF	FF	FF	FF	FF	FF	00	07	26	19	94	04	00	07	26	19	94	04
50	A5	1B	60	C4	B1	9A	02	00	00	64	00	11	00	00	11	44	2D	4C	69
6E	6B	5F	44	49	52	2D	38	30	35	2D	35	47	01	08	8C	12	98	24	B0
48	60	6C	05	04	00	01	00	00	2D	1A	6E	18	1E	FF	00	00	00	00	00
00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	3D	16	95
05	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
00	30	14	01	00	00	0F	AC	04	01	00	00	0F	AC	04	01	00	00	0F	AC
02	00	00	DD	18	00	50	F2	02	01	01	00	00	03	A4	00	00	27	A4	00
00	42	43	5E	00	62	32	2F	00	DD	1E	00	90	4C	33	6E	18	1E	FF	00
00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
00	DD	1A	00	90	4C	34	95	05	00	00	00	00	00	00	00	00	00	00	00
00	00	00	00	00	00	00	00	00	DD	06	00	E0	4C	02	01	60			

Figure 12. The captured data of a beacon frame from an AP set into IEEE802.11a/n.

tion is also essential for following frame body analyzing. Notice that the management frame header of IEEE Std 802.11-2012 [12] has an extra HT Control field compared to IEEE Std 802.11-2007 [11]. However, the existing data captured from experiment all conform to IEEE Std 802.11-2007. So only the frame format of IEEE Std 802.11-2007 will be examined in this paper.

00	00	12	00	2E	48	00	00	00	02	94	09	A0	00	DE	03	00	00	80	00
00	00	FF	FF	FF	FF	FF	FF	00	07	26	19	94	08	00	07	26	19	94	08
30	95	AD	41	86	0C	00	00	00	00	64	00	11	04	00	0E	44	2D	4C	69
6E	6B	5F	44	49	52	2D	38	30	35	01	08	82	84	8B	96	0C	12	18	24
03	01	09	05	04	02	03	00	00	2A	01	04	32	04	30	48	60	6C	2D	1A
2C	18	1E	FF	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
00	00	00	00	00	00	3D	16	09	00	00	00	00	00	00	00	00	00	00	00
00	00	00	00	00	00	00	00	00	00	30	14	01	00	00	0F	AC	04	01	00
00	0F	AC	04	01	00	00	0F	AC	02	00	00	DD	18	00	50	F2	02	01	01
00	00	03	A4	00	00	27	A4	00	00	42	43	5E	00	62	32	2F	00	DD	1E
00	90	4C	33	2C	18	1E	FF	00	00	00	00	00	00	00	00	00	00	00	00
00	00	00	00	00	00	00	00	00	00	DD	1A	00	90	4C	34	09	00	00	00
00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	DD	06
00	E0	4C	02	01	60														

Figure 13. The captured data of a beacon frame from an AP set into IEEE 802.11b/g/n.

A multi byte numeric field needs to be converted from the network order to host order when parsing a captured packet. The sub-fields of a numeric field need to be reversely picked up from the binary value after the order converting, i.e. the last sub-field is picked up at first from the highest bit of the binary value. A non-numeric field, such as address, and its sub-fields, if existing, can be sequentially obtained from the captured data. This solution is illustrated with the data shown in **Figure 2**.

The 24-byte data, which starts from 27th byte of the data shown in **Figure 2**, is the header of the beacon frame. Value of the fields in the beacon frame header after parsing the captured data is shown in **Table 1**. The host byte order of a multi byte numeric field is different from its network byte order in Linux, so that the byte order of Frame Control, Duration and Sequence Control is reversed if compared to that of captured data.

The value of Frame Control filed in above example is 0x0080, which is 0000000010000000 in binary. According to resolving method for sub-field in the Frame Control shown in **Figure 4**, the results are drawn in **Table 2**.

According to the standard [11], this is a management frame (Type = 00), of which the body is a beacon frame body (Subtype = 1000).

Applying the same method, we can get two subfields' value for Sequence Control shown in **Table 3**.

3. Detection Method of PHY Protocol Type

3.1. The Information Elements and Detection Algorithm for PHY Protocols

The commonly used WLAN PHY protocols are IEEE 802.11a, b, g and n. In order to analyze the type of protocol from the captured data, the information ele-

Table 1. Value of each field in beacon frame header.

Field Name	Length (in bytes)	Value (in hexadecimal)	Remarks
Frame Ctrl	2	0080	Bytes in reverse order
Duration	2	0000	Bytes in reverse order
DA	6	FFFFFFFFFFFF	Sequential order
SA	6	6CE8739EE536	Sequential order
BSSID	6	6CE8739EE536	Sequential order
Sequence Ctrl	2	6240	Bytes in reverse order

Table 2. Value of each subfield in Frame Control.

Subfield Name	Length (in bits)	Value (in binary)
Protocol Version	2	00
Type	2	00
Subtype	4	1000
To DS	1	0
From DS	1	0
More Fragments	1	0
Retry	1	0
Power Management	1	0
More Data	1	0
Protected Frame	1	0
Order	1	0

Table 3. Value of each subfield in Sequence Control.

Subfield Name	Length (in bits)	Value (in hexadecimal)
Fragment Number	4	0
Sequence Number	12	624

ments in the frame body need to be analyzed after parsing the content of beacon frame as described in previous sections.

The format of beacon frame body is shown in **Figure 6** [13]. There are two types of components in management frame body: 1) Fixed-length field, such as Timestamp; 2) Variable-length field, called Information Element (IE), such as SSID. The common general format of an information element is shown in **Figure 7** [11]. Each element is assigned to a unique Element ID as defined in IEEE 802.11 standard to indicate its function. The Length field specifies the number of octets in the Information field. The Information field is variable-length and element-specific [11] [12].

The information elements used by the PHY protocol type have not been explicitly defined in the standard. This can lead to confusion when designing a de-

tecting algorithm. So first list several possible information elements, such as ERP element and HT Capability element, based on the standard. Then during the experiments, use the aforementioned analytical method to analyse the captured beacon frame.

The results of information elements contained in the beacon frame body received from different PHY protocol APs are shown in **Table 4**. Notice that the structure of the captured frame header is consistent with the format defined in IEEE Std802.11-2007. Information element of HT Capabilities is fully defined in IEEE Std802.11-2012 while its element ID is reserved in IEEE Std802.11-2007. According to **Table 4**, the detection algorithm of the PHY protocol types is shown in **Figure 8**.

3.2. NIC Working Frequency Acquisition Method

The algorithm shown in **Figure 8** needs to obtain working frequency of NIC (Network Interface Card). During the experiment, we find that if the length of frame preamble in captured data is 26 bytes, the frequency value of NIC is located in 19th and 20th byte of data. If the length of frame preamble in captured data is 18bytes, the frequency value of NIC is located in 11th and 12th byte of data. Using the analytical method in Section 2.2, we can get the working frequency of NIC. The specific examples are shown in Section 4.

4. Case Study

The effectiveness of the proposed methods can be verified through the following examples. Testing environment consists of a dual-band supported AP and a STA which are installed with the frame capturing program. The operating system of STA is Linux. The experiment AP is set to different PHY protocols. Launch the frame capturing program on STA and let it last for 5 minutes to get a certain number of frames. When obtaining a sufficient number of frames, stop the frame capturing program. Analyze the captured beacon frames according to the analysis method in section 2.2 and algorithm shown in **Figure 8**.

4.1. IEEE 802.11b

Set the PHY protocol of AP to IEEE 802.11b. The captured data of a beacon frame are shown in **Figure 9**. We find that HT Capabilities information element and ERP information element do not exist. The octets containing the working frequency are 6C 09. Shaded area in the figure shows the location of the working frequency octets. According to the previous frame resolution method, the frequency value is 0x096C, which is 2412 MHz in decimal, that is, the working frequency of AP is on the 2.4 GHz band. According to the algorithm shown in **Figure 8**, the PHY protocol of the AP is IEEE 802.11b, consistent with the preset.

4.2. IEEE 802.11a

Set the PHY protocol of AP to IEEE 802.11a. The captured data of a beacon

frame are shown in **Figure 10**. We find that HT Capabilities information element and ERP information element do not exist. The octets containing the working frequency are 71 16. Shaded area in the figure shows the location of the working frequency octets. According to the previous frame resolution method, the frequency value is 0x1671, which is 5745 MHz in decimal, that is, the working frequency of AP is on the 5 GHz band. According to the algorithm shown in **Figure 8**, the PHY protocol of AP is IEEE 802.11a, consistent with the preset.

4.3. IEEE 802.11b/g

Set the PHY protocol of AP to IEEE 802.11b/g mixed mode. The captured data of a beacon frame are shown in **Figure 11**. The ERP information element is 2A 01 04 (the second shaded area in the figure). The HT Capabilities information element does not exist. According to the algorithm shown in **Figure 8**, the PHY protocol of AP is IEEE 802.11 g, consistent with the preset. The working frequency octets are 6C 09 (first shaded part in the figure). According to the previous frame resolution method, the frequency is 2412 MHz, proving that the working frequency of AP is on the 2.4 GHz band.

The algorithm under the condition of IEEE 802.11 g single mode is the same as that of IEEE 802.11b/g.

4.4. IEEE 802.11a/n

Set the PHY protocol of AP to IEEE 802.11a/n. The captured data of a beacon frame are shown in **Figure 12**. There is no ERP information element. The HT Capabilities information element exists (the second shaded area in the figure). According to the algorithm shown in **Figure 8**, the PHY protocol of AP is IEEE 802.11a/n, consistent with the preset. The working frequency octets are 71 16 (first shaded part in the figure). According to the previous frame resolution method, the frequency is 5745 MHz, proving that the working frequency of AP is on the 5 GHz band.

The algorithm under the condition of IEEE 802.11n (5G) single mode is the same as that of IEEE 802.11a/n.

4.5. IEEE 802.11b/g/n

Set the PHY protocol of AP to IEEE 802.11b/g/n mixed mode. The captured data of a beacon frame are shown in **Figure 13**. Both HT Capabilities information element (the third shaded part in the figure) and ERP information element (the second shaded part in the figure) are existed. According to the algorithm shown in **Figure 8**, the PHY protocol of AP is IEEE 802.11b/g/n, consistent with the preset. The working frequency octets are 94 09 (first shaded part in the figure). According to the previous frame resolution method, the frequency is 2452 MHz, proving that the working frequency of AP is on the 2.4 GHz band.

The algorithm under the condition of IEEE 802.11n (2.4 G) single mode is the same as that of IEEE 802.11 b/g/n.

5. Conclusions

Capturing and resolving the MAC frames are the technical basis of kinds of security systems for IEEE 802.11 wireless network. Real-time detection of PHY protocol types of APs or STAs can help network manager to analyse the WLAN environment to identify suspicious devices. However, their solutions cannot be exported by the specifications due to different implementations and specifications not detailed enough. Also, no literature presents the related solutions, which might be due the research of packet capture and analysis focused on the PDU encapsulated in TCP or UDP rather than that in link layer frame in the past.

This paper proposed an analytical method for IEEE 802.11MAC frame and an algorithm for detecting PHY protocol types. The proposed method is based on analysing a large amount of captured MAC frames, and proved in an intrusion prevention system for WLAN. The detection algorithm of PHY protocols is easy to implement. The proposed ideas can not only be a reference for the research and development based on IEEE 802.11 Link Layer frame analysis, but also for capture and analysis of industrial protocol frames which are directly encapsulated in link layer frames, such as SV or GOOSE message in Smart Substation communications according to IEC 61850. That is, this work is also helpful for the research and development of testing and analysis systems for industrial devices, of which application PDUs are encapsulated in link layer frames.

We will research the relationship between the length of frame preamble and NIC. The data structure of frame preamble could also be further analysed. The detection method of the newest PHY standard IEEE 802.11ac, single mode and mixed mode of PHY protocol could be further explored etc.

Acknowledgements

We thank National Natural Science Foundation of China for funding (51377122).

References

[1] Gan, Y. (2012) Analysis on Military Application Pro- spects and Development of WLAN. *Communications Technology*, **45**, 1-9.

[2] You, T. and Liu, J. (2010) Research on Application of Wireless Local Area Network in Smart Power Grid. *Jilin Electric Power*, **38**, 20-23.

[3] Lai, Y., Wang, C., Tong, W. and Wang, X. (2014) Research on the Key Technology and Main Issues of Power Wireless Communication Network. *Electric Power Information and Communication Technology*, **12**, 10-14.

[4] Cai, Z. (2012) Discussion on the Application of Wireless Network Technology in Substation. *China New Technologies and Products*, **4**, 144.

[5] Boland, H. and Mousavi, H. (2004) Security Issues of the IEEE 802.11b Wireless LAN. *Electrical and Computer Engineering*, **1**, 333-336. https://doi.org/10.1109/ccece.2004.1345023

[6] Feng, P. (2012) Wireless LAN Security Issues and Solutions. *The Proceedings of IEEE Symposium on Robotics and Applications* (*ISRA*), Kuala Lumpur, 921-924.

https://doi.org/10.1109/isra.2012.6219343

[7] Singh, P., Mishra, M. and Barwal, P.N. (2014) Analysis of Security Issues and Their Solutions in Wireless LAN. *Information Communication and Embedded Systems* (*ICICES*), Chennai, 1-6. https://doi.org/10.1109/icices.2014.7033871

[8] Arockiam, L. and Vani, B. (2010) A Survey of Denial of Service Attacks and It's Countermeasures on Wireless Network. *International Journal on Computer Science and Engineering*, **2**, 1563-1571.

[9] Wu, K., Zhang, W. and Zhu, W. (2011) A Study on the Application of Intrusion Detection Technology to WLAN. Communication Software and Networks (ICCSN), Xi'an, 344-346.

[10] Overlay vs. Integrated Wireless Security—The Pros and Cons of Different Approaches to Wireless Intrusion Prevention. http://www.flukenetworks.com

[11] IEEE Std 802.11-2007 (2007) IEEE Standard for Information Technology—Telecommunications and Information Exchange between Systems—Local and Metropolitan Area Networks—Specific Requirements, Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications.

[12] IEEE Std 802.11-2012 (2012) IEEE Standard for Information Technology—Telecommunications and Information Exchange between Systems—Local and Metropolitan Area Networks—Specific Requirements, Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications.

[13] Gast, M.S. (2005) 802.11 Wireless Networks: The Definitive Guide. O'Reilly Media.