DISCUSSION OF CLASSICAL AND PUBLIC KEY CRYPTOGRAPHY

John E. Hershey
Peter M. McManamon
National Telecommunications and Information Administration
Institute for Telecommunication Sciences
Boulder, Colorado 80303

ABSTRACT

Classical and public key cryptography for communications privacy are discussed regarding their relative implementation complexity and overall applicability.

INTRODUCTION

The past few years have witnessed the development of a most fascinating discipline termed public key cryptography. Cryptography, the set of procedures for rendering messages unreadable except to those intended and those procedures for authenticating commands or "signing" messages to prevent spoofing, is an age-old pursuit. Developed over thousands of years, it entered the 20th century as an art form. Necessity, the mother of invention, accentuated the development and refinement of cryptographic methods and techniques. Following passage through two world wars into the present technological age, the art changed quickly to a science. Of premier importance in marking this milestone, the evolvement from art to science, was the attempt to quantify defensive cryptanalysis, i.e., the attempt to determine the strength of a given system under specific scenarios. Standards can help one structure cryptographic methods and responsibly select their parameters.

Before public key cryptography, it was necessary for two parties, who wished to exchange messages securely, to previously exchange secret quantities usually termed "keys" or "keying variables." These exchanges could not be made public and had to be effected through a secure medium such as by courier or other protected channel. Public cryptography may free us from this constraint and do so in an ingenious manner. The mechanism relies on the apparent asymmetric complexity of a set of operations and their inverses.

As might be expected, this mechanism has given rise to a different set of security concerns than those that beset "classical" cryptography. The first concern is, obviously, the evaluation of the algorithm's strength, i.e., "shortcuts" to reduce complexity of

implementation of the inverse operations. Second, because correspondents are not in possession of privileged material (keys, authentication words or other secret items) prior to communications, there may be significant spoofing attacks possible. These vulnerabilities are grouped under the heading of "identification assurance" or "resolution." This paper considers public key cryptography in light of the second concern, but balanced by the operational advantages that may accrue from its use.

CLASSICAL CRYPTOGRAPHY

A "classical" cryptographic architecture is depicted in Figure 1. What makes this situation "classical" is that each of the two operators are using a cryptographic algorithm (realized in the hardware they are operating) that is initialized or configured, prior to their communicating, by a secret "keying variable" which has been physically distributed to both of them through some sort of protected channel; in Figure 1's case, this protected channel is a courier.

A classical cryptographic system might use the Data Encryption Standard or DES (1). This algorithm is a procedure for converting 64 bits, considered the "plaintext," into 64 different bits, considered the "ciphertext." The conversion of plaintext to ciphertext is governed by a 64-bit keying variable. Eight of the 64 keying variable bits are reserved for parity purposes and thus the number of possible DES keying variables is 2^{56}. The DES algorithm itself (as opposed to the operating mode) is an example of "codebook" cryptography, the name deriving from the old (WWI vintage) cryptographic procedure for encrypting words, letter combinations or other equivalents to stand for message text elements, usually words, letters, numbers, or phrases. The particular correspondence is defined by a specific codebook or system keying variable. In the case of the DES, the correspondence is one of 2^{56} possible one-to-one correspondences between all 2^{64} possible 64-bit words of plaintext and all 2^{64} possible 64-bit words of ciphertext.

Let us now examine the privacy of (or, perhaps, afforded by) the encrypted communications passed between the two operators of Figure 1. We submit that communications privacy is not a program, not a piece of equipment or a fascicle of doctrine but rather a condition, i.e., either the communications are free from exploitation or they are not. The encryption user faces the problem of determining how much in terms of costly resources is required to provide appropriate conditions for communications privacy. Making this determination involves correctly assessing and extrapolating the threat to the communications. This is a difficult task and is often approached through an incremental process. What we must do is to lay out the gradations of threat and then establish the costs and complexity to counter each level of threat. This allows management to draw the line which determines the appropriate funding for privacy to counter the perceived threat. It

also makes management incur responsibility. In the case of the scenario depicted in Figure 1, the communications privacy afforded is dependent on the following parameters:

- the integrity of the operators;
- the integrity of the courier;
- the physical and electronic integrity of the cryptographic machines;
- the cryptographic "strength" of the cryptographic algorithm; and
- the "goodness" of the keying variable.

The above set of prerequisites constitutes a logical "AND," i.e. , they must all be met for communications privacy to obtain. It is a sad fact of life, but one any security service must recognize, that reputation and perhaps corporate existence depends upon the ability to completely specify modules of responsibility and to quantify and demonstrably measure the efficacy of each such module. The reason, of course, is to be able to creditably disavow or transfer blame for compromise to other elements in the larger system. Thus, a host of standards and proposed standards have sprung up about classical cryptography ranging from operator security through cryptographic security.

PUBLIC KEY CRYPTOGRAPHY

During the past few years, a new approach has been added to cryptography by the evolution of what has become generically termed as "public key cryptography" or PKC. This discipline of cryptography is philosophically intriguing and potentially useful. In short, PKC does not require a priori distribution of keying material to the two parties who wish to communicate; that is PKC's distinct advantage. Its distinct disadvantage is that it can be spoofed. We will examine these facets later but first we wish to review, by example, public key cryptography.

A PKC depends on what has become known as asymmetric complexity. In essence, there are processes or operations which appear to require a lesser effort to do or perform than to undo, hence the oft used term, "trapdoor" cryptography. As an example of the trapdoor concept, consider that we are asked to multiply the two primes 7432339208719 and 341117531003194129. We obtain 2535301200456458802993406410751 without much effort. (This product is, incidentally, 2^{101}.)

Factoring, i.e., finding the factors through performing the inverse operation od multiplication, is a much more difficult undertaking. In fact, the factoring of 2^{101} into its two prime factors was a contribution by G.D. Johnson (2) to the field of computational mathematics.

A PKC endeavors to allow two parties to create a secret quantity (number or vector) through the use of an asymmetric complex process or function f(). The function f() will usually possess the following property f(a,f(b,c)) = f(b,f(a,c)). As an example, the Diffie-Hellman system (3) depends upon the difficulty of finding "discrete logarithms" within finite fields. Two parties, A and B, agree on a base, α, which is announced, or is at least available, publicly. The two parties also publicly agree on a prime number P which will be used to perform modular reduction. Party A then picks a number in secret, call it A, computes α^A divides by P which forms α^A modulo P and sends the remainder to party B. Meanwhile Party B has picked a secret number B, computed α^B, divided by P and sent the remainder to Party A. Party A upon receipt of α^B modulo P raises it to the Ath power; Party B similarly raises α^A modulo P to the Bth power. As a result both parties possess α^{AB} modulo P. All that a passive interceptor can glean from the communications is α^A and α^B (both "reduced" modulo P). Note further that Party A never needs to recover B nor does Party B need to know A for both parties A and B to arrive at the mutually held secret quantity α^{AB} modulo P. The system derives its cryptographic strength from the apparent asymmetric complexity that given α, A, and P, it is relatively easy to compute α^A modulo P, but, given α, α^A modulo P and P, it is relatively difficult to find A. Following our formal functional equation above, we see that for the Diffie-Hellman system $f(x,y) = y^x$ modulo P.

As an example of the Diffie-Hellman system, let us assume that parties A and B choose $\alpha = 3$ and P = 127. The process flow would proceed as follows.

PARTY A	PARTY B
• BOTH PARTIES AGREE TO USE $\alpha = 3$ AND REDUCE MOD 127	
• PARTY A CHOOSES (GENERATES IN A RANDOM MANNER) A = 16	• PARTY B CHOOSES B = 72
• PARTY A COMPUTES 3^{16} MOD 127 = 71	• PARTY B COMPUTES 3^{72} MOD 127 = 2
• PARTY A TRANSMITS 71 to PARTY B	• PARTY B TRANSMITS 2 TO PARTY A
• PARTY A COMPUTES 2^{16} MOD 127 = 4	• PARTY B COMPUTES 71^{72} MOD 127 = 4
• BOTH PARTIES NOW POSSESS A QUANTITY, 4, WHICH IS KNOWN TO THEM ONLY.	

If the Diffie-Hellman procedure is used with appropriately sized parameters, the commonly derived secret quantity can be used as an additive keytext or as a cryptovariable for a classical cryptographic system such as the DES. Thus we appear to have a method for dispensing with a separate key generation facility and the overhead of keying variable transfer via courier or other protected channel. There is a hitch, however, and this is what we call the “active transparency attack.”

The active transparency attack is depicted in Figure 2. What we show are two parties communicating but through an interloper who has actively interposed himself into their communications flow. The interloper is transparent to the communicators. He forms a secret variable which he uses in communications with the first and second parties. Then, when the first party encrypts a message and sends it to the second party, the interloper decrypts the message, copies it and re-encrypts the message for transmission to the second party using the key that the interloper holds in common with both parties. This weakness engendered by the active transparency attack is at the heart of much of the skepticism and reservation that surrounds PKCs. See for example (4).

TRADEOFFS

Our goal is to provide communications privacy at reasonable cost and reasonable risk. For some cases the cost and risk measures will vary greatly. It is our thesis that the spoofer (the perpetrator of the active threat) should answer some very basic questions. It is useful to evaluate the risk by looking at the problem through their eyes. First, the communications must be worthwhile reading. This is not always to be taken for granted. Second, there must be opportunity for electronic interpositioning. Third, the interloper must be willing to assume the risk of discovery. Let us examine these conditions a bit more deeply:

(a) Value of the communications - If the protected information is of value, but its loss or premature disclosure to the wrong parties is not an event with costly consequences, the interloper may simply elect to leave it alone. In this case, a PKC may be cost effective vis-a-vis a classical cryptographic system if it reduces the cost associated with the generation, transfer and storage of cryptovariables.

(b) Opportunity - It is difficult to transparently insert oneself into some communications links. For example, if the two parties are talking via the dial telephone network within the continental United States, it would be extremely difficult and costly for a spoofer to carry out the active transparency attack between line of sight microwave towers. The spoofer would have to receive the signal, demodulate the channel of interest after first demodulating the appropriate (jumbo/super/master) group and then remodulate the entire baseband for transmission to the next tower. The spoofer retransmitted signal would arrive at the next microwave tower in competition with the original

signal creating RF interference. Similarly, it would be difficult to spoof on an omnidirectional VHF radio network as someone would probably notice the very peculiar signal activity that would transpire. A wireline spoof, on the other hand, may be relatively easier to perform and quite difficult to detect. For example, the authors are aware of a specific instance of such a spoofing effort in which all communications were routed through a single communications facility. A spoofing attempt was conducted. The spoofers appeared transparent to the communication flow and the scheme was foiled only by considerations external to the communications. The communications link appeared absolutely normal throughout the entire operation.

(c) Risk of discovery - This is perhaps the most difficult of the variables to study and perhaps the most important. Before the spoofers attempt the attack, they must evaluate that if they are discovered, they may do greater harm to their overall interests than the good which would have accrued from a successful operation. This is so because discovery carries two messages with it. The first is that the data sought could be proven to be extremely important to the opposition. Second, it reinforces the knowledge that the victim's communications system is at least threatened. It is quite conceivable that following detection of an attempted exploitation, the intended victim will shore up his system to such a degree that other, more elaborate, attacks are necessary.

AN EXAMPLE

Consider that we wish to provide communications privacy to an instrumented testing range. Let the hypothetical range have a large and diverse set of sensors in the field. These sensors are clustered, that is they are arranged into local groups. Each group is managed by a base station and the sensors pass their data to their base station for preprocessing and concentration. The base stations communicate with and are controlled by the net control or master station. The function of the net control station is to pass messages between base stations. This architecture is depicted in Figure 3.

Let us now specify the communication architecture as follows:

(a) there are k base stations denoted by B_1, B_2,...,B_k;
(b) each base station is responsible for m sensors. The sensors associated with the ith base station are denoted by S_{i1} S_{i2} S_{im} and
(c) there is a single net control station denoted by N.

If it is desired to protect all the links in the network, there will be 2k(m+l) duplex privacy units. Assuming that the send and receive keying variables on any link are the same and that a different keying variable is assigned to each duplex link, there will be K=k(m+l)

different keying variables. If we let the function d(a,b) represent the distance in miles between the entities denoted by a and b, then we can compute an upper bound on the total travel, T, that must be performed to key the system. It is:

$$T = 2 \sum_{i=1}^{k} [d(N,B_i) + \sum_{j=1}^{m} d(B_i,S_{ij})] \text{ miles of travel.} \qquad (1)$$

If the terrain is amenable, the necessary travel may of course be reduced by base personnel visiting more than one sensor before returning to base. For a reasonably sized range, K and T can be sufficiently large to require a significant effort by those responsible for communications privacy.

Figure 3 is known as a “star” architecture. Note that K and T are linear with k. If, at some later time, it is desirable to make the net capable of faster response by allowing each base station to directly communicate with any other base station, then the new K and T

$$K = k(m+1) + \frac{1}{2}(k^2-k) \quad \text{and}$$

$$T = 2 \sum_{i=1}^{k} [d(N,B_i) + \sum_{j=1}^{m} (B_i,S_{ij})] + 2 \sum_{i=1}^{k-1} \sum_{j=i+1}^{k} d(B_i,B_j). \qquad (2)$$

The quantities K and T are now non-linear in k and as k increases, the classical keying variable distribution effort quickly becomes herculean. Obviously one can achieve a minimum travel distance by having one party carry all the keying variables via the traveling salesman route. This may increase the risk of loss of keying variables.

By using a public key architecture, however, one can greatly reduce the above problems. with a PKC, stations can be “written in and out” and nets reconfigured without elaborate bookkeeping. All that is required is a random source and a PKC algorithm at each site.

CONCLUSION

We have attempted to review briefly the two genres of privacy-type cryptographies, i.e., the classical and the modern public-key concept. We believe that the latter is not just an academic curiosity but may have a place in today’s communications even though it adds more responsibilities to those in charge of communications privacy. As sensors and processors become more widely distributed, often to geographically inconvenient regions, the advantages of automated keying through a PKC system are worth considering in trade-off studies.

REFERENCES

(1) National Bureau of Standards, 1977, Federal Information Processing Standard (FIPS PUB) Number 46.

(2) Brillhart, J. and Selfridge, J., 1967, Some factorizations of $2^n \pm 1$ and related results, Mathematics of Computation, Vol. 21, No. 97, pp. 87-96.

(3) Diffie, W. and Hellman, M., 1976, New directions in cryptography, IEEE Transactions on Information Theory, Vol. IT-22, No. 6, pp. 644-654.

(4) Kline, C. and Popek, G., 1979, Public key vs. conventional key encryption, Proceedings of the National Computer Conference, Vol. 48, pp. 831-837.

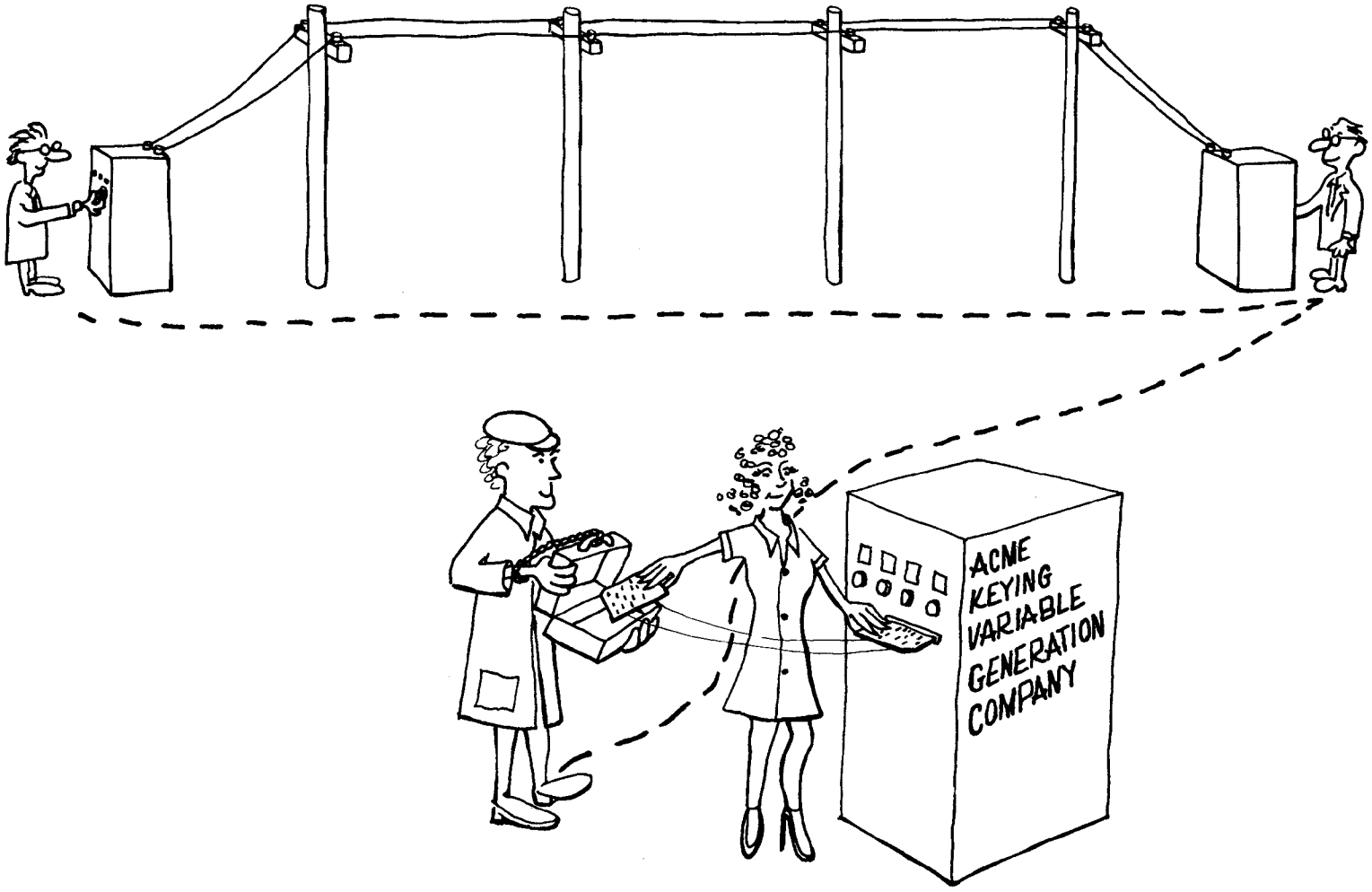

FIGURE 1
CLASSICAL CRYPTOGRAPHY

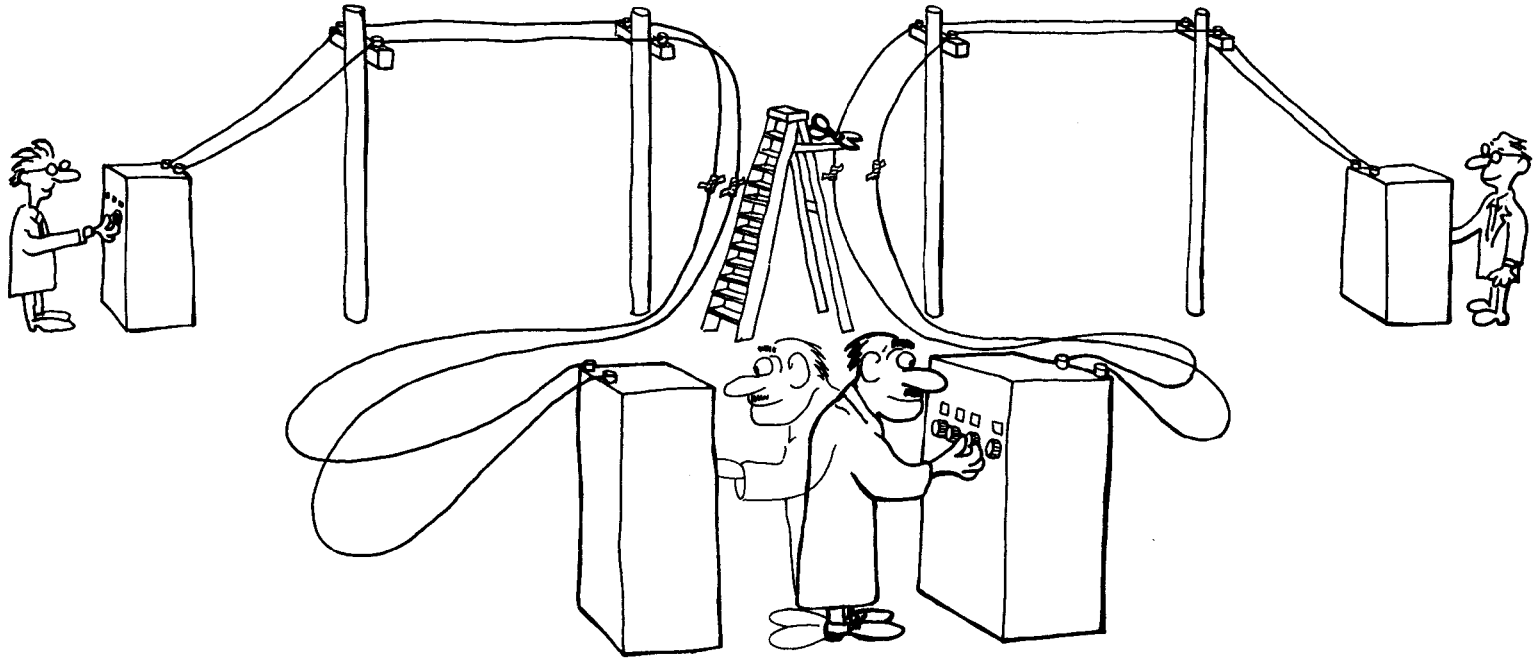

FIGURE 2
THE ACTIVE TRANSPARENCY ATTACK

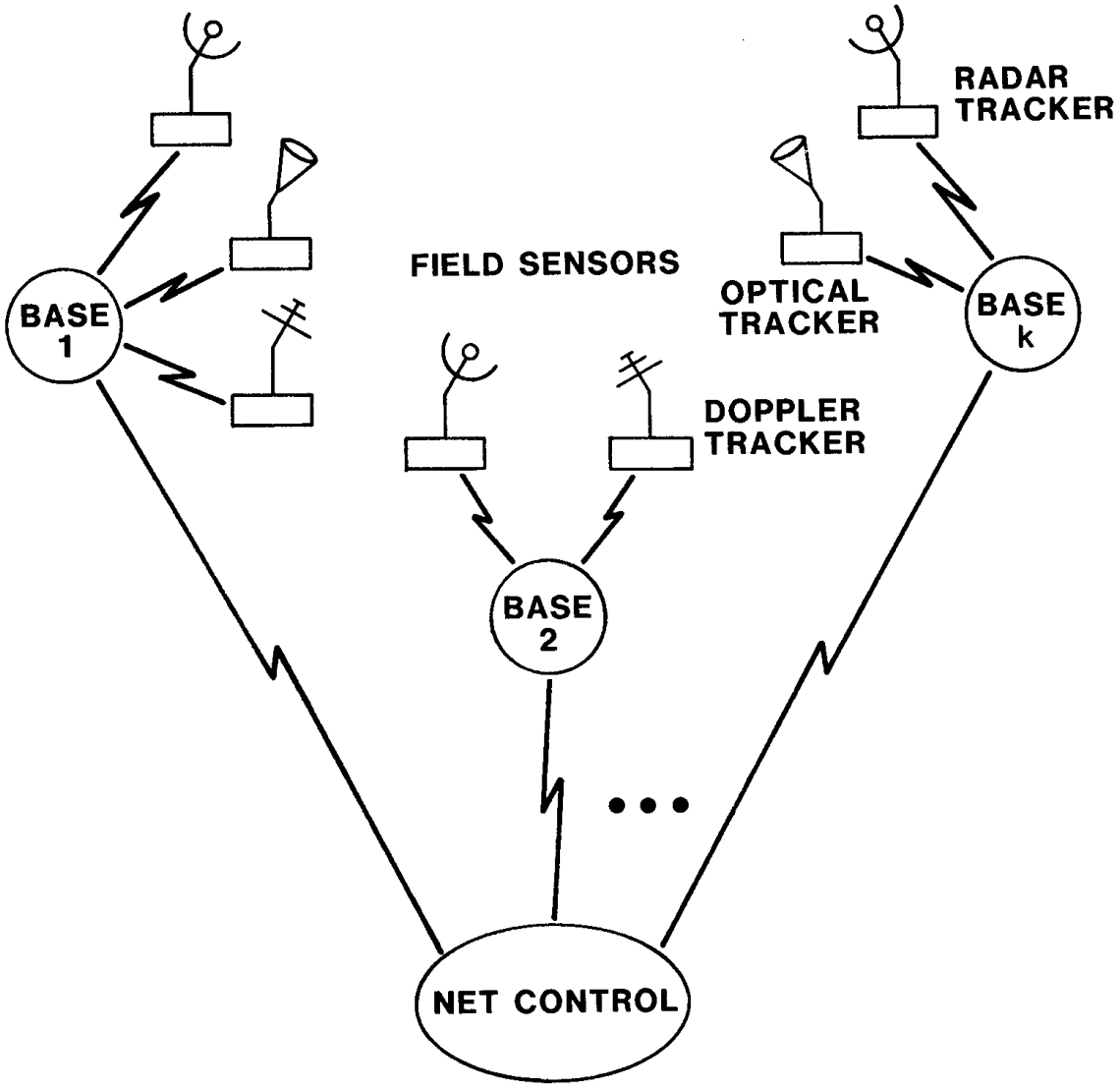

FIGURE 3
NETWORK EXAMPLE