西方体制Mark XIIA的Mode 5数据格式分析

谭源泉[1,2]，李胜强[1]，王厚军[1]

(1. 电子科技大学通信抗干扰技术国家级重点实验室 成都 611731; 2. 四川九洲电器集团有限责任公司 四川 绵阳 621000)

【摘要】Mark XIIA是北约盟军统一研制的新型敌我识别系统，该系统的核心是Mode 5敌我识别。该文概述了Mark XIIA敌我识别系统的发展和系统组成，总结了Mode 5的4级工作模式，表明Mode 5不仅能完成基本的敌我识别功能，并具有态势感知、数据传输等功能；其次从安全性、数据容量、系统可靠性3个方面详细分析了Mode 5 Level 1和Level 2的数据格式特征，指出了Mode 5 Level 1和Level 2询问应答数据中的加解密数据段；最后，总结了Mode 5 IFF系统的特点。

关 键 词 加密; 纠错码; 敌我识别; Mode 5; 扩频

中图分类号 TN959.1 **文献标识码** A doi:10.3969/j.issn.1001-0548.2011.04.011

Analysis on Data Format of Mode 5 in Western Mark XIIA

TAN Yuan-quan[1,2], LI Sheng-qiang[1], and WANG Hou-jun[1]

(1. National Key Laboratory of Communication, University of Electronic Science and Technology of China Chengdu 611731;
2. Sichuan Jiuzhou Electric Group Co., Ltd Mianyang Sichuan 621000)

Abstract Mark XIIA is an new type identification foe or friend (IFF) system developed by NATO armies, and Mode 5 IFF is the core of the system. Firstly, the development and the framework of western Mark XIIA IFF system are summarized, the four operating modes of Mode 5 IFF system are introduced. It is shown that Mode 5 has not only the ability of IFF, but also the ability of battlefield situation awareness and data transmission. Secondly, from the viewpoint of security, capacity and reliability separately, the characters of the data format of Mode 5 Level 1 and Level 2 are analyzed in detail, the encrypted data and decrypted data in interrogation and reply are given. Finally, the characters of Mode 5 IFF are summarized.

Key words encryption; error-correct codes; IFF; Mode 5; spread spectrum

Mark XIIA敌我识别(IFF)系统是Mark XII的升级版本[1-2]。Mark XIIA于20世纪末开始研发，1998年以美国为首的“北约”5国(美国、英国、法国、德国和意大利)成立了Mode 5技术工作组，至2004年，工作组完成了Mode 5的统一设计和原理样机研究。目前，工作组成员国均已联合世界知名雷达生产商生产出了Mode 5敌我识别系统，且该类系统通常都兼容Mode 4的功能。到目前为止，TALES公司已向全球60多个国家和多种平台供应了16 000多套敌我识别设备[3-4]。

Mark XIIA敌我识别系统由询问机和应答机组成，用于进行协作式目标身份识别。Mark XIIA在Mark XII的基础上增加了Mode 5 IFF，它是Mark XIIA系统必须具备的核心。Mode 5加密敌我识别系统仍然遵循二次雷达系统的基本原理，并对二次雷达与Mode 4等原有技术作了较大的变革，如采用MSK调制技术、扩频技术、数据链路传输技术、计算机现代加密技术等，提高了敌我识别系统的抗干扰与欺骗、抗侦收能力，增强了敌我识别系统在各军兵种、盟军联合作战时的协同作战能力。采用Mode 5协同作战的各平台可实现空–空、空–海、空–地、海–空、海–海、地–空、地–地等全方位识别，能最大程度地满足现代信息战争及时掌握战场瞬息万变的信息的要求[5-6]。

1 Mark XIIA系统组成

Mark XIIA系统可作为单独的询问机和应答机装备在作战平台上，具有组合询问/应答的能力。图1为组合询问/应答机系统组成框图[7]，主要由天线单元、发射机/接收机单元、询问/应答信号处理单元和目标显示控制单元组成。在该系统中，Mode 5密码机作为系统的一个独立组件完成信息的加解密任务。Mode 5密码机和Mode 4兼容。

收稿日期：2011 – 05 – 02; 修回日期：2011 – 06 – 08
基金项目：部级预研基金
作者简介：谭源泉(1951 –)，男，研究员，主要从事二次雷达方面的研究.

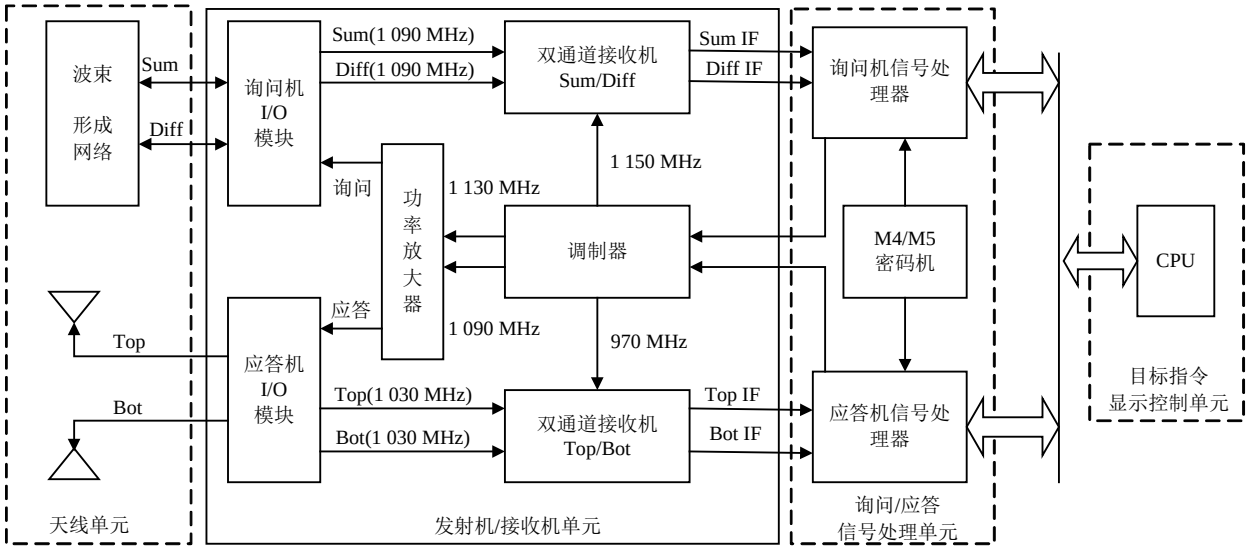

图1　Mark XIIA组合询问/应答机系统框图

2　Mode 5 IFF的应用模式

Mark XII Mode 4只能完成基本的识别功能，Mode 5不仅具有改进的询问/应答识别方式，而且还利用近年来的科技成果，增加了态势感知、选址询问、数据传输以及空对地识别模式。Mode 5有 4 级工作模式，分别为Level 1、Level 2、Level 3和Level 4[8]。各级工作模式的功能如下：

1) Level 1为改进的询问/应答识别模式，询问/应答信息中增加了平台识别编号和致命因子，致命因子为带有命令攻击意图的杀伤性询问信息；

2) Level 2为带有GPS位置报告的态势感知识别模式，位置报告中包含纬度、经度、高度、国家代码和任务代码等信息；

3) Level 3为友方目标选址询问模式，该模式实现了对友方战斗群中特定平台，如舰队的旗舰、飞行中队的长机进行个别询问；

4) Level 4是数据传输方式，可实现空中、水面、地面等各种武器平台间的高容量、高速率数据传输和交换。

3　Mark XIIA Mode 5的数据格式

Mode 5 Level 1和Level 2模式的询问/应答消息格式如图2～图4所示[9-10]。

图2为询问消息格式，其中，图2a为询问主机传递给加密机的消息；图2b为加密机回传给询问主机的消息；图2c为应答主机传递给解密机的消息；图2d为解密机回传给应答主机的消息。

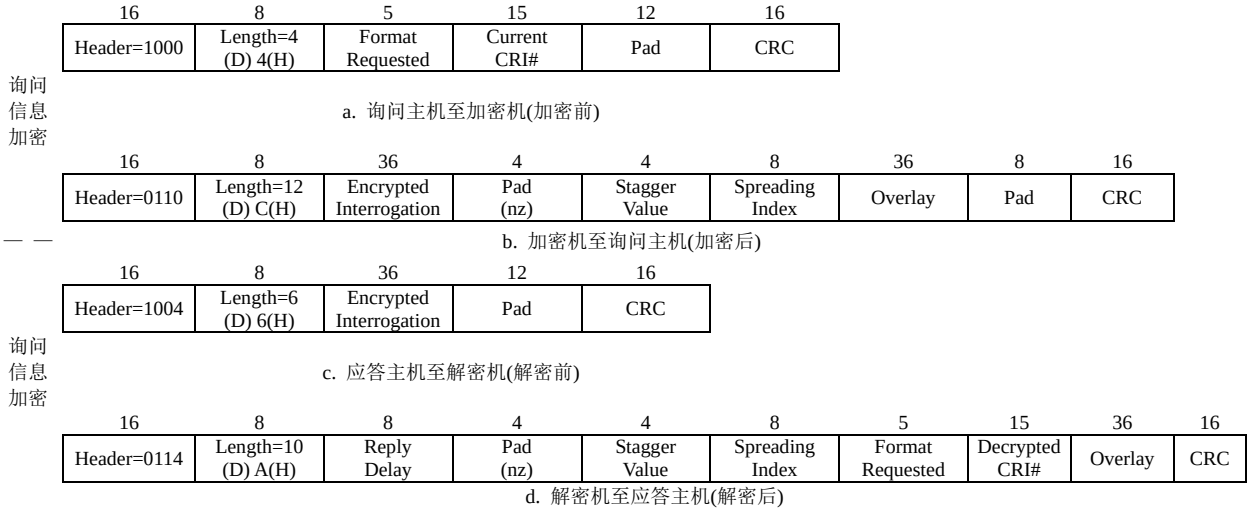

图2　Level 1和Level 2询问消息格式

图3为Level 1应答消息格式，根据询问信号的请求，Level 1应答分为两种情况，一是ID(身份)应答，二是Data(数据)应答。其中，图3a和图3c为应答主机传递给加密机的消息；图3b和图3d为加密机回传给应答主机的消息；图3e为询问主机传递给解密机的消息；图3f为解密机回传给询问主机的消息。36 bit的ID应答码包含两个8 bit RRD码和两个10 bit随机码，Data应答码包含8 bit RRD码和28 bit数据码。Data应答根据28 bit数据的不同，区分为Mode 1/2数据应答、Mode 3/C数据应答和PIIN数据应答3种情况。

图4为Level 2应答消息格式。其中，图4a为应答主机传递给加密机的消息；图4b为加密机回传给应答主机的消息；图4c为询问主机传递给解密机的消息；图4d为解密机回传给询问主机的消息。Level 2应答报告中的4 bit Format Requested字段将Level 2的报告内容分为ID PIN(0000)、Data M1/M2(0001)、Data M3/Altitude(0010)、Lethal PIN(0011)和Data High-Res PIN(0100) 5种情况。27 bit的Tactical Data字段中包括纬度、经度、海拔等信息。

ID应答加密 / 数据应答加密 / 应答解密

16	8	36	12	16
Header=1008	Length=6 (D) 6(H)	Protected Reply	Pad	CRC

a. 应答主机至加密机(加密前)

16	8	36	12	16
Header=0118	Length=6 (D) 6(H)	Encrypted Reply	Pad	CRC

b. 加密机至应答主机(加密后)

16	8	36	12	16
Header=1009	Length=6 (D) 6(H)	Protected Reply	Pad	CRC

c. 应答主机至加密机(加密前)

16	8	36	12	16
Header=0119	Length=6 (D) 6(H)	Encrypted Reply	Pad	CRC

d. 加密机至应答主机(加密后)

16	8	36	12	16
Header=100A	Length=6 (D) 6(H)	Encrypted Reply	Pad	CRC

c. 询问主机至解密机(解密前)

16	8	36	12	16
Header=0119	Length=6 (D) 6(H)	Protected Reply	Pad	CRC

f. 解密机至询问主机(解密后)

图3 Level 1应答消息格式

应答信息加密

16	8	77	4	15	16
Header=1001	Length=12 (D) C(H)	Tactical Data	Format Requested	Current CVI#	CRC

a. 应答主机至加密机(加密前)

16	8	108	4	16
Header=0111	Length=14 (D) E(H)	Encrypted Report	Pad	CRC

b. 加密机至应答主机(加密后)

应答信息解密

16	8	108	4	16
Header=1005	Length=14 (D) E(H)	Encrypted Report	Pad	CRC

c. 询问主机至加密机(解密前)

16	8	77	12	4	15	4	16
Header=0115	Length=14 (D) E(H)	Tactical Data	Unique	Format Requested	Current CRI#	Pad	CRC

d. 加密机至询问主机(解密后)

图4 Level 2应答消息格式

3.1 安全性分析

在Mode 5 IFF中，询问/应答信息均是经过加密处理后再在识别传输信道上传输的。NSA采用的加解密算法为JOSEKI算法，该算法是NSA所设计的4类密码算法之一。

在Mode 5中，加解密算法的设计具有较大的灵活性，只要满足加解密机与询问/应答机之间的接口要求，并且加解密算法达到指定的安全性即可。加解密算法的灵活性可满足多个不结盟国家对敌我识别系统的需要。

表1列出了Mode 5 IFF Level 1和Level 2询问信息通过加解密算法的输入、输出字段及其长度。

表2列出了Level 1应答信息通过加解密算法的输入、输出字段及其长度。

表1 Level 1和Level 2询问信息通过加解密算法情况

	输入字段及其长度	输出字段及其长度
加密算法	Format Requested (5 bit)+ Current CVI (15 bit)	Encrypted Interrogation (36 bit)
解密算法	Encrypted Interrogation (36 bit)	Format Requested (5 bit) + Decrypted CVI (15 bit)

表2 Level 1应答信息通过加解密算法情况

	加密算法		解密算法	
	输入字段及其长度	输出字段及其长度	输入字段及其长度	输出字段及其长度
ID应答	Protected Reply (36 bit)	Encrypted Reply (36 bit)	Encrypted Reply (36 bit)	Protected Reply (36 bit)
Data应答	Protected Reply (36 bit)	Encrypted Reply (36 bit)	Encrypted Reply (36 bit)	Protected Reply (36 bit)

表3列出了Level 2应答信息通过加解密算法的输入、输出字段及其长度。

表3　Level 2应答信息通过加解密算法情况

	输入字段及其长度	输出字段及其长度
加密算法	Tactical Data (77 bit)+ Format Requested (4 bit)+ Current CVI (15 bit)	Encrypted Report (108 bit)
解密算法	Encrypted Report (108 bit)	Tactical Data (77 bit)+ Format Requested (4 bit)+ Current CVI (15 bit)

从表1～表3可知，Mode 5密码机中加密算法的输入和输出数据的长度并不完全相同，因此，所设计的加解密算法的输入输出长度必须满足表1～表3所列的对输入输出的长度要求。

3.2　容量分析

图5为Mode 5 IFF的询问信号格式。该询问信号格式由4个同步脉冲(*P*1,*P*2,*P*3,*P*4)，2个旁瓣抑制脉冲(*L*1,*L*2)和11个数据脉冲(*D*1～*D*11)组成。11个数据脉冲是由图3中的Encrypted Interrogation(36 bit)经(11,9,1) RS码编码扩展成44 bit后再经调制形成的。脉冲信号调制方式为MSK，调制码速率为16 Mb/s。

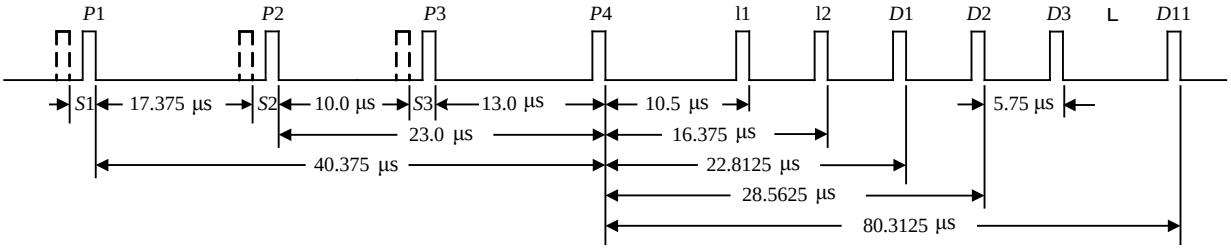

图5　Level 1和Level 2询问信号格式

图6为Mode 5 Level 1的应答信号格式。该应答信号格式由两个同步脉冲(*P*1,*P*2)和一个数据长脉冲(9个字符*D*1～*D*9)组成。同步脉冲及数据长脉冲采用MSK调制，调制码速率为16 Mb/s。

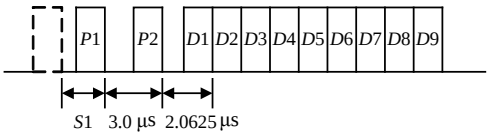

图6　Level 1应答信号格式

图7为Mode 5 Level 2的应答信号格式。该应答信号格式由4个同步脉冲(*P*1,*P*2,*P*3,*P*4)和一个数据长脉冲(33个字符*D*1～*D*33)组成。数据长脉冲中，每一个字符包含4 bit，33个字符共含132 bit，由图5中的Encrypted Report (108 bit)字段经 (11,9,1) RS码编码扩展成132 bit后再经调制形成。脉冲调制方式为MSK调制，调制码速率为16 Mb/s。

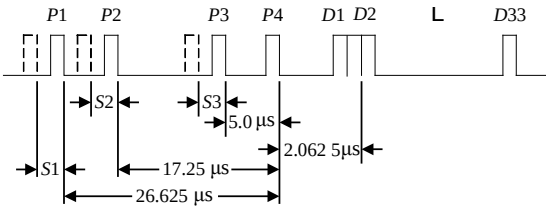

图7　Level 2应答信号格式

3.3　可靠性分析

从数据格式的角度，Mode 5采用纠错编码和直接序列扩频两种技术提高了传输数据的抗干扰能力。

RS码是一类具有很强纠错能力的多进制BCH码，特别适用于存在突发错误的信道。Mode 5 IFF中采用的是有限域GF(16)上的(11,9,1) RS码，该码由GF(16)上的(15,13,1) RS码截短而得到。(11,9,1) RS码能纠正一个符号错误和擦除两个符号错误。

在扩频方面，Mode 5采用基于Walsh码的直接序列扩频最小相移键控调制方式，使用周期为16的Walsh码(0111100010001001)对每一个前导脉冲符号和数据符号进行扩频，调制码速率为16 Mb/s。Walsh码具有很好的同步互相关特性，可有效防止多址干扰，并为系统的选址询问提供了可能。

4　结　论

Mark XIIA Mode 5敌我识别系统是针对现役IFF Mark X或IFF Mark XII所存在的目标正确识别概率不高、信号串扰和混扰严重等不足而设计的。它具有向下兼容，可为友方部队提供确切的加密敌我识别信息，构造方式灵活等优点，同时，Mode 5所提供的保密性也优于Mode 4。

综上所述，Mode 5 IFF系统具有以下特点：

1) Mode 5 IFF 与现役的MK系列敌我识别器在技术体制和工作频率上并无本质区别，上行载波频率为1 030 MHz，下行载波频率为1 090 MHz，大大减少了平台升级的难度。

2) 工作模式多，Mode 5 IFF有4级工作模式，可满足多种应用场合。

3) 对询问/应答信息进行了加密处理，增强了信息的保密性，且加密算法的设计具有较大灵活性，可满足多个不结盟国家对敌我识别系统的需求。

参 考 文 献

[1] 黄成芳, 何利民. 敌我识别MK XIIA浅析[J]. 电讯技术, 2007, 47(4): 66-71.
HUANG Cheng-fang, HE Li-min. Discussion of IFF MK XIIA Mode 5[J]. Telecommunication Engineering, 2007, 47(4): 66-71.

[2] 时宏伟. 模式V加密敌我识别系统[J]. 电讯技术, 2001, 41(2): 25-28.
SHI Hong-wei. Mode V encryption IFF system[J]. Telecommunication Engineering, 2001, 41(2): 25-28.

[3] 张尉. 二次雷达原理[M]. 北京: 国防工业出版社, 2007.
ZHANG Wei. Secondary surveillance radar heory[M]. Beijin: National Defence Industry Press, 2007.

[4] 王洪, 刘昌忠, 汪学刚. 二次雷达S模式综述[J]. 电讯技术, 2008, 48(7): 113-118.
WANG Hong, LIU Chang-zhong, WANG Xue-gang. Mode S for secondary surveillance radar: an introduction and overview[J]. Telecommunication Engineering, 2008, 48(7): 113- 118.

[5] MANUEL L G, JOHN M H. Test for success: next generation aircraft identification system RF simulation [C]//Integrated Communications, Navigation and Surveillance Conference. Virginia: IEEE Press, 2007: 1-10.

[6] 邱宏坤, 杨建波, 毛虎. Mark XIIA 系统及其信号消息格式[J]. 电讯技术, 2010, 50(6): 16-21.
QIU Hong-kun, YANG Jian-bo, MAO Hu. Mark XIIA IFF system and its signal message formats[J]. Telecommunication Engineering, 2010, 50(6): 16-21.

编 辑 张 俊

(上接第511页)

[8] GUI Lin, LI Qi, LIU Bo, et al. Low complexity channel estimation method for TDS-OFDM based chinese DTTB system[J]. IEEE Transactions on Consumer Electronics, 2009, 55(3): 1135-1140.

[9] LIU Guang-hui, ZHIDKOV S V. A composite PN-correlation based synchronizer for TDS-OFDM receiver[J]. IEEE Transactions on Broadcasting, 2010, 56(1): 77-85.

[10] MA Rui-feng, DAI Ling-long, WANG Zhao-cheng, et al. Secure communication in TDS-OFDM system using constellation rotation and noise insertion[J]. IEEE Transactions on Consumer Electronics, 2010, 56(3): 1328-1332.

[11] HE Li-feng, YANG Fang, ZHANG Chao, et al. Synchronization for TDS-OFDM over multipath fading channels[J]. IEEE Transactions on Consumer Electronics, 2010, 56(4): 2141-2147.

[12] SONG Bo-wei, GUI Lin, GUAN Yun-feng, et al. On channel estimation and equalization in TDS-OFDM based terrestrial HDTV broadcasting system[J]. IEEE Transactions on Consumer Electronics, 2005, 51(3): 790-797.

[13] A.V.奥本海姆, R.W.谢弗. 离散时间信号处理[M]. 黄建国, 刘树棠, 译. 北京: 科学出版社, 2000: 632-634.
OPPENHEIM A V, SCHAFER R W. Discrete-time signal processing [M]. Translated by Huang Jian-guo, Liu Shu-tang. Beijing: Science Press, 2000: 632-634.

编 辑 张 俊