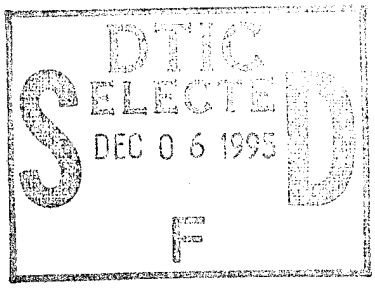
ESC-TR-95-050

Technical Report 1023

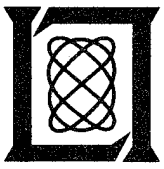
A Combat Identification Model for Netted Theater Air Defense Systems



S.D. Weiner
D.P. Cebula

27 November 1995

Lincoln Laboratory
MASSACHUSETTS INSTITUTE OF TECHNOLOGY
LEXINGTON, MASSACHUSETTS



Prepared for the Ballistic Missile Defense Organization
under Air Force Contract F19628-95-C-0002.

This report is based on studies performed at Lincoln Laboratory, a center for research operated by Massachusetts Institute of Technology. The work was sponsored by the Ballistic Missile Defense Organization, under Air Force Contract F19628-95-C-0002.

The ESC Public Affairs Office has reviewed this report, and it is releasable to the National Technical Information Service, where it will be available to the general public, including foreign nationals.

This technical report has been reviewed and is approved for publication.

FOR THE COMMANDER

Gary Tutungian
Administrative Contracting Officer
Contracted Support Management

MASSACHUSETTS INSTITUTE OF TECHNOLOGY
LINCOLN LABORATORY

A COMBAT IDENTIFICATION MODEL FOR NETTED THEATER AIR DEFENSE SYSTEMS

S.D. WEINER
Group 32

D.P. CEBULA
Group 106

TECHNICAL REPORT 1023

27 NOVEMBER 1995

LEXINGTON MASSACHUSETTS

ABSTRACT

An integrated Theater Air Defense (TAD) system must handle a variety of targets including Theater Ballistic Missiles (TBMs), Cruise Missiles (CMs) and manned aircraft (A/C). It must destroy enemy targets without attacking friendly and neutral targets, especially manned A/C. The process of deciding which targets should be attacked is called Combat Identification (CID) which includes cooperative Identification Friend or Foe (IFF) as a sub-case.

Recently there has been considerable interest in netted TAD systems in which information on enemy targets and defense actions is passed from one defense system element to others. As a consequence, a defense sensor may have information available on a target that is better than (or different from) that which it obtains directly by its own measurements; this information may include target ID. The defense elements must use the combination of internal and external information to decide on subsequent actions.

There are several important cases where use of external ID information may significantly improve TAD performance. One of these is when one defense sensor detects the launch or take-off of an A/C or CM providing ID by virtue of country of origin. If the target remains in track by at least one sensor at all times, its ID can be passed along. A second case is where a high quality sensor which can do non-cooperative ID but cannot engage the target passes its ID information to a lower quality sensor which can engage the target.

This report presents a parametric model of how well the combat ID function can be performed in a netted TAD system. It does not assess the performance of particular ID techniques but rather assumes parametric values for this performance in terms of leakage (mistaking an enemy for a friend) and fratricide (mistaking a friend or neutral for an enemy) for an individual target. It uses statistical models to determine the probability of track handover from one sensor to another. Given the quality of different ID techniques and the probability of track handovers, it is possible to determine the overall system performance in terms of total leakage and fratricide for a given scenario of attackers and defenders.

The overall CID model is a composite of relatively simple models for each of the elements of the problem including IFF effectiveness, target signature ID, track origin ID, sensor coverage, track handover probability, and mixture of attacking and friendly CMs and A/C. Sample results are presented but the emphasis is on determining scaling laws and rules of thumb relating model inputs to model outputs.

1. INTRODUCTION

An integrated Theater Air Defense (TAD) system must handle a variety of targets including Theater Ballistic Missiles (TBMs), Cruise Missiles (CMs), and manned aircraft (A/C). It must destroy enemy targets without attacking friendly and neutral targets especially manned A/C. The process of deciding which targets should be attacked is called Combat Identification (CID), which includes cooperative Identification Friend or Foe (IFF) as a subcase.

Recently, there has been considerable interest in netted TAD systems in which information on enemy targets and defense actions are passed from one defense system element to others. As a consequence, a defense sensor may have information available on a target that is better than (or different from) that which it obtains directly by its own measurements; this information may include target ID. The defense elements must use the combination of internal and external information to decide on subsequent actions. The work described here was started as part of the Theater Defense Netting Study (TDNS) sponsored by the Ballistic Missile Defense Office (BMDO) and supported by many organizations.

There are several important cases where use of external ID information may significantly improve TAD performance. One of these is when one defense sensor detects the launch or takeoff of an A/C or CM providing ID by virtue of country-of-origin. If the target remains in track by at least one sensor at all times, its ID can be passed along. A second case is where a high-quality sensor that can provide noncooperative ID but cannot engage the target passes its ID information to a lower-quality sensor that can engage the target.

This report presents a parametric model of how well the combat ID function can be performed in a netted TAD system. It does not assess the performance of particular ID techniques but rather assumes parametric values for this performance in terms of leakage (mistaking an enemy for a friend) and fratricide (mistaking a friend or neutral for an enemy) for an individual target. It uses statistical models to determine the probability of track hand over from one sensor to another. Given the quality of different ID techniques and the probability of track hand overs, it is possible to determine the overall system performance in terms of total leakage and fratricide for a given scenario of attackers and defenders.

The overall CID model is a composite of relatively simple models for each of the elements of the problem including IFF effectiveness, target signature ID, track origin ID, sensor coverage, track hand over probability, and mixture of attacking and friendly CMs and A/C. Sample results are presented but the emphasis is on determining scaling laws and rules of thumb relating model inputs to model outputs.

The next section describes the CID process and the overall structure of the CID model used. Subsequent sections describe the individual elements of the CID model including the individual sensor performance, the defense coverage and the hand over performance. Many of these elements of the overall model also can be used individually for assessing aspects of TAD other than CID. After describing the model and showing examples of its use, sample results will be presented for scenarios taken from some TDNS cases. A final section will summarize the results and discuss some general insights into the CID problem and suggestions for refinements to the model.

2. COMBAT ID IN A NETTED TAD SYSTEM

Any TAD system must operate in an environment containing aircraft, CMs, and TBMs, that are friendly, neutral or hostile. The objective of the defense is to destroy all enemy targets without killing any that are friendly or neutral, particularly manned A/C. Figure 1 illustrates the major considerations in the combat ID problem. Ideally, the defense must correctly identify all nine classes of targets shown in the matrix. In practice, some of the identifications, particularly of the TBMs, are relatively easy. Furthermore, some mistaken identifications, such as confusing friends with neutrals, will not degrade defense performance. The critical fratricide concerns are mistaking friendly or neutral manned A/C for enemy A/C or CMs. The critical leakage concerns are improperly identifying enemy CMs or A/C. The major techniques for combat ID are active IFF, signatures such as wideband pulse shapes, and track origin resulting from birth-to-death tracking. The potential pay off for netting in combat ID is the ability to pass ID information from a defense asset that can identify but not intercept to an asset that can intercept but not identify.

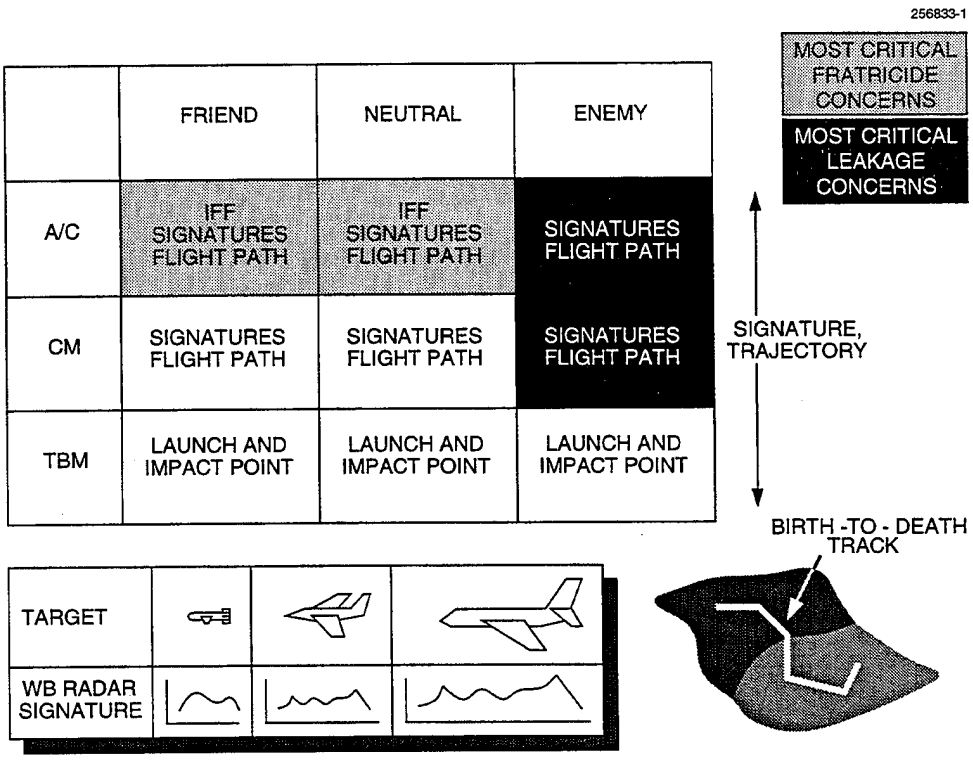


Figure 1. Combat ID techniques.

The possible errors in Figure 1 and their consequences are shown in Figure 2. (Some of these errors are extremely unlikely - that will be discussed below). The diagonal elements correspond to making the correct decision. Cross-hatched boxes correspond to confusing one type of friendly or neutral target for another. Strictly speaking these are errors but there are no significant consequences. If one type of enemy target is mistaken for another, the defense may plan a suboptimum engagement or even fire a less than optimum interceptor but this will not result in fratricide and may only increase the leakage slightly. Much more serious consequences result if an enemy is mistaken for a friend or neutral and not engaged. This contributes directly to leakage. There are two classes of cases where a friend or neutral is mistaken for an enemy and intercepted. If a friendly CM or TBM is shot down, it is wasteful of resources but not as serious as shooting down a manned A/C, either friendly or neutral by mistake. It is this human fratricide that must be minimized and that sets performance constraints on all combat ID functions. The next matrix, Figure 3, considers the ability of the defense to distinguish between the target combinations indicated. This will determine the likelihood of the errors indicated. Each box of the matrix is divided into four subboxes according to the ID technique applied. The techniques are graded according to their estimated ability to separate the two classes. The measure of performance, the k-factor, will be discussed in Section 4 below. Active IFF is likely to provide the most confident ID but is available only for friends and (possibly) neutrals. If all friendly and neutral targets could be counted on to give an IFF signal, this could form the sole basis for CID. However, some fraction of friendly targets will not give an IFF signal due to equipment failure, a desire to minimize observability, or effects resulting from traffic density or propagation. It is also possible that an enemy would try to spoof or degrade the cooperative IFF system. If IFF errors are larger than the acceptable fratricide level, the defense must rely partly on noncooperative ID techniques.

If available, birth-to-death track can provide confident country of origin information. To be effective, it requires detection of launch and continuous track to the time of intercept. Degraded performance will result from any gaps in coverage or from crossing targets that could yield missed associations. Other noncooperative techniques make use of different observables of the target to indicate what type of vehicle it is and what its mission might be. These observables include wideband measurements that can distinguish small targets such as CMs from medium sized targets such as fighter A/C and large targets such as transport A/C. Other observables may recognize specific characteristics of particular targets such as F-4s or F-15s. However, none of these techniques can distinguish a friendly F-4 from an enemy F-4. Trajectory observables can give different information on target altitude, speed, and heading that may give some indication as to its mission. However, interpretation of the information may be ambiguous, resulting in partial confusion of friends and enemies. As indicated in Figure 3, there are a variety of techniques that may distinguish between A/C and CMs with reasonable confidence. However, the performance of these techniques will likely be much worse for distinguishing friendly A/C from enemy A/C. A simplified version of Figure 3 is shown in Figure 4 where only the most important cases from Figure 2 are shown.

It must be remembered that CID is an extremely complex and important problem that is solved by a combination of operating rules and technical systems. In the models described here, both approaches are addressed and modeled to the extent practicable.

256833-2

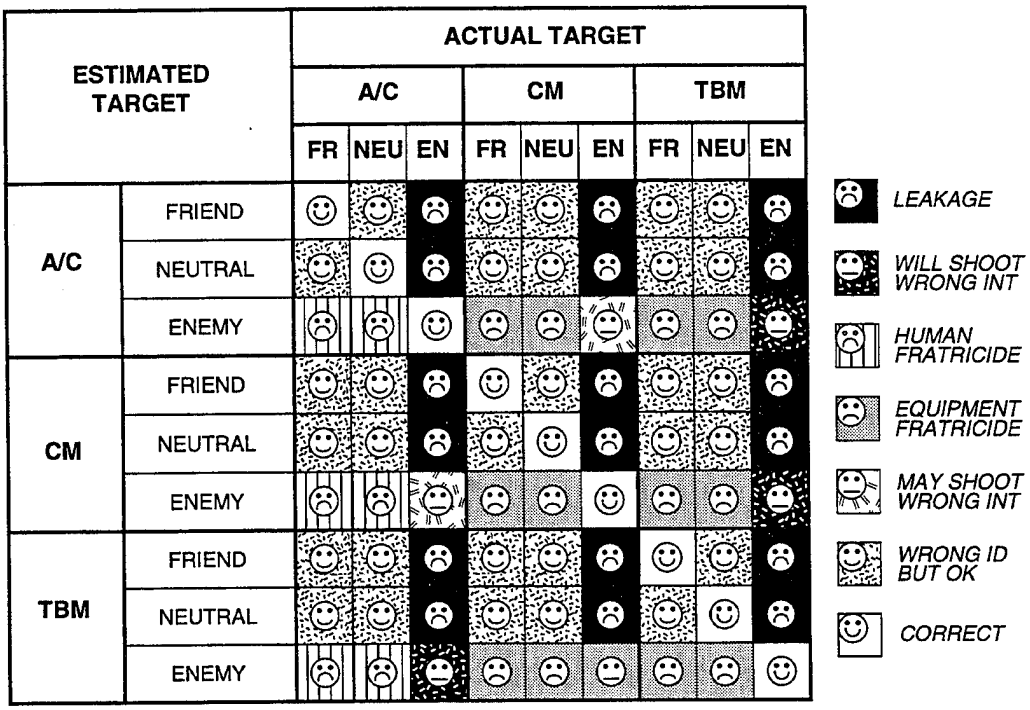


Figure 2. Combat ID error matrix.

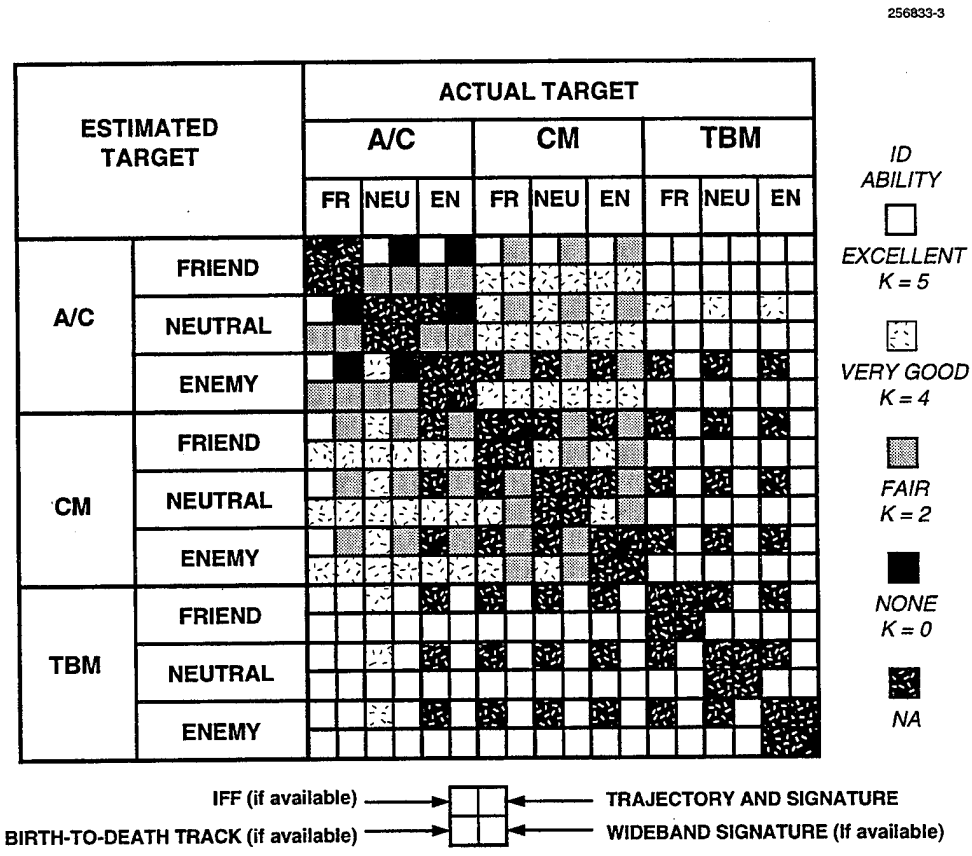


Figure 3. Combat ID error matrix.

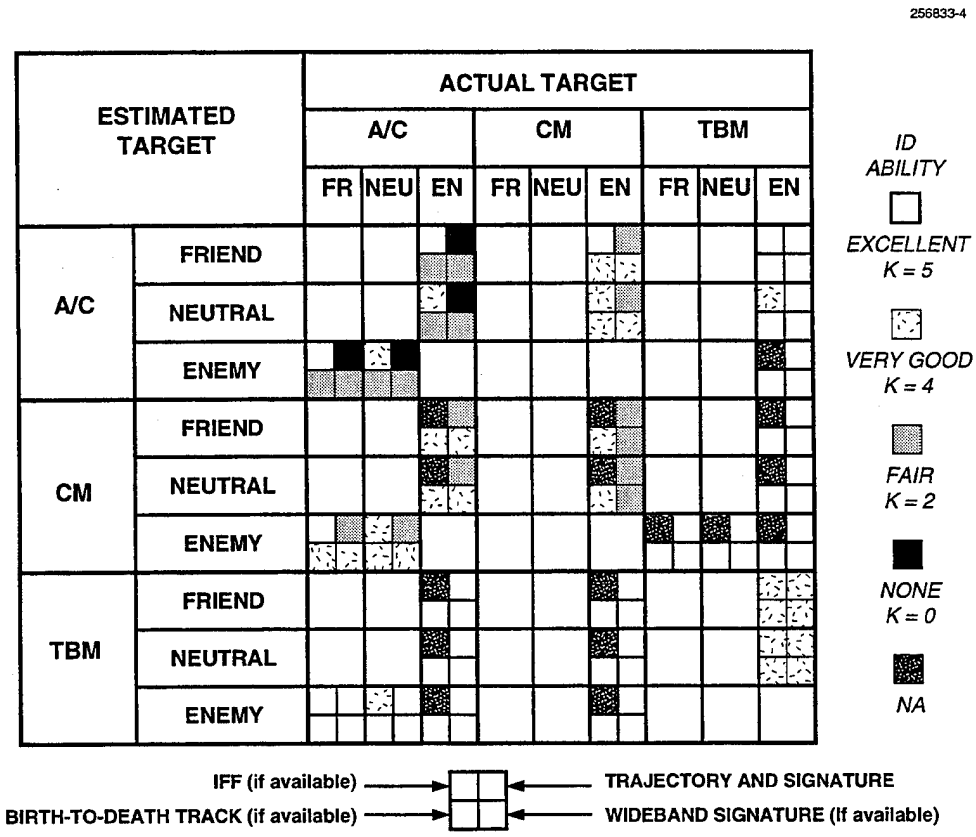


Figure 4. Combat ID error matrix.

3. MODELING OF COMBAT ID

The basic approach to modeling combat ID in a TAD system is shown schematically in Figure 5. The input consists of a mixture of friendly, neutral, and enemy A/C, CMs, and TBMs. The defense system then processes all these targets objectively, using the same rules of engagement and measurements for friendly, neutral and enemy targets. On the basis of its rules and measurements, the defense decides which objects to intercept and which to let go. The measures of effectiveness of the defense are the errors it makes: friendly kills (fratricide) and enemy leakers. By changing decision thresholds and operating rules it is possible to trade off fratricide and leakage. For example, requiring positive hostile ID will decrease fratricide at the expense of increasing leakage. Similarly, requiring positive friendly ID will decrease leakage but increase fratricide. Both errors must be calculated to evaluate CID performance.

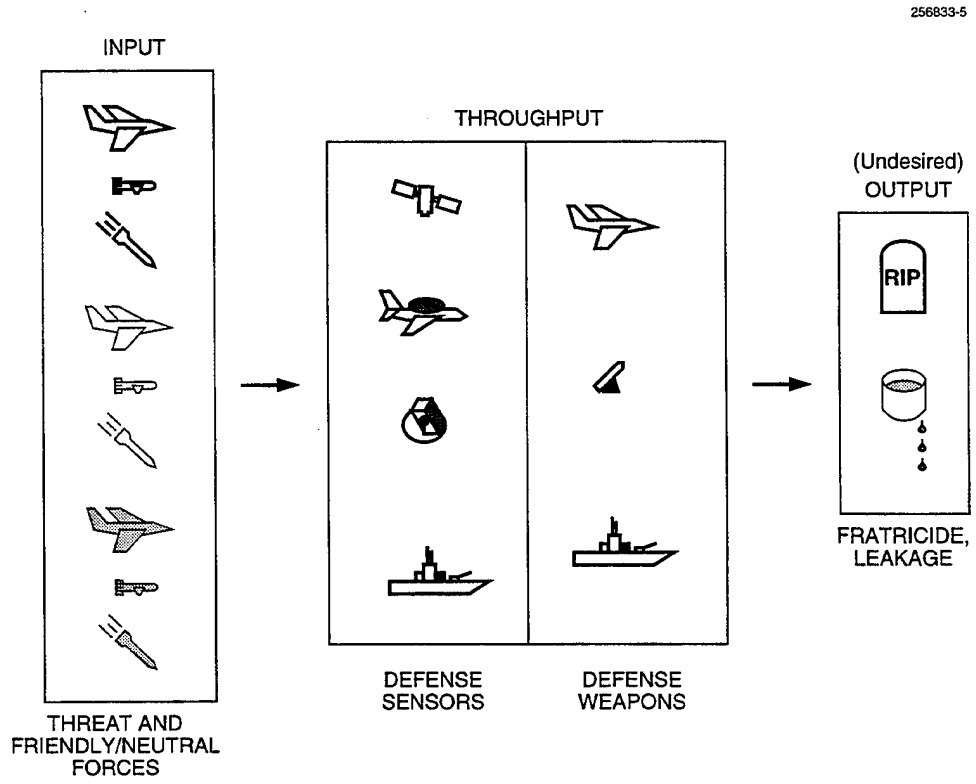


Figure 5. Combat ID modeling.

To get a feeling for the major parts of a combat ID model for netted TAD systems, a simplified ID decision process was postulated in Figure 6. The guiding principles for selecting this model were: (1) to rely on local decisions if possible and (2) to rely on more confident measurements if possible. In Figure 6, the

defense uses local measurements to classify each target as hostile, friendly or uncertain. In the first case (hostile), it will shoot if it can and put its ID information onto the net. In the second case (friendly), it will not shoot and will put its ID information on the net. In the third case (uncertain), it will look onto the net to see if there is confident ID information on the target and then act on this external information.

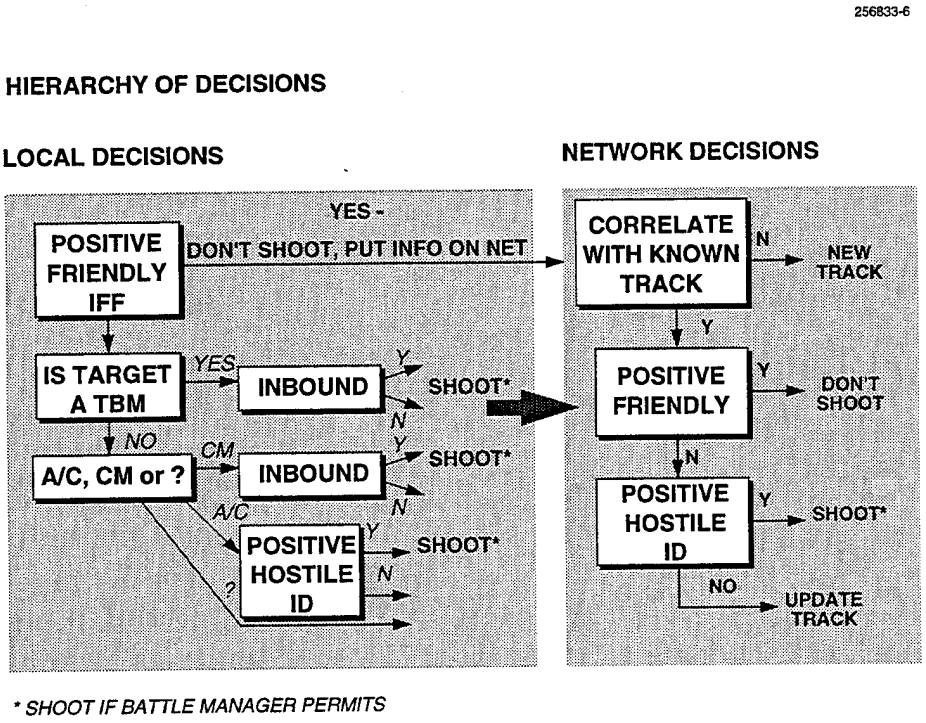


Figure 6. Combat ID decision process.

The local decision process uses confident ID techniques first, and then less confident techniques, only if necessary. The most confident technique will be cooperative IFF, which is available only for a fraction of friendly and neutral targets. The next most confident measurements are those distinguishing ballistic targets from air-breathers. Ballistic targets can be confidently identified as to friendly or hostile on the basis of launch and impact point. Air-breathing targets can be classified into A/C and CMs using a variety of techniques including signatures and trajectories. The defense is more willing to shoot at CMs than at A/C and might use target heading to indicate threat for CMs. For A/C or uncertain targets, the defense will probably require a positive hostile ID in order to shoot. In most cases, a local defense battery will not be able to make this positive hostile ID and will have to rely on network information or just keep the target as uncertain.

There are two important submodels that are needed to assess the ID performance of a netted system. The first submodel determines how well particular measurements can separate friendlies from hostiles. This

is analogous to the discrimination model commonly used in Ballistic Missile Defense (BMD) to separate warheads from decoys. It is described in the next section. The second submodel determines how well targets can be handed over from one sensor to another. This is a statistical model that was developed for the TDNS and can be used to determine the likelihood of CMs avoiding sensor coverage and the likelihood of hand over from one sensor to another without coverage gaps. This submodel is described in Section 5.

4. IDENTIFICATION MODEL

The identification function is a set of measurements and logic that operates on all targets and tries to put them into the proper classes; in particular, friendly and hostile. The function is subject to two major types of errors: leakage and fratricide. The likelihood of these errors is a measure of the identification performance. The ID model used in this report is a statistical one that has been used successfully for BMD discrimination and kill assessment. It has the advantages of great simplicity together with reasonable fidelity.

The ID measurements available on a target can be compressed into a one-dimensional measure of the estimated "friendliness" or "hostility" of the target. There will be a statistical spread in this value due to measurement uncertainty, target and geometry variability, and uncertainty in modeling the connection between measurements and "ability to threaten." In the simple model, the combined ID observable is assumed to have a Gaussian distribution for both friends and foes. The means of the distributions are separated by a factor, k, times the standard deviation of the distribution (assumed equal for both target classes). This is shown in Figure 7, where a decision threshold separates those targets called friends from those called foes. For the case shown, k = 2; there is significant leakage (mistaking an enemy for a friend) and fratricide (mistaking a friend for an enemy). By changing the threshold location, the defense can decrease fratricide at the expense of increasing leakage or vice versa. The resulting errors will lie on an "operating curve" as shown on the right side of Figure 7. If leakage and fratricide probabilities are graphed on probability scales, the operating curve is a straight line with 45 deg slope. For k = 0 (no separation of targets), the leakage and fratricide probabilities add up to 1. As k increases beyond 3 or 4, it is possible to have very low fratricide without excessive leakage. In analyzing ID performance, the k-factor determines which curve in Figure 7 should be used. The defense then selects a threshold to operate at the point on the curve that best balances leakage and fratricide to achieve its overall objectives. This balance between leakage and fratricide will depend on the environment and other elements of the CID system. For example, for an uncertain target approaching an aircraft carrier, the defense might set a threshold to minimize leakage whereas for an uncertain target approaching a civilian airport, the goal might be to minimize fratricide. If an "acceptable" level of overall fratricide is 0.001 (1 per 1000 sorties) and 99% of friendly A/C have working IFF systems, then the threshold for noncooperative ID could be set to yield a fratricide of 10%. However, if only 50% of friendly A/C have working IFF systems, then the noncooperative ID must have a fratricide of 0.2% or less.

Comparison of Figure 3 and Figure 7 indicates the level of performance expected of the different ID techniques considered. In the results sections of this report, sensitivity of overall system performance to the k-factors of individual techniques will be examined. It is important to keep in mind that the results presented here are parametric; they indicate what happens if the ID performance is at a given level. They do not address the extremely important problem of determining the actual performance achievable by the various ID techniques. Furthermore the primary focus of this work is to investigate how netting of sensors can contribute to the ID process.

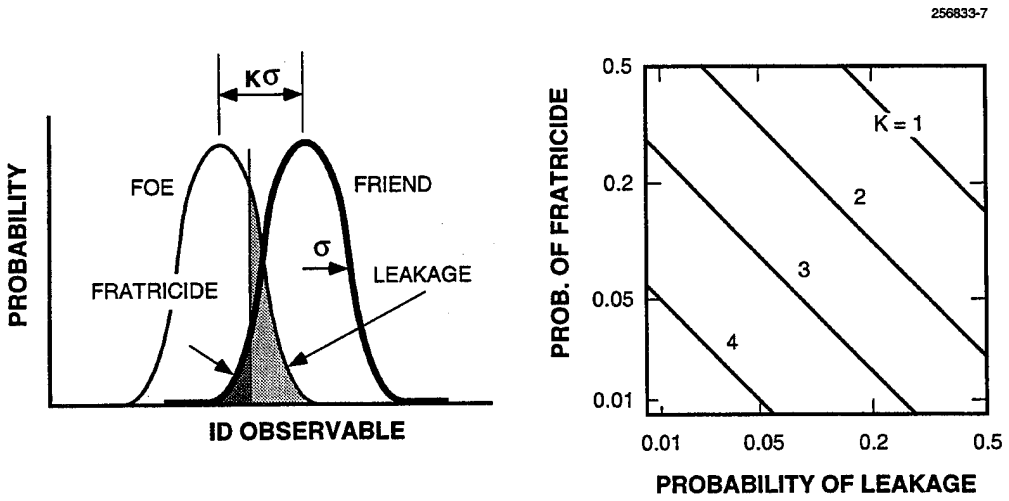


Figure 7. Combat ID performance model.

It is important to be aware of the limitations of the k-factor model described here. The assumptions of Gaussian distributions and equal standard deviations make it possible to characterize ID performance using a single parameter. In actuality, target observable distributions will be more complicated, probably including a variety of different objects with different means and standard deviations in both the friend and foe classes. This can be accommodated in the ID model by using composite operating curves rather than the simple linear models in Figure 7. This increases the complexity of the model but does not affect the basic principle that the defense must operate with a balance between leakage and fratricide. A more serious limitation of the model (or any model) is that it is extremely difficult to make a model that will be correct in the tails of the distribution because it must be concerned with events that occur less than 0.1% of the time. If fratricide is to be kept to these very low values, it is necessary to correctly model these very rare events. This requires examination of all the combinations of circumstances that could result in ID observables in the tails of the distributions.

5. COVERAGE MODEL

A statistical parametric coverage model was used to analyze combat ID performance in a netted sensor environment. By flying a large number of CMs through an array of defense batteries, it is possible to determine the distribution of overlapping coverage that is needed for passing on ID information. The major characteristics of the coverage model are shown in Figure 8. The upper-left figure shows some of the problems that can arise when there are gaps in coverage. A target passing through sensor 1 coverage can be identified (to the capability of the sensor) and this information passed on to sensor 2. If the target does not maneuver and no other targets are in the vicinity, the target will show up in sensor 2 coverage at the appointed time and sensor 2 can assume it is the previously identified target. However, if the target maneuvers in the coverage gap or if another target appears where this target was expected, then the defense can make serious ID errors. For simplicity of analysis, it is assumed that target ID cannot be carried across a coverage gap.

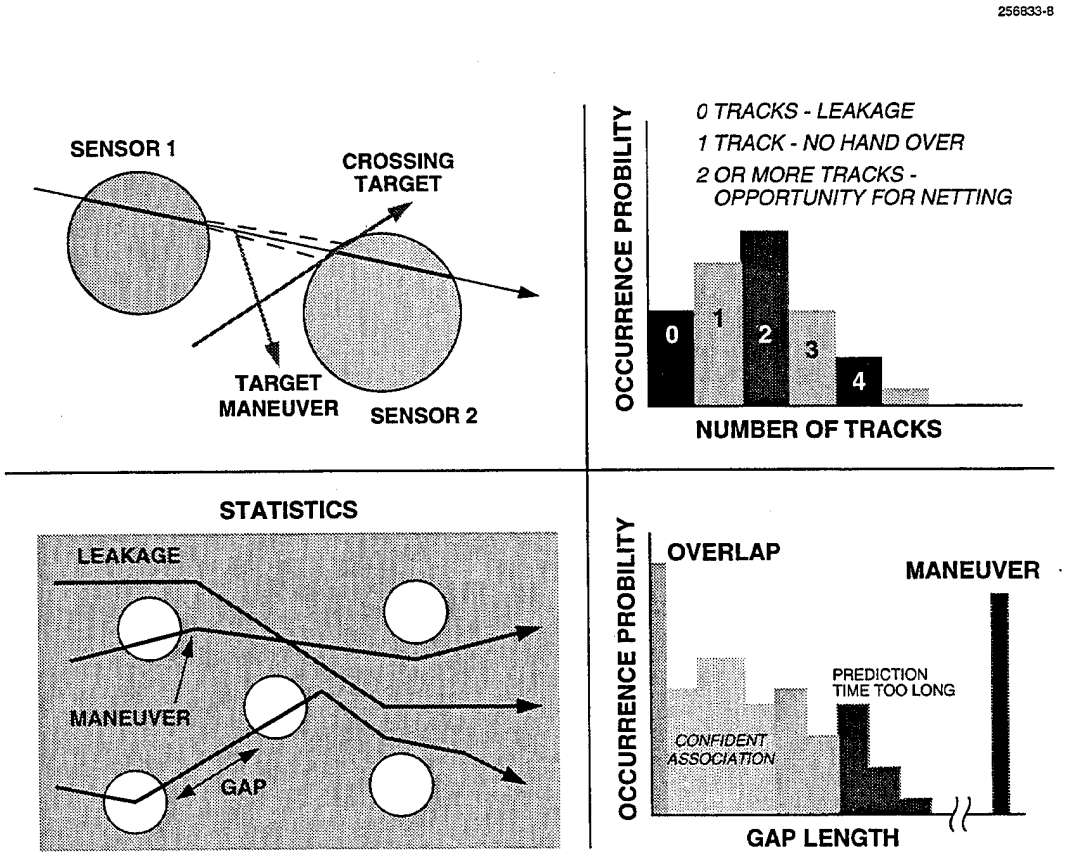


Figure 8. Track correlation analysis.

To get a feeling for the likelihood of multiple sensor coverage and gaps in coverage, the model shown in the lower left of Figure 8 was used. A defended area was assumed and a parametric number of defense batteries with parametric coverage radii were deployed at random. A large number of CM trajectories were flown randomly through this area and various statistics compiled. The CMs flew without knowledge of the defense deployment and the defense batteries were deployed without knowledge of the CM trajectories. Each CM flew a series of straight-line segments with randomly occurring maneuvers in random directions. The average distance between maneuvers and the average change in heading can be varied. As seen in the figure, some CMs will fly through the coverage and never be detected. Others will just fly through one coverage circle while others will fly through multiple coverages. Statistics are complied on the fraction of CMs detected by 0, 1, 2, etc. sites; a sample histogram is shown in the upper-right of the figure. Finally, for those CMs passing through multiple coverages, statistics are compiled on the distribution of coverage gaps as indicated in the lower-right figure. A certain fraction of cases will have no gap that represents an overlap in coverage. In these cases, the ID from sensor 1 can be passed to sensor 2. At the other extreme, a fraction of CMs will maneuver in the coverage gap and will be lost from an ID point-of-view (also from a cueing or interceptor precommit point-of-view). Depending on the gap length, the defense may or may not be able to correctly associate the target tracks handed over from sensor 1 to sensor 2. Again, in the current analysis, any gap was considered too much to pass ID information with confidence.

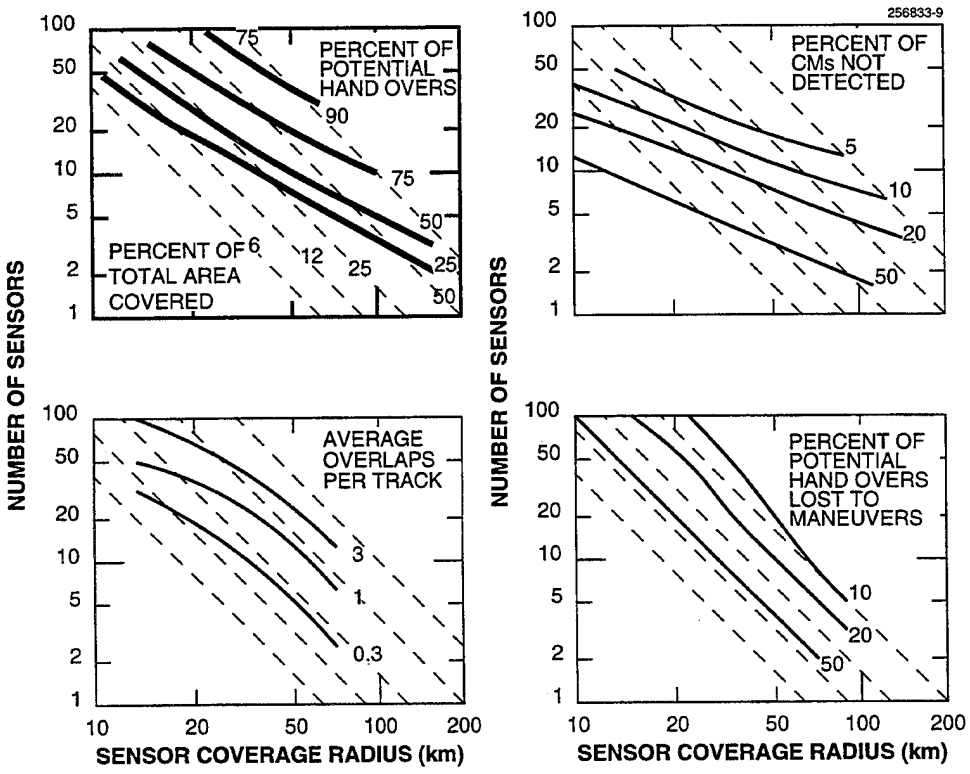


Figure 9. Track correction trade-offs.

By varying the number of defense sites and their coverage, it is possible to see how track correlation and ID hand over performance depends on these variables. Figure 9 is a sample of the results obtained with this model corresponding to CM maneuvers of about 20 deg occuring on average every 100 km of flight path. Each frame shows how a given variable depends on the number of sensors deployed and the coverage radius of each sensor. The straight lines at about 45 deg correspond to given percentages of the total area that is covered. (It approaches 100% asymptotically because the sensors are deployed randomly.) The upper right curves show the fraction of CMs that are never detected. A sample result for a 300 X 600 km theater (Korea sized) with 20 horizon limited sensors having 40-km coverage radius results in about 6% of the CMs never being detected. The lower-right curves show the percent of potential hand overs (CM path goes through coverage of 2 neighboring sensors) in which the CM maneuvers in the gap between sensors. For the sample case, about 20% of the CMs will maneuver in this gap. This is strongly dependent on the CM maneuver frequency. This level of track loss due to coverage gaps is not acceptable for combat ID but may still be useful for sensor cueing. Combining these results gives the curves in the upper left for the probability of successful hand over from one sensor to another. It is seen that, for constant area coverage, hand over is more likely for many small coverage regions than for a few large coverage regions. This is because the required coverage is more like a barrier than full area coverage. The final set of curves in the lower left is of most importance for combat ID. They show the expected number of coverage overlaps per CM track. Because the requirement for fratricide is very low, confident track association for passing ID information will require track overlap. This overlap probability (or the absence of track gaps) will be an input parameter to the netted combat ID model described in the next section.

The interceptor coverage is determined by the sensor coverage and the relative interceptor and target speeds. Some of these effects are shown in Figure 10 for both subsonic and supersonic CMs. The outer circle is the sensor detection range (which could differ for autonomous or cued operation). After target detection and a certain time for decision making, an interceptor is launched to reach the intercept point at the same time the target does. For subsonic CMs, the interceptor flies much faster than the target and the initial intercept point is quite close to the detection point. For supersonic CMs, the target and interceptor speeds are comparable and the intercept occurs much closer to the sensor. In either case, if the intercept is successful, the target is killed. If the intercept is not successful, the sensor will observe this fact and, after a short decision time, will launch another interceptor. This process is repeated until either the target is killed or it passes out of the defense coverage. The right-hand side of Figure 10 shows how many shot opportunities the defense gets for each type of CM as a function of the point of closest approach. The defense can fail to kill in a number of ways. If the point of closest approach is too far from the defense, it is not possible to make any intercepts. This is more likely for supersonic CMs. The defense can also fail if all the interceptors shot at a target fail to kill. For any given interceptor probability of kill, P_k, the probability that all N shots will fail is $(1-P_k)^N$. These two effects can be combined statistically to yield either an effective kill probability over the sensor coverage or an effective coverage through which kill is certain. The former approach is used below. It should be noted that the effective kill probability can be larger than the single-shot kill probability because of the efficiency of shoot-look-shoot operation.

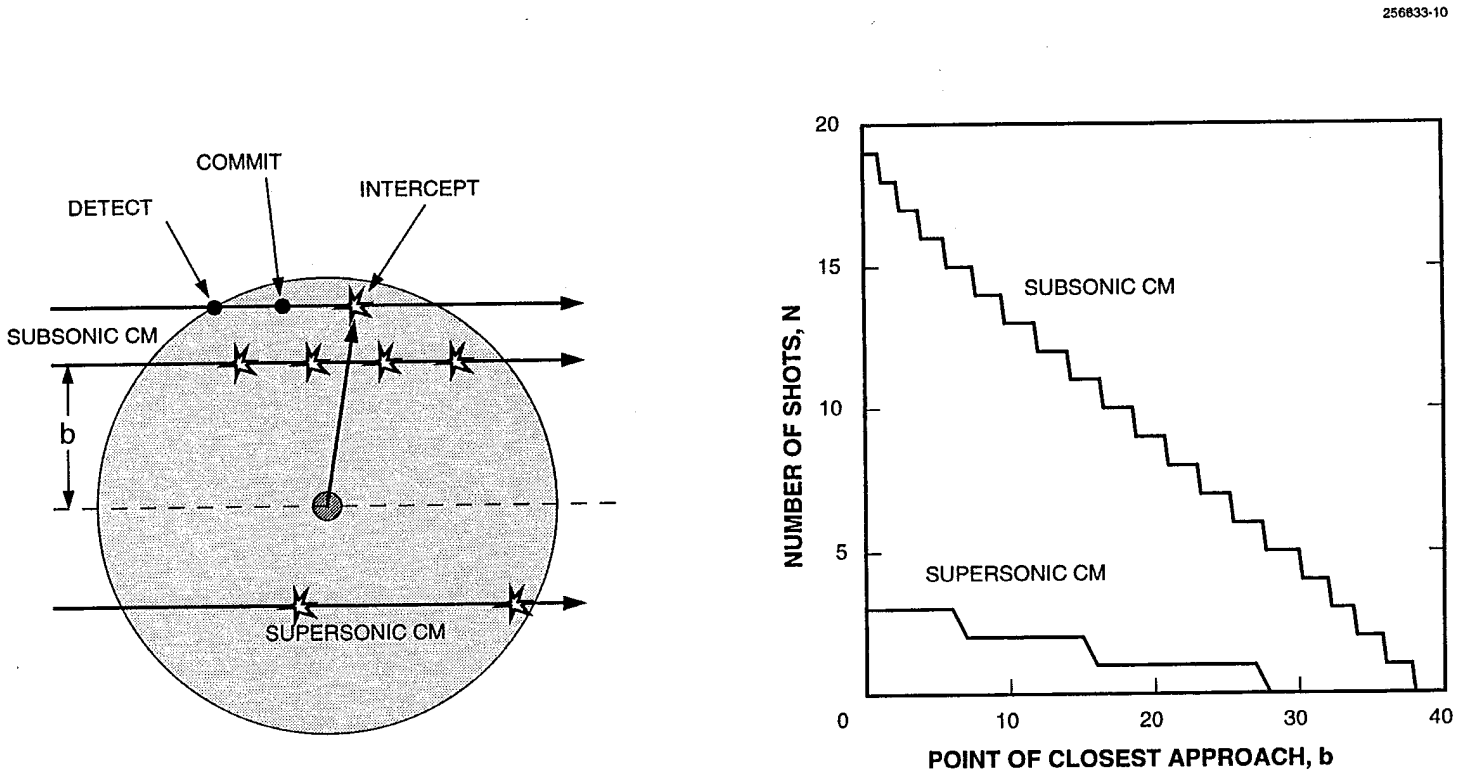


Figure 10. Coverage model.

6. NETTED CID MODEL

Figure 6 showed how the defense could use both local and network ID decisions in netted operation. This section describes how the netting processes are modeled including effects of coverage and track association. It is convenient to classify all targets into a small number of states depending on what their track and ID history have been Figure 11 is a simplified state model with five major variables: whether or not target take-off was detected, whether or not the target is in track, whether or not the target has been identified, whether or not the target has been shot at, and whether or not the target has been killed. The possible states for a target are shown in Figure 11. If the target take-off is detected it goes into state "B T ID s k" where upper-case letters correspond to a "yes" and lower case letters to a "no". B refers to birth detected, T to target in track, ID to target identified (perhaps incorrectly), S to being shot at and K to being killed. If target launch is not detected, the target is in state "b t id s k". A target stays in its state until something happens. Things that can happen include: coming within sensor coverage, going out of sensor coverage, coming within ID sensor coverage, coming within interceptor coverage, getting shot at, getting killed. Note that once a target leaves state "B T ID s k" because of a coverage gap, it can never return. ID is done in one of three ways. If friendly IFF is working, it always returns a correct ID. If the target stays in birth-to-death track until an interceptor can reach it, the ID is based on the k-factor for birth-to-death track. Otherwise, the ID is based on the best signature/trajectory ID of any sensor in the current track. The probabilities for track gaps and sensor and interceptor coverage are based on the statistical models described above.

Starting at the top of Figure 11, a certain fraction of hostile targets will be observed taking off. Hopefully, almost all friendly takeoffs will be detected. When a target is in radar coverage, it has a certain probability of being correctly identified, of being engaged by an interceptor, and of being killed. If it leaves one sensor's coverage without being killed, it has a certain probability of reaching its target (leaking) prior to being detected again. It has a different probability of entering the coverage of another sensor immediately (no gap). By varying the decision thresholds for the different ID functions, it is possible to constrain the fratricide and use leakage as the performance measure. A simple spreadsheet permits the user to look at the time evolution of target states and to vary the ID decision thresholds to minimize leakage for a given set of parameters. To illustrate how this process works, Figure 12 shows how friendly A/C and enemy CMs will progress through the ID process. The parameter values are nominal ones; other cases are considered in the next section.

Figure 12 shows the fraction of targets in each state of Figure 11 as a function of time. The unit of time is the interceptor flyout time and, on average, the targets spend about 4 time units within radar coverage. At each time unit, some targets will come into coverage, some will go out of coverage, some will be identified (correctly or incorrectly), some will be shot at, some will be killed and others will reach their intended targets (leakage for enemies, safety for friends). The curves in Figure 12 are for friendly A/C and enemy CMs. Different results would obtain for enemy A/C because the ID performance would be expected to be worse. The ID decision thresholds were set to yield an overall fratricide rate of 0.001. Because only a fraction of the friendlies have arrived safe at home in Figure 12, the actual number of fratricides is proportionately less than 0.001. For the friendlies, there is a gradual transition from birth-to-death track to non-birth-to-death track with a change in the k-factor for ID. However, the decision thresholds are changed accordingly to constrain the fratricide. A different behavior is seen for hostiles. Initially, a certain fraction of CMs are in birth-to-death track and these are rather quickly identified and killed. As time goes on, those

targets not in track are acquired, correctly identified, and killed. However, because the k-factor for nonbirth-to-death ID is lower, the rate of correct identification is less and the killing takes longer with more time for leakage to occur. The resulting leakage is the overall measure of performance.

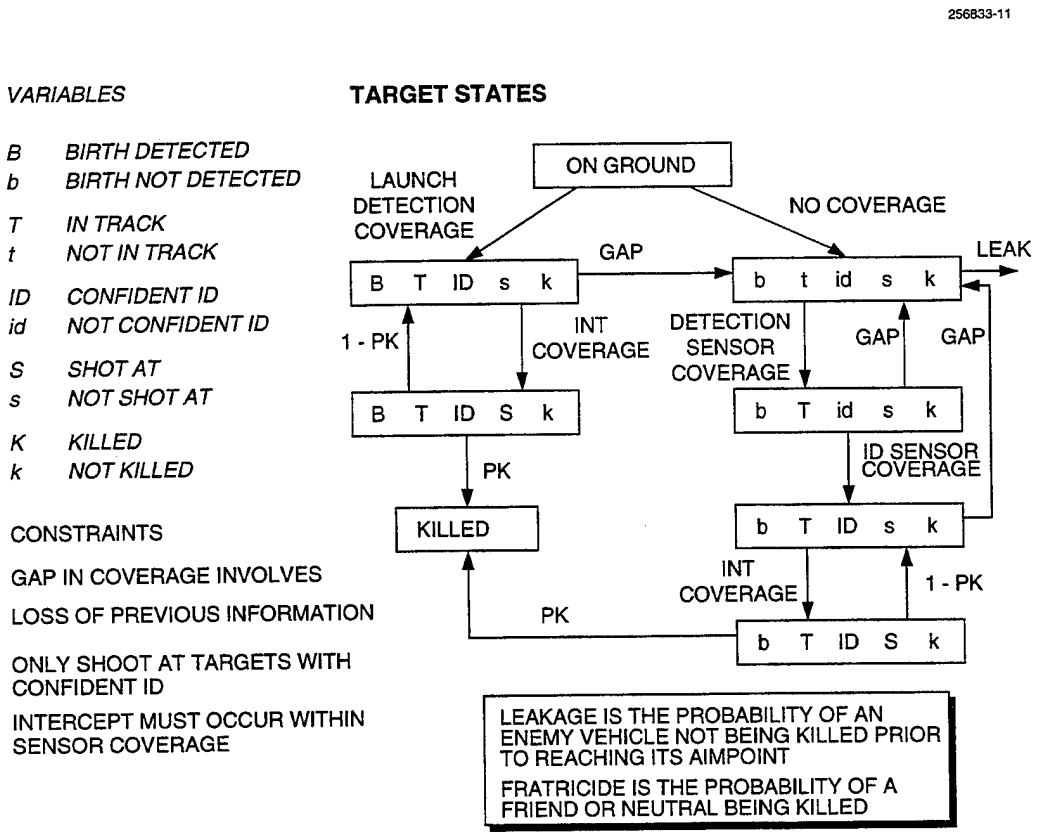


Figure 11. Simplified network combat ID model.

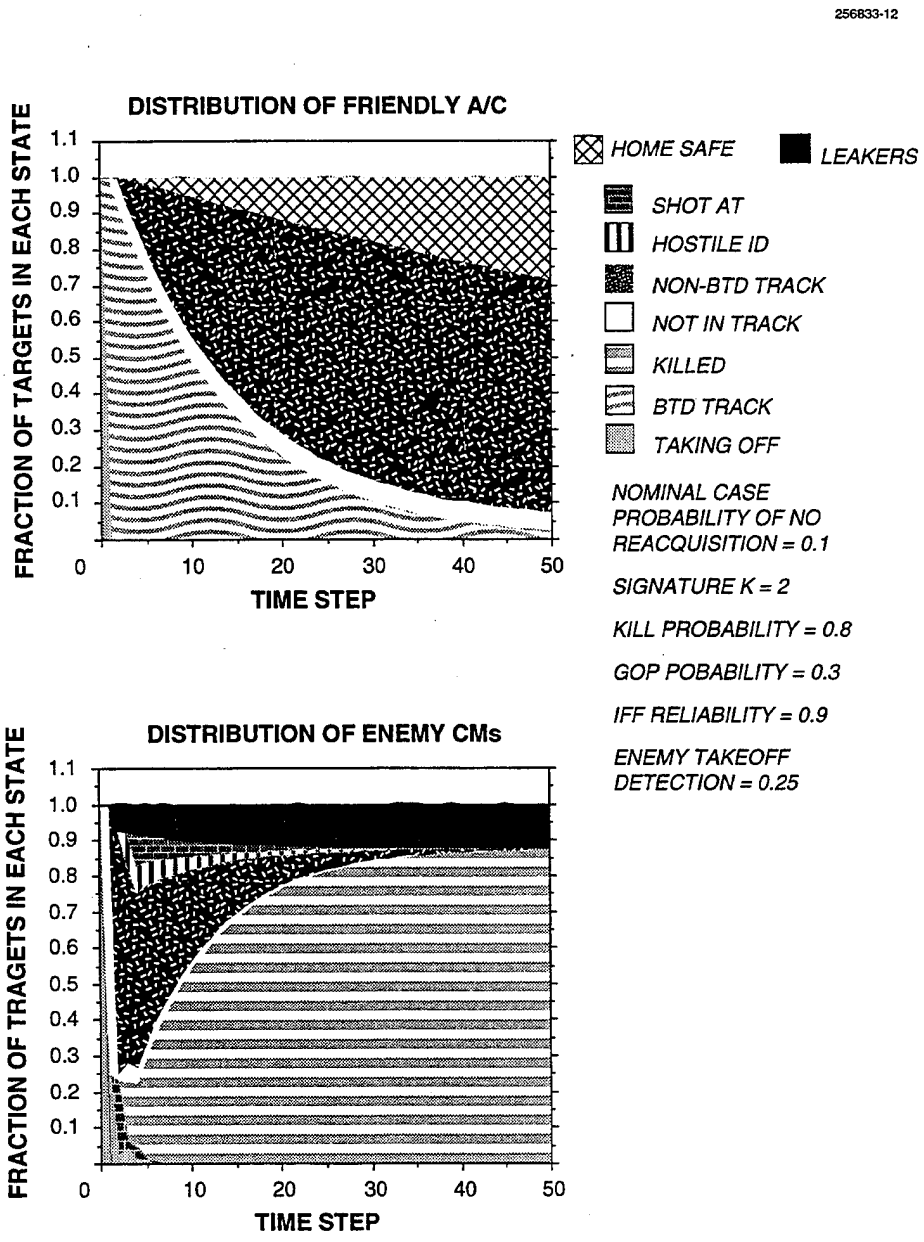


Figure 12. Evolution of target states.

7. SAMPLE RESULTS

The results presented here will fall into two categories: single defense site results using the model of Figure 6, and netted site results using the model of Figure 11. The single site results are shown first for a sensor with fairly good ID capability. Figure 13 repeats Figure 6 with arrows representing the fraction of friendly A/C and enemy CMs that take various paths through the logic. The thresholds have been set to achieve 0.1% fratricide locally. In reality, a friendly A/C might have to pass through a number of defense sites so the fratricide at each site should be even lower. For the simplified model used here, it is assumed that distinguishing A/C from CMs constitutes identification and can be done with a k-factor of 4. It is also assumed that 90% of the friendly A/C have working cooperative IFF so that the noncooperative ID function can have a fratricide of 1%, which, with a k = 4, gives a leakage of about 5% (see Figure 7). The boxes that decide whether a specific CM or A/C is friendly or hostile are assumed to be disabled so the overall leakage will be 5%. This level of leakage is probably tolerable but the reader must be cautioned that it cannot be brought down solely by providing another defense battery to pick up the leakers. If another battery is deployed, the friendly A/C must also fly through its coverage and the decision thresholds must be adjusted to reduce the fratricide accordingly -- this will increase the leakage at each battery but the defense will still be better off with multiple sites.

The situation is completely different if the ID capability of the defense sensor is only fair, k = 2. Figure 14 shows the results for this case. Here the resulting leakage increases to 65% if the overall fratricide is to be held to 0.1%.

To assess the effects of netting on the defense CID capability, it is necessary to use the model of Figure 11 and perform a series of calculations similar to those shown in Figure 12. A summary of the dependence of overall leakage on a variety of defense parameters is given in Figure 15 again for the case of friendly A/C and hostile CMs. Each point in each figure represents a selection of decision thresholds to minimize overall leakage for an overall fratricide rate of 0.001 (one per thousand sorties). For the nominal cases given by the circles, 25% of enemy take offs are observed with a k-factor of 4 for birth-to-death track ID. Furthermore, 90% of friendly A/C have working IFF and 30% of CMs will have a track gap prior to entering another sensor's coverage. For ID based on trajectory (but not birth-to-death track) and signature, the k-factor is 2. The two baseline cases considered have a track loss probability of 0.3 and 0.1, which is the probability that a CM out of track will never be reacquired. For the two baseline cases, the overall leakage is 35% (for 0.3 track loss probability) and 18% (for 0.1 track loss probability). By varying parameters one-at-a-time from the baseline values, the four performance curves are obtained. The leakage depends, roughly, linearly, on birth detection probability and gap probability (no overlap). The dependence on signature k-factor shows plateaus for $k<1$ and $k>3$ with greater variation in between. The dependence on IFF reliability is linear on a probability scale because the number of friendlies without IFF determines how the decision thresholds must be set to constrain the overall fratricide. It must be kept in mind that all the ID techniques are modeled parametrically in terms of their k-factors. Considerable further work would be required to determine the ID performance against real targets in real environments.

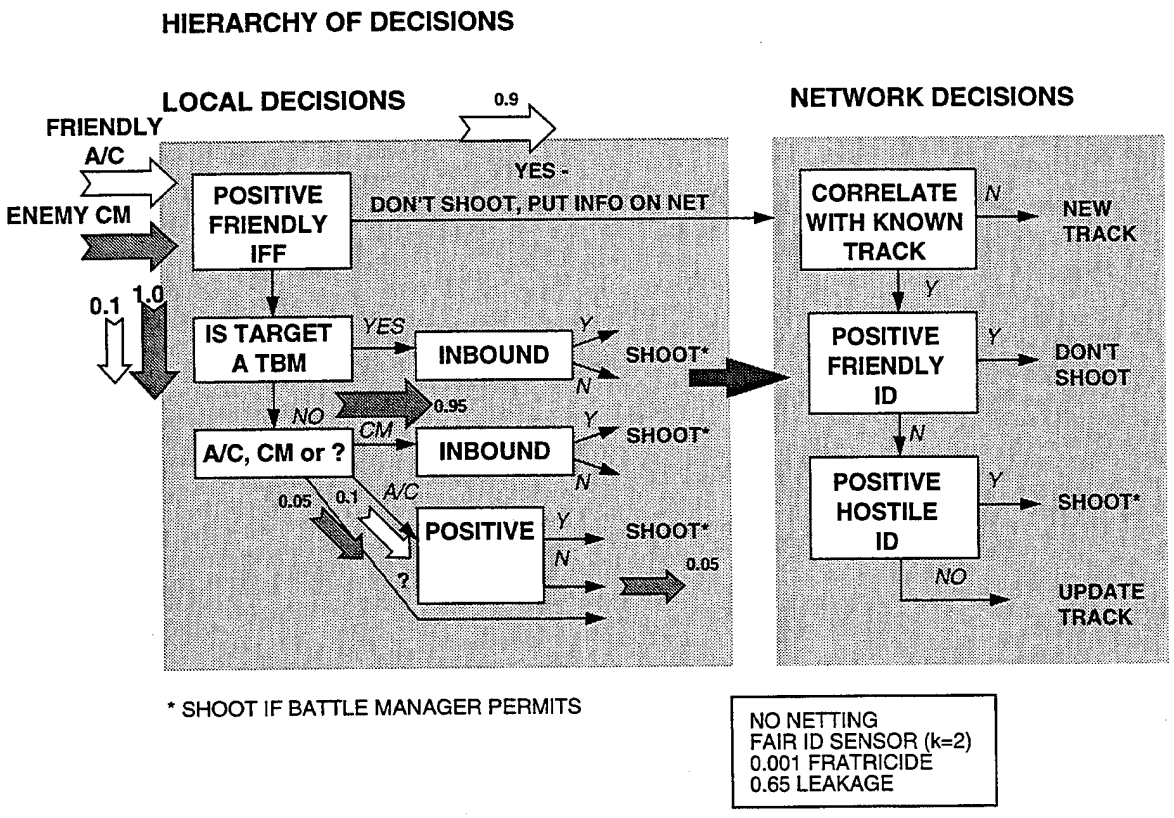


Figure 13. Combat ID decision process.

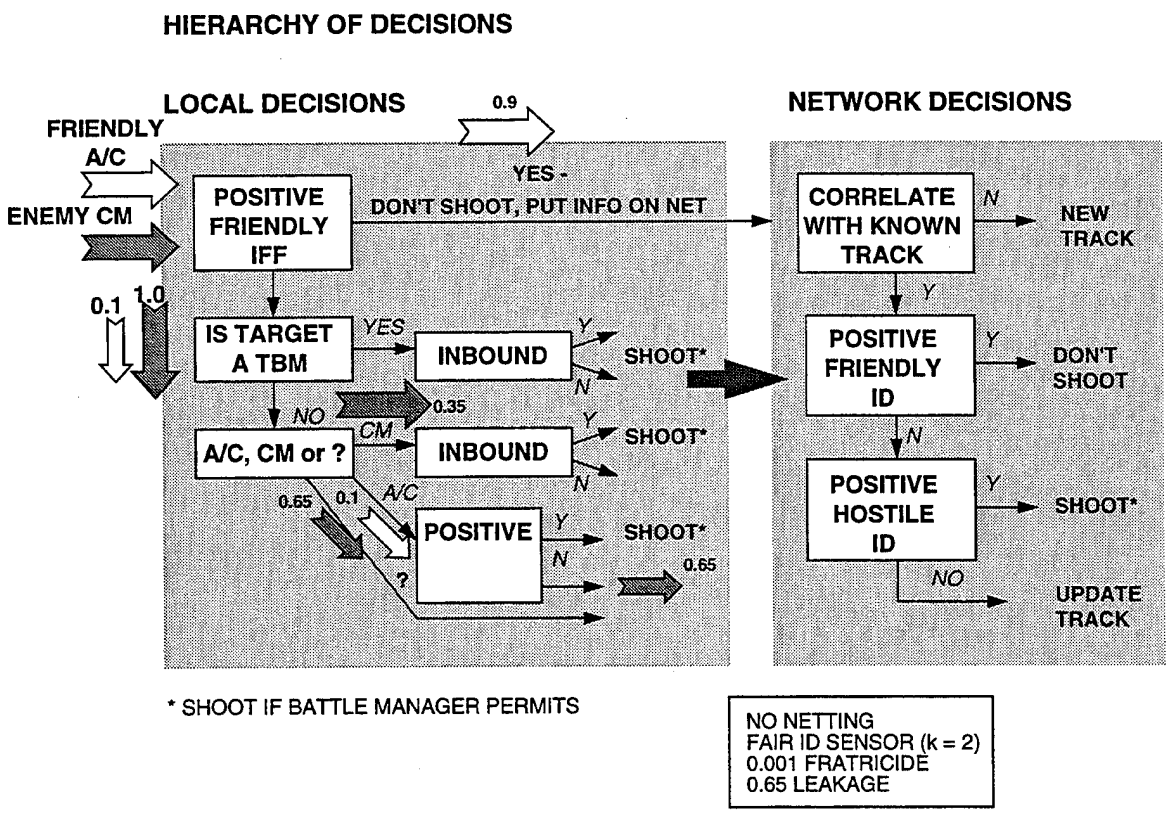


Figure 14. Combat ID decision process.

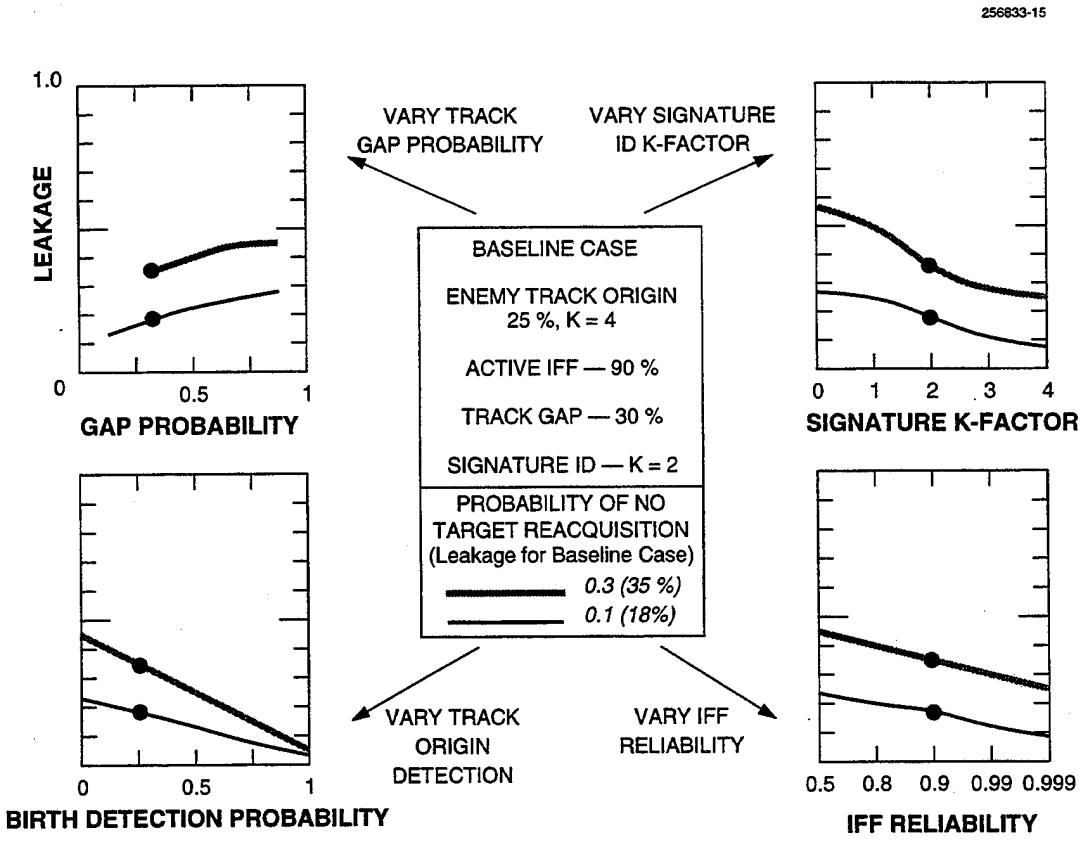


Figure 15. Sample netted combat ID results.

8. DISCUSSION AND FUTURE UPGRADES

The CID model described here is focused on the effects of netting on the overall ID function. The key features of the model include statistical modeling of the ID process at a given sensor and of the hand over from sensor to sensor. The interactions in the model permit determination of the trade-offs among better identification, greater coverage, and increased netting. The model is meant to be used together with other analysis techniques that can determine the actual performance of ID techniques in terms of achievable k-factors or actual leakage and fratricide probabilities.

In addition to incorporation of realistic data, the model itself can be improved in a number of ways. Currently, the model assumes the same coverage, handover and ID performance for all sensors (with the exception of birth-to-death ID performance). An important upgrade would be the inclusion of multiple types of sensors including airborne (larger coverage) vs surface based (smaller coverage) and good ID (signature or cooperative) vs fair ID (cooperative only). This upgrade would involve inclusion of many more states and additional transition probabilities. In extending the model, the user must strike a balance between faithfully modeling processes of interest and maintaining ease of use and understanding.

Another important future task is to compare results from this (or other) statistical models with results from deterministic or Monte Carlo simulation models. It is expected that comparison of different approaches to modeling an extremely complex problem would offer additional insights into critical issues and their interrelations.

REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 0704-0188

1. AGENCY USE ONLY (*Leave blank*)	2. REPORT DATE	3. REPORT TYPE AND DATES COVERED
	27 November 1995	Technical Report

4. TITLE AND SUBTITLE
A Combat Identification Model for
Netted Theater Air Defense Systems

5. FUNDING NUMBERS
C — F19628-95-C-0002
PR — 363
PE — 61101E,
62712E

6. AUTHOR(S)
Stephen D. Weiner and David P. Cebula

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)
Lincoln Laboratory, MIT
244 Wood Street
Lexington, MA 02173-9108

8. PERFORMING ORGANIZATION REPORT NUMBER
TR-1023

9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)
BMDO
7100 Defense Pentagon
Washington, DC 29301-7100

10. SPONSORING/MONITORING AGENCY REPORT NUMBER
ESC-TR-95-050

11. SUPPLEMENTARY NOTES
None

12a. DISTRIBUTION/AVAILABILITY STATEMENT
Approved for public release; distribution unlimited.

12b. DISTRIBUTION CODE

13. ABSTRACT (*Maximum 200 words*)

This report presents a parametric model of how well the combat ID function can be performed in a netted TAD system. It does not assess the performance of particular ID techniques but rather assumes parametric values for this performance in terms of leakage (mistaking an enemy for a friend) and fratricide (mistaking a friend or neutral for an enemy) for an individual target. It uses statistical models to determine the probability of track handover from one sensor to another. Given the quality of different ID techniques and the probability of track handovers, it is possible to determine the overall system performance in terms of total leakage and fratricide for a given scenario of attackers and defenders.

14. SUBJECT TERMS
air defense
identification
netting

15. NUMBER OF PAGES
38

16. PRICE CODE

17. SECURITY CLASSIFICATION OF REPORT	18. SECURITY CLASSIFICATION OF THIS PAGE	19. SECURITY CLASSIFICATION OF ABSTRACT	20. LIMITATION OF ABSTRACT
Unclassified	Unclassified	Unclassified	Same as Report