doi: 10.7690/bgzdh.2014.11.007

MIL-STD-188-220C 网控站识别方法

方凌江，蔡雨珈
（济南军区联勤部后勤信息中心，济南 250022）

摘要：为了在报文不解密条件下快速分析出基于 MIL-STD-188-220C 协议的某无线电台的网控站，提出一种基于识别状态通知消息的 MIL-STD-188-220C 网控站识别方法。在不对目标网络通信报文进行解密的情况下，运用探测节点截获的数据，对运行 MIL-STD-188-220C 协议的网络的网控站所在位置进行识别，将网控站的识别问题转换为对其发起的状态通知消息的识别，推导并建立了网控站识别算法，确定网控站所在位置。仿真结果表明，该方法能以较高的正确率实现在信息不解密条件下网控站所在位置的识别。

关键词：MIL-STD-188-220C；网控站；状态通知消息
中图分类号：TP393.02　　**文献标志码**：A

Recognition Algorithm of Network Controller of MIL-STD-188-220C

Fang Lingjiang, Cai Yujia
(*Logistics Information Centre*, *Joint Services Department*, *Jinan Military Region*, *Jinan* 250022, *China*)

Abstract: Under non-decryption message condition, for fast analysis of certain type wireless radio station network controller based on MIL-STD-188-220C protocol, design a network controller recognition algorithm based on recognition on the status notification message of MIL-STD-188-220C. On the condition of unknowing the content of the frame, use the data which the detecting nodes get to work out the location of the network controller in MIL-STD-188-220C network by converting the position recognition to the status notification message recognition. This paper also gets the algorithm of recognition on network controller to points out the location of the network controller. Simulation results show that the algorithm can get the location of the network controller at the high level of correction on the condition of the frame is not decrypt.

Keywords: MIL-STD-188-220C; network controller; status notification message

0 引言

MIL-STD-188-220C 协议是一种兼容 C4I 体系的互操作标准。它满足了指挥、控制、通信等协同一体的要求，因而广泛运用于某无线网络的组网和通信之中[1]。

在信息化条件的无线网络环境中，如何在报文不解密条件下快速分析出基于 MIL-STD-188-220C 协议的某无线网络的网控站具有重要的意义。通过在报文不解密条件下分析网控站所在区域，可以在被探测方非觉察的情况下确定网络控制与配置节点，进而大大提升干扰此类节点的精确性和有效性[2]。

笔者通过分析 MIL-STD-188-220C 协议，总结出网控站发送消息的特点，提出通过识别网控站发送的状态通知消息来获得网控站所在区域的网控站识别算法，并通过仿真对提出方法的有效性进行了验证。

1 MIL-STD-188-220C 网控站识别整体思路

网控站是运行 220C 协议的某无线网络中用于维持全网正常通信的管理节点，其地位十分重要。为了增强其隐蔽性，除了网络管理业务和拓扑更新外，它并不参与普通的数据传输。因此，识别网控站，只能从它的管理业务入手进行分析[3]。

220C 协议的 CNR 管理规程规定，为了保证全网节点都以最新的网络参数进行通信，网控站需要周期性地广播状态通知消息[4]。这种消息的作用是告知每个节点网络的最新状态、网控站身份、参数更新标志等信息[5]。为了保障网络中的节点尽快获得最新参数，此消息发送的优先级较一般消息高，通常插入报文队列队头进行发送，是一种以帧间间隔为保护措施的广播消息[6]。

笔者从网控站发送的广播消息中的状态通知消息入手，通过对状态通知消息的识别来确定网控站位置，其基本的识别过程为：首先将探测节点截获的报文按照到达时间进行排序，之后从报文中提取状态通知消息，最后根据识别出的状态通知消息序列中的第一个消息的发起方位置确定网控站所在的探测区域，即以最近一次状态通知过程中最先截获状态通知消息的探测节点的探测范围作为网控站所

收稿日期：2014-06-03；修回日期：2014-08-12
作者简介：方凌江（1955—），男，湖南人，硕士，高级工程师，从事指挥自动化及网络安全技术研究。

在的区域。由此过程可以看出：整个识别过程的关键在于第 2 步——在信息不解密条件下，如何对状态通知消息进行识别。

2　状态通知消息识别方法

2.1　状态通知消息建模

为了分析状态通知消息的特点，首先对一次状态通知过程进行建模。

网络中出现一次状态通知消息广播过程为一次状态通知过程。网络中出现的第 j 次状态通知过程可以表示为：

$$p_j=\{f_1(l_1,t'_1),f_2(l_2,t'_2),f_3(l_3,t'_3),\cdots,f_i(l_i,t'_i),f_n(l_n,t'_n)\} \quad (1)$$

其中：$f_i(l_i,t'_i)$ 表示在第 j 次状态通知过程中出现的第 i 个状态通知消息。t'_i 表示第 i 个状态通知消息的到达时间(截获时间)，l_i 表示第 i 个状态通知消息的长度；n 表示网络中出现的状态通知消息的个数。由于状态通知消息在广播过程中长度不发生变化，因此有 $l_1=l_2=l_3=\cdots=l_n=l$。若网络中存在 S 个目标节点，则在理想情况下，在一次状态通知过程中，n 等于目标节点个数 S。同时，由于状态通知消息的优先级较高且是一种帧间间隔为保护措施的广播，因此，其帧间间隔的均值 $E[t'_i-t'_{i-1}]$ 以较大概率小于 2 个无关且长度为 l 的帧的帧间间隔。

网络中连续出现多次状态通知过程可表示为：

$$P=\begin{Bmatrix} p_1(L_1,t_1) \\ p_2(L_2,t_2) \\ \vdots \\ p_j(L_j,t_j) \\ \vdots \end{Bmatrix} \quad (2)$$

其中，$p_j(L_j,t_j)$ 表示第 j 次状态通知过程，t_j 表示第 j 次状态通知过程的开始时间，L_j 表示第 j 次状态通知过程中状态通知消息的长度。由于网控站周期式地发送状态通知消息，因此有 $t_j=t_{j-1}=T+\delta$，$1<j\leqslant n+1$，T 为状态通知消息发起周期，δ 为扰动项。又因为状态通知消息为定长，因此有 $L_1=L_2=\cdots=L$。

由建立的模型可以看出，对状态通知消息的识别可分为 2 步。首先将数据帧按照接收时间的先后顺序进行排列，之后根据帧长和帧间间隔对截获的数据帧进行分类和过程划分，形成多个按照时间排列的数据帧集合。最后通过状态通知过程的周期性对生成的多个帧集合进行筛选，进而识别出真正的状态通知消息。

2.2　一次状态通知过程划分方法

2.2.1　根据帧间间隔对状态通知过程进行划分

由协议可知，网控站发送的状态通知消息是等长的具有较高优先级的广播帧。节点在转发这些帧的过程中，选择的退避时隙数比普通数据要小。220C 协议规定，普通消息和状态通知消息的最大退避窗长计算公式分别为公式 (3) 和公式 (4)。

$$F=2(NS+1) \quad (3)$$

$$F=NS+1 \quad (4)$$

其中 NS 为目标节点个数。同时，220C 协议还规定，当节点发送状态通知消息时，会将此消息插入队头进行发送。同时，状态通知消息具有帧间间隔保护措施，当节点收到状态通知消息时，在规定的保护时隙内，除了发送状态通知消息之外，不得发送其他帧。为了测试状态通知消息的特点，可以采用 NS2 仿真软件模拟 220C 网络。通过仿真生成的 trace 文件，可以对相邻状态通知消息和相邻 2 个非状态通知消息但长度等于状态通知消息长度的消息(以下称为“类状态通知消息”)的帧间间隔进行统计。在整个仿真中，一次状态通知过程中，状态通知消息的平均帧间间隔最大为 0.003 7 s，统计 100 次状态通知过程，得到的状态通知消息平均帧间间隔为 0.002 1 s；以状态通知过程周期为观测的单位时间，在单位时间内，统计类状态通知消息的平均最大帧间间隔为 0.76 s。在整个仿真过程中的平均帧间间隔为 0.3 s。可以看出 2 种消息的平均帧间间隔存在明显差异。

设在一次状态通知过程中，任意 2 个相邻状态通知消息的平均帧间间隔为 $\overline{T_{\text{通知}}}$，任意 2 个节点产生的状态通知消息的平均时间间隔为 $\overline{T_1}$，平均选择的退避时隙数为 $\overline{T_2}$，则

$$\overline{T_{\text{通知}}}=\overline{T_1}+\overline{T_2}=\overline{T_{\text{delay}}}/\text{NAD\_slot}+\overline{T_2}\ [7] \quad (5)$$

其中：$\overline{T_{\text{delay}}}$ 表示一跳时延；NAD_slot 为网络接入时延单位时隙。当网络中的节点个数为 $NS-1$ 时，

对于状态通知消息来说，

$$\overline{T_2}=\frac{1}{NS}\bullet\frac{1}{NS}\bullet(NS-1)+2\frac{1}{NS}\bullet\frac{1}{NS}\bullet(NS-2)+\cdots+\frac{1}{NS}\bullet\frac{1}{NS}\bullet\left[NS-(NS-1)\right](NS-1)=\sum_{k=1}^{NS-1}k\bullet\frac{1}{NS^2}(NS-k) \tag{6}$$

将公式 (6) 代入 (5)，可得

$$\overline{T_{\text{通知}}}=\overline{T_{\text{delay}}}/\text{NAD\_slot}+\sum_{k=1}^{NS-1}k\bullet\frac{1}{NS^2}(NS-k) \tag{7}$$

设类状态通知消息的平均帧间间隔为 $\overline{T_{\text{类}}}$，任意 2 个相邻类状态通知消息的平均到达时隔为 $\overline{T_3}$，类状态通知消息发送时，平均选择的退避时隙数为 $\overline{T_4}$，则

$$\overline{T_{\text{类}}}=\overline{T_3}+\overline{T_4} \tag{8}$$

若网络中分组的产生速率为 λ，网络中节点个数为 $NS-1$，数据帧长度服从 3～61 字节均匀分布，最大退避窗长为 $2NS$，则，

$$\overline{T_3}=\frac{61-3}{\lambda\bullet\text{NAD\_slot}} \tag{9}$$

$$\overline{T_4}=\frac{1}{2NS}\bullet\frac{1}{2NS}\bullet(2NS-1)+2\frac{1}{2NS}\bullet\frac{1}{2NS}\bullet(2NS-2)+\cdots+\frac{1}{2NS}\bullet\frac{1}{2NS}\bullet[2NS-(2NS-1)](2NS-1)=\sum_{k=1}^{2NS-1}k\bullet\frac{1}{4NS^2}(2NS-k) \tag{10}$$

将公式 (9) 和公式 (10) 代入公式 (8) 可得

$$\overline{T_{\text{类}}}=\overline{T_3}+\overline{T_4}=\frac{61-3}{\lambda\bullet\text{NAD\_slot}}+\sum_{k=1}^{2NS-1}k\bullet\frac{1}{4NS^2}(2NS-k)=\frac{58}{\lambda\bullet\text{NAD\_slot}}+\sum_{k=1}^{2NS-1}k\bullet\frac{1}{4NS^2}(2NS-k) \tag{10}$$

公式 (7) 和 (11) 从理论上说明了状态通知消息与类状态通知消息的平均帧间间隔存在较大差距的原因。对于探测方来说，公式中的参数 $\overline{T_{\text{delay}}}$、NAD_slot、$\lambda$ 等都可以通过 220C 协议规定和实际网络情况测得。因此，通过将估计值代入公式 (7) 和 (11)，可以得到状态通知消息和类状态通知消息的平均帧间间隔，进而设定分类门限。在文中，用 $t_{\max}$ 次状态通知过程帧间间隔分类门限，并根据多次仿真获得的经验值规定 $t_{\max}=(2\sim5)\overline{T_{\text{通知}}}$[8]。在上文仿真条件下，探测方通过观测网络中报文的出现速率可以得到 $\overline{T_{\text{通知}}}=10\text{NAD\_slot}$，$\overline{T_{\text{类}}}=750\text{NAD\_slot}$。设 $t_{\max}=2\overline{T_{\text{通知}}}=20\text{NAD\_slot}$，当 2 个连续出现在网络中的等长帧的帧间间隔小于 $t_{\max}$ 时，这 2 个帧被认为是 1 个状态通知过程中的状态通知消息，否则认为是 2 个状态通知过程的状态通知消息[9]。

2.2.2 对一次状态通知过程进行粗筛

在第一步识别中，探测方得到了多个可能为状态通知过程的过程集合。为了减小下一步识别的计算量，提高准确性，需要对这些过程进行粗筛。

设目标节点个数为 NS，则在一次状态通知过程中，状态通知消息被发送的次数为 NS。但是，由于目标节点本身发生故障、丢包等情况，使得第一步识别的输出中，一般不会含有太多分组个数恰好为 NS 的过程。因此，结合 220C 网络的丢包率，笔者采用 $NS/2$ 作为判断一次状态通知过程的标准[10]。对于第一步识别得到的多个过程，如果某个过程含有的分组个数小于 $NS/2$，则认为这个过程不是状态通知过程而直接剔除。

经过以上两步，可以将状态通知消息组成的过程及其他部分满足条件的广播过程等识别出来。

2.2.3 对状态通知消息进行识别

在上述单个状态通知过程识别的基础上，下面通过状态通知过程发起的周期性对满足第一、二步筛选条件的非状态通知消息进行剔除，从而最终完成状态通知消息的识别。

设网控站发送状态通知消息的周期为常数 T，则 2 次相邻的状态通知过程的开始时间差值满足下式：

$$t_i-t_{i-1}=T+\delta \tag{11}$$

其中：t_i 为第 i 次状态通知过程的开始时间；δ 为扰动项。当网控站进行信道竞争或正在发送其他数据而延迟状态通知消息的发送时，都会引入周期的扰动。

但是，相较于其他没有周期性的广播来说，这种扰动是较小的。通过上文中对状态通知消息进行仿真，并对 100 次状态通知过程的相邻过程到达时间间隔进行统计，可以得到其过程间隔方差为 0.83。

同时，在仿真中加入非周期产生的广播消息，并计算广播消息的间隔方差，可以得到过程间隔的方差为 6.75，明显大于状态通知消息的方差。因此，可以通过过程到达时间间隔的方差对状态通知消息进行识别。

设探测时间为 T'，集合 i 中含有的过程个数为 m_i，过程到达间隔均值为 ΔT_i，过程到达间隔方差为 D_i，$i=1,2,3,\cdots,K$，K 为第一步识别中得到的集合个数。首先将只含有 2 个或少于 2 个过程的集合直接剔除，然后选取满足不等式 $\left|\frac{T'}{\Delta T_i}-m_i\right|\leqslant\varepsilon$ 的集合计算 D_i，ε 为过程个数误差参数。文中通过大量仿真，选取 $\varepsilon=3$ 作为过程个数误差参数。最后，选取在满足 $\left|\frac{T'}{\Delta T_i}-m_i\right|\leqslant\varepsilon$ 条件下具有最小方差的过程集合为状态通知过程集合。

综上所述，对状态通知消息的识别可分为 3 步：

第 1 步为一次状态通知过程的识别，首先将截获的数据按照帧长分为不同的集合，之后对每个集合，以门限 $t_{\max}$ 对其中的帧进行划分，得到多个可能的状态通知过程集合；

第 2 步对可能的状态通知过程集合进行二次筛选，将帧个数不满足条件的过程剔除；

第 3 步计算每个过程的开始时间间隔的均值及方差，选取在满足 $\left|\frac{T'}{\Delta T_i}-m_i\right|\leqslant\varepsilon$ 条件下具有最小方差的集合作为状态通知过程集合。

需要注意的是，这种识别状态通知消息的方法也有一定的局限性。首先，当网络中含有其他周期等长广播业务时，如果不附加其他条件，此识别方法失效；第二，目标节点个数对探测方来说是已知的；第三，为了保证探测数据中尽可能多地含有状态通知过程，探测时间应足够长。

3　网控站识别算法流程

将上文状态通知消息识别的过程进行总结和抽象，可以得到网控站识别算法流程。

1) 在截获的报文中加入探测节点信息，并按照报文到达时间的先后对报文进行排列以形成数据集合 X。$x_i=\{\text{spyid},t_i,f_i\},x_i\in X$。其中，$t_i$ 为报文到达时间，f_i 为帧长，spyid 为探测节点标号。

2) 对数据集合 X 进行遍历，以帧长 $f_1,f_2,\cdots,f_k$ 为特征将数据集合划分为 k 类，划分依据如下准则：若 $f_i=f_j$，则 x_i 和 x_j 被划分为一类。其中 $i=1,\cdots,n$；$j=1,\cdots,n$，n 为截取的数据总数。

3) 根据公式 $\overline{T_{\text{通知}}}=\overline{T_{\text{delay}}}/\text{NAD\_slot}+\sum_{k=1}^{NS-1}k\cdot\frac{1}{NS^2}(NS-k)$ 算出相邻状态通知消息的平均帧间间隔及帧间间隔识别门限 $t_{\max}$，$t_{\max}=(2\sim5)\overline{T_{\text{通知}}}$。其中，计算 $\overline{T_{\text{通知}}}$ 所需的参数通过 220C 协议获得，NS 为已知条件。

4) 对 k 类数据集合进行二次划分，划分依据如下准则：对于每个集合中的元素 x_i 和 x_j，若 $0<t_j-t_i<t_{\max}$，则 x_i 和 x_j 被划分为 1 个过程。当遍历集合中的每个元素后，会形成若干个过程。在每个过程中包含若干个帧，其前一帧与其后一帧均满足 $t_j-t_i<t_{\max}$。

5) 对于每个过程 $P_i=\{x_1,x_2,\cdots,x_m\}$，若 $m<\frac{NS}{2}$，则删去此过程。

6) 删去含有 2 个或 2 个以下过程的集合，然后计算剩余的每个集合中相邻过程的到达时间间隔的均值和方差，选取在满足 $\left|\frac{T'}{\Delta T_i}-m_i\right|\leqslant\varepsilon$ 的条件下具有最小方差的集合作为状态通知过程集合。

7) 选取状态通知过程集合中的最后一个过程中截获第一帧的探测节点的探测范围作为网控站的所在区域。

4　仿真验证

为了验证该方法的有效性，笔者通过采用 NS2 仿真软件，依据 220C 网络层、数据链路层和 CNR 管理层协议搭建了一个 220C 目标网络。目标网络场景设置如表 1 所示。分别对 3 种网络场景进行仿真。每个场景仿真 30 次，每次目标节点位置随机生成，一次仿真时间为 600 s。

表 1 验证场景的参数设置

场景参数	仿真场景		
	1	2	3
CBR 业务速率/(包/s)	2	5	10
状态通知周期/s	10	20	30
仿真区域/m^2	600×600	600×600	600×600
节点个数	15	15	15
NAD_slot/μs	260×10^{-3}	260×10^{-3}	260×10^{-3}
探测节点个数	9	9	9
数据包长度	3～61 字节随机选取	3～61 字节随机选取	3～61 字节随机选取
队列模型	高优先级报头插入队头发送	高优先级报头插入队头发送	高优先级报头插入队头发送

探测节点布设方法如图 1 所示。在探测方获取所有报文后，对每个报文提取帧长、到达时间、截获探测节点标号三类信息并组成数据元，之后按照到达时间先后将数据元进行排列以作为算法的输入数据。

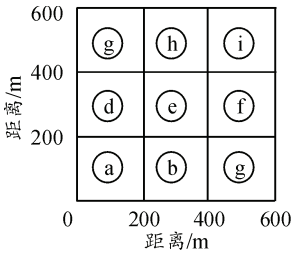

图 1 探测节点布设方法

表 2 3 种场景下网控站识别算法正确识别概率 %

识别概率	仿真场景		
	1	2	3
正确概率	86	83.6	71.2
总识别率	80.2	80.2	80.2

分别对 3 种仿真场景提供的数据应用识别算法，并将识别结果与仿真中实际的网控站位置进行对比，以判断是否正确识别出网控站所在的区域。得到的正确识别概率如表 2 所示。其中，场景 3 的识别率较其他场景低。这是由于当 λ 变大时，$\overline{T_{类}}$ 变小，在帧间间隔门限 $t_{\max}$ 不变的情况下，在第 1 步识别中，算法将更多的无关的等长消息判为可能的状态通知消息。这样不仅影响到第一步识别的正确率，还间接导致第 2 步识别率的降低；同时，在探测时间相等的情况下，场景 3 中网控站发起状态通知消息的周期最长，导致了探测节点截获的状态通知消息样本较少。基于以上这 2 个原因，场景 3 获得的正确识别率最低。

5 结束语

在信息不解密条件下实现网控站的识别，具有识别速度快、条件自适应强的优势，对无线网络的隐蔽式攻击具有重要意义。笔者研究了在不对目标网络通信报文进行解密的情况下，运用探测节点截获的数据，对运行 MIL-STD-188-220C 协议的网络的网控站所在位置进行识别的方法，将网控站的识别问题转化为对其发起的状态通知消息的识别，设计了网控站识别算法，并通过仿真数据验证了其有效性。理论推导和仿真结果表明：该算法能够识别出网控站所在区域，满足识别和攻击的要求。

参考文献：

[1] MIL-STD-188-220C[EB/OL]. Department of Defense Interface Standard. http://www-cnrwg.its.disa.rail.mal, 1998.

[2] 李冬, 宋里宏, 王璐, 等. 战场网络攻击效能分析[J]. 网络安全技术与应用, 2007, 24(3): 78-79.

[3] 数字信息传输子系统接口标准[D]. C 版. 广州: 中电科技集团公司第七研究所, 2003.

[4] 伍春华. 因特网流量建模及其在网络仿真中的应用[D]. 长沙: 中南大学, 2001.

[5] 徐江涛. 战术无线电互联网传输协议仿真研究[D]. 西安: 西安工业大学, 2006.

[6] 费忠霞, 尹华锐, 徐佩霞. 基于 DSP 的 LINK11 数据链对抗系统[J]. 航天电子对抗, 2005, 21(4): 51-54.

[7] Whitehill, E. A. Use of end-to-end acknowledgement in MIL-STD-188-220 extended netword[C]. Tactical Communication Conference, Fort Wayne, USA, 1996.

[8] 唐桂华. 基于 220C 协议的网络层及其测试平台的设计与实现[D]. 北京: 北京航空航天大学, 2004.

[9] 池凯莉, 董林玺. BP 神经网络分步赋初值算法的研究[J]. 机电工程, 2013, 30(2): 245-248.

[10] 陈志昊, 陈正捷. 基于多 Agent 技术的非战争军事行动应急指挥平台[J]. 兵工自动化, 2009, 28(2): 1-5.