Multisensor Data Fusion for Next Generation Distributed Intrusion Detection Systems

Tim Bass
ERIM International & Silk Road
Ann Arbor, MI 48113

Abstract—
Next generation cyberspace intrusion detection systems will fuse data from heterogeneous distributed network sensors to create *cyberspace situational awareness*. This paper provides a few first steps toward developing the engineering requirements using the art and science of multisensor data fusion as the underlying model. Current generation internet-based intrusion detection systems and basic multisensor data fusion constructs are summarized. The TCP/IP model is used to develop framework sensor and database models. The SNMP ASN.1 MIB construct is recommended for the representation of context-dependent threat & vulnerabilities databases.

I. Introduction

Industry forecasts estimate that the consumer market for security assessment tools will grow from approximately $150M dollars per year in 1999 to over $600M dollars in the year 2002 [1]. The Department of Energy (DoE) recently brought together network security experts to provide guidance to the US government for R&D technology projections in the area of malicious code, anomalous activity and intrusion detection [2]. Clearly, there are significant technical challenges ahead in a rapidly growing cyberspace intrusion detection & situational awareness marketplace.

Figure 1 illustrates the levels of situational awareness inference required to support both the warfighter and the network manager during cyberoperations [3]. Both commercial and military operations require cyberspace intrusion detection and situational awareness systems; sophisticated electronics must identify objects against a noise saturated environment, track the objects, calculate the velocity, and estimate the projected threat. These are non-trivial technical requirements.

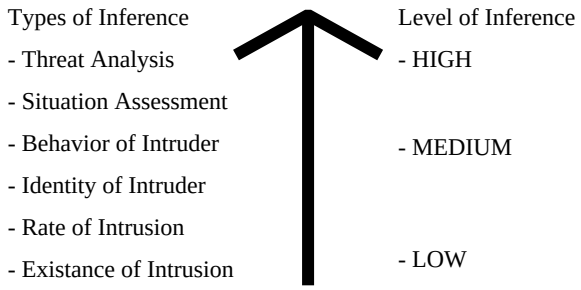

Fig. 1. Hierarchy of IDS Data Fusion Inferences

Network security professionals agree that current generation intrusion detection systems (IDS) are not technically advanced enough to detect non-signature based cyberattacks. During Operation Allied Forces, NATO Internet servers were attacked by Serbian hackers using e-mail bombs and network administration utilities to deny service by consuming network resources [4]. In 1997, the e-mail bombs of *The Langley Cyber Attack* demonstrated to the Marsh Commission on Critical Infrastructure Protection how current generation ID systems fail to detect serious threats to critical computer hardware and software [5]. One of the reasons for this shortfall is the fact that false alarms from ID systems are persistently problematic. False alarms cause serious organizational losses when technical resources are denied access to computer systems or security resources are misdirected to investigate non-intrusion events; systems which are prone to false alarms are practically useless as user confidence is marginalized.

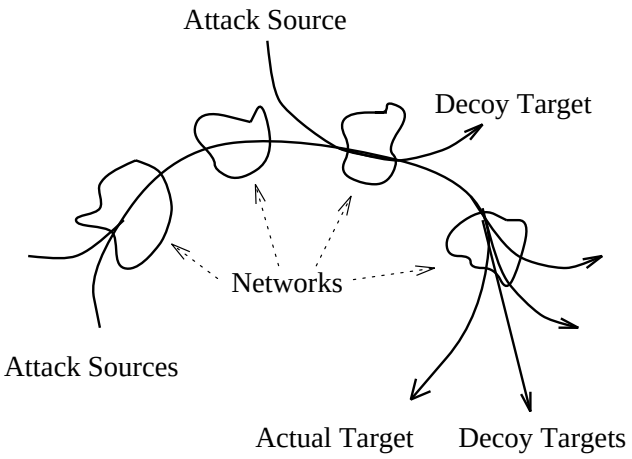

Fig. 2. Cyberattack with Multiple Sources & Targets

Another reason for the shortfall is that situational awareness technology is alarmingly primitive relative to protecting our critical electronic infrastructures. Commanders of network-centric operations do not have reliable tools to identify, track and estimate the attack rates multiple of "i-objects" in the infosphere, illustrated in Fig. 2. Adversaries in asymmetrical conflicts are at an advantage in cyberspace because no one dominates and those in power and authority have only primitive situational knowledge; this is causal to a void, or power vacuum, in present-day cyberspace.

Next generation cyberspace intrusion detection (ID) systems require the fusion of data from heterogeneous distributed network sensors. Section II reviews computer network

ID systems; and section III summarizes the high-level IDS fusion requirements identified in our recent ACM paper [3] on the subject. The underlying issues and challenges are by no means unique to intrusion detection systems; network management is also a very expensive infrastructure to operate. Generally, these systems fail to provide network engineers concrete situational information, typically overwhelming operators with system messages and other low-level data. Next generation network management and intrusion detection systems will interoperate in a uniform and cooperative model, fusing data into information and knowledge, so network operators can make informed decisions about the health and real-time security of their "corner" of cyberspace [3].

This paper provides a functional overview of how the art and science of multisensor data fusion enhances the performance and reliability of advanced cyberspace management systems, touches on design challenges, and suggests areas of further research and development. In addition, it is suggested that traditional thinking in broad concepts such as "network management" should evolve to fusion based "cyberspace situational awareness."

II. Intrusion Detection Systems Summary

Internet ID systems historically examine operating system audit trails and Internet traffic [6] [7] to protect the *availability*, *confidentiality* and *integrity* of critical information infrastructures. ID systems attempt to protect information infrastructures against denial of service (DoS) attacks, unauthorized disclosure of information, and the modification or destruction of data. The automated detection and immediate reporting of these events are required to respond to information attacks against networks and computers. The basic approaches to intrusion detection today may be summarized as *known pattern templates*, *threatening behavior templates*, *traffic analysis*, *statistical-anomaly detection* and *state-based detection*. These systems have not matured to a level where new network-centric attacks are reliably detected, verified, and assessed [3].

Computer intrusion detection systems were introduced in the mid-1980's to compliment conventional approaches to computer security. IDS designers often cite Denning's [6] 1987 intrusion detection model built on host-based subject profiles, systems objects, audit logs, anomaly records and activity rules. The underlying ID construct is a rules-based pattern matching system; audit trails are matched against subject profiles to detect computer misuse based on logins, program executions, and file access [3].

The subject-anomaly model was applied in the design of many host-based intrusion detection systems, i.e. *Intrusion Detection Expert System* (IDES) [8], *Network Intrusion Detection Expert System* (NDIX) [10] and *Wisdom & Sense* (W&S), *Haystack*, and *Network Anomaly Detection and Intrusion Reporter* (NADIR) [11]. There are other ID systems based on the Denning model and an excellent survey of these systems may be found in [7]. The basic detection algorithms used in these systems include [3]:

- weighted functions to detect deviations from normal usage patterns,
- covariance-matrix based approaches for normal usage profiling,
- rules-based expert systems approach to detect security events.

The second leading technical approach to present-day intrusion detection is *multi-host network-based*. Heberlein *et al.* extended the Denning model to traffic-analysis on ethernet based networks with the *Network Security Monitor* (NSM) framework [12]. This was further extended with the *Distributed Intrusion Detection System* (DIDS) which combined host-based intrusion detection with network traffic monitoring [7] [9]. Current commercial IDS such as *Real Secure* and *Computer Misuse Detection System* (CMDS) have distributed architectures using either rules-based detection, statistical-anomaly detection, or both [3].

A significant challenge remains for IDS designers to fuse sensor, threat, and situational information from numerous heterogeneous distributed agents, system managers, and databases. A coherent picture which can be used to visualize and evaluate the security of cyberspace is required. First, we review the basic constructs of the art and science of *multisensor data fusion* applied to ID systems in [3]. A scientific approach is required to develop highly reliable cyberspace intrusion detection systems which identify, track, and assess cyberspace situations with multiple complex threats.

III. Internet IDS Data Fusion

In a typical military command and control (C2) system, data fusion sensors are used to observe electromagnetic radiation, acoustic and thermal energy, nuclear particles, infrared radiation, noise and other signals. In cyberspace ID systems the sensors are different because the environmental dimension is different. Instead of a missile launch and supersonic transport through the atmosphere, cyberspace sensors observe information flowing in networks. However, just as C2 operational personnel are interested in the origin, velocity, threat, and targets of a warhead; network security personnel are interested in the identity, rate of attacks, threats, and targets of malicious intruders and criminals [3].

Input into next generation ID systems consists of sensor data, commands and *a priori* data from established databases. For example, the system input would be data from numerous distributed packet sniffers, system log-files, SNMP traps and queries, signature-based ID systems, user profile databases, system messages, threat databases and operator commands. This is illustrated in Fig. 3[1].

The output of fusion-based ID systems are estimates of the identity (and possibly the location) of a threat source, the malicious activity, taxonomy of the threats, the attack rates, and an assessment of the potential severity of the projected target(s) [3]. In [3] we built upon Waltz [13] to describe the generic sensor characteristics of a cyberspace

[1] Adapted from Waltz [14] to cyberspace ID system in [3]

multisensor fusion system; extensions to these attributes will be suggested in Section IV:

Detection Performance is the detection characteristics, i.e. false alarm rate, detection probabilities and ranges, for an intrusion characteristic against a given network-centric noise background. For example, when detecting malicious activity, non-malicious activity may be modeled as noise.

Spatial/Temporal Resolution is the ability to distinguish between two or more network-centric objects in space or time. A few of these primitive attributes are suggested in Section IV.

Spatial Coverage is the span of coverage, or field of view, of the sensor, (i.e. a the spatial coverage of a system log file is the computer system processes and system calls being monitored.)

Detection/Tracking Modes is the mode of operation of the sensor, i.e. scanning, single or multiple cyber object tracking; or multimode operation.

Target Revisit Rate is the rate at which an "i-object" or event is revisited by the sensor to perform measurements.

Measurement Accuracy is the statistical probability that the cyberspace sensor measurement or observation is accurate and reliable.

Measurement Dimensionality is the number or measurement variables for network object categories.

Hard vs. Soft Data Reporting is the decision status of the sensor reports, i.e. can a command decision be made without correlation or does the sensor require confirmation?

Detection/Tracking Reporting is the characteristic of the sensor with regard to reporting cyber events. Does the sensor maintain a time-sequence of the events?

In the fusion model, situational data is collected from network sensors with elementary observation primitives; identifiers, times of observation, and descriptions. The raw data requires calibration and filtering; referred to as *Level 0 Refinement*. Level 1 Object Refinement correlates data in time (and space if required) and the data is assigned weighted metrics. Observations may be associated, paired, and classified according to intrusion detection primitives [3].

Situation Refinement, provides situational knowledge and awareness after objects have been aligned, correlated and placed in context in an object base, aggregated sets of objects are detected by their coordinated behavior, dependencies, common points of origin, common protocols, common targets, correlated attack rates[2]. or other high-level attributes. Readers interested in additional high-level attributes are kindly referred to [3] for further discussion in this functional framework[3]. We begin by looking at the sensors and the level 0 data and level 1 object refinement processes.

[2] A threat taxonomy is discussed in Section V.

[3] Internet URL - http://www.silkroad.com/papers/html/ids/

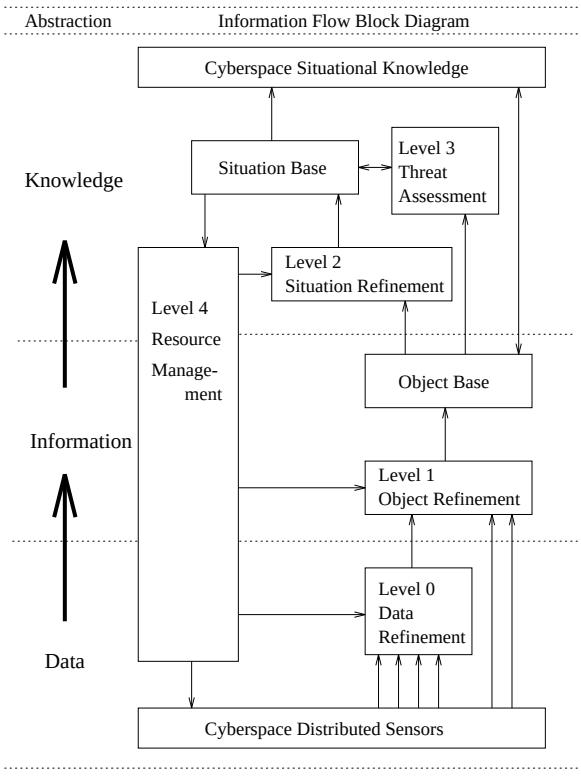

Fig. 3. Intrusion Detection Data Fusion

IV. Fusion Based Intrusion Detection System

Prior to proceeding into the details of tracking and identifying network-centric objects we offer a generic model of an object traversing the Internet, Fig. 4. The elemental construct is an IP datagram moving in a store-and-forward environment from source to destination; routed based on a destination address with a uncertain source address; decrementing the datagram time-to-live (TTL) at every router[4] [19]. The datagram is routed through both large and small networks, intranets, and Internet interdomain transit service providers. The confidence in the accuracy of the destination IP address will be considered 100 percent in this paper as well as that of the datagram TTL[5].

In the Internet interdomain transit model of Fig. 4, cyberflows are be identified and tracked by sensors at (or between) the interdomain gateways. At this point of the discussion we offer *a priori* this temporal construct:

> The temporal resolution of the cyberspace situational awareness, ? (Gamma), is directly proportional to the ratio of the transit time of the datagram, D_t, to the sensory fusion process and inference time, S_t.

The *Gamma Factor* is expressed in the basic linear relationship of Equation 1. It is also offered, *a priori*, that the transit time of the datagram must be much greater than the sensory fusion time. Stated in other terms, the tracking and

[4] known as a 'hop' in IP terminology

[5] this is not necessarily true in the general case

identication system must sense, transit, process, correlate, and react to a network object faster than the time it takes the object to reaches its target.

$$? = \frac{D_t}{S_t} \quad (1)$$

For an analogy we offer the tracking of an object in airspace, e.g. a projectile. If the intercept time of the projectile is greater than the radar tracking system and other associated processes, then it is not possible to track and react to the object before the projectile hits the target. If the network object reaches its destination in 30ms (for example), then the decision fusion process required for cyberspace situational awareness must be much less than 30 ms[6].

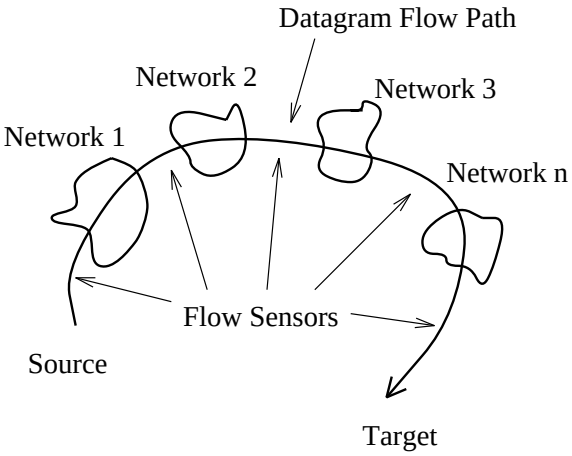

Fig. 4. Internet Attack ID Sensor Placement

The *Gamma Factor* is an interesting area for further research as these concepts are further developed. At this point in the discussion, we offer *a priori*:

> It is not mathematically feasible to develop effective cyberspace situational awareness systems (with high-resolution spatial and temporal correlation) using in-band (or in channel) communications.

This construct states that the network of sensors of Fig. 4 must be out-of-band and faster than the network under surveillance, as conceptually illustrated in Figs. 5 and 6. In this construct, an out-of-band network collects sensor information and issues C2 (command and control) directives to filters, firewalls and other active network devices. Highly critical situational awareness can be achieved by networking the sensors (and optional command and control links) with a very high Gamma Factor.

[6]This *a priori* construct has a side effect in security architectural relationships: Critical network systems requiring a very high degree of protection against cyberattacks should not be placed on high bandwidth, high speed (capacity) Internet links if the high network capacity is not a requirement of the critical system.

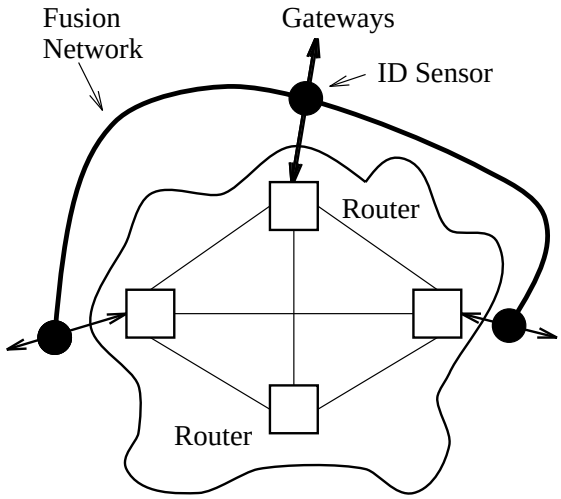

Fig. 5. Gateway Sensors on CSA Fusion Network

V. Sensor Data Reduction and Threat Objects

The volume of IP packets processed at the busy Internet gateways of Figures 4 and 5 can be enormous; consequently, gateway sensors acquire and forward proportionally large amounts of data to packet analysis and correlation engines. For example a router processing 100,000 packets per second on a high speed interface, logging 14 bytes of information per packet, produces approximately 1.4 MBPS of data per sensor. It is clear that distributed sensors in network-centric IP fusion systems require local processing, Fig. 7.

Consequently, sensor output data should be reduced at the sensor to the extent possible in order to minimize central fusion processing and transport overhead costs. This paper does not further address the actual sensor data reduction or selection algorithms, T_s, and leaves this for another discussion.

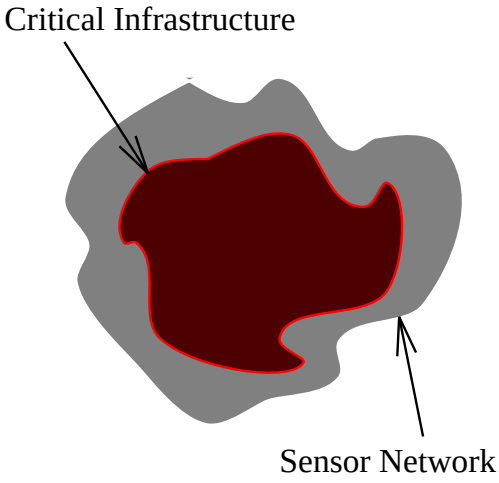

Fig. 6. Critical Infrastructure - Sensor Network

The sensor data reduction ratio (SDRR), Δ (delta) is directly proportional to the ratio of the input to the sensor,

S_{in}, to the output, S_{out}.

$$\Delta = \frac{S_{in}}{S_{out}} \quad (2)$$

In the remaining discussion of this section we focus on the sensor output D_s^{out}. This is introduced by "shifting gears" and outlining an example taxonomy of TCP/IP based threats which can be used as a a framework in the design of local sensor processing and database requirements. The reader is referred to Antony's very complete discussion [17] on database requirements for fusion system and situational knowledge constructs. Knowledge is either *declarative* or *procedural*; declarative knowledge is passive factual or knowledge of relationships (e.g. files). Procedural knowledge is a special case of declarative knowledge represented as patterns, algorithms, and mathematical transformations. It is generally accepted that the size of declarative knowledge-base will be much greater than that of procedural knowledge-base.

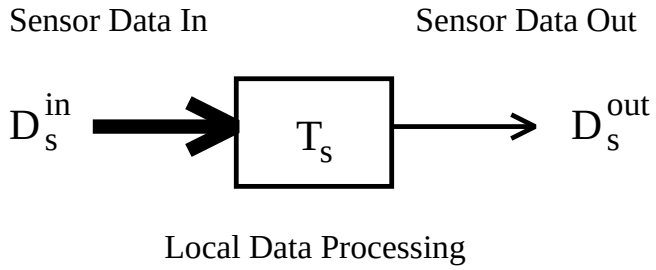

Fig. 7. Sensor Data Reduction

Entity-relationships are the most fundamental declarative models for sensor data representation. Binaries trees, family trees, and general taxonomies are examples of the elemental database relationships required for situational analysis; the vast majority can be represented by the SQL command [17]:

SELECT(attribute) FROM (table) WHERE (condition)

With this basic database model and data selection primitives in mind, this paper offers a framework TCP/IP threat taxonomy based on TCP/IP and the SNMP management information base (MIB) [18], illustrated in Figs. 8 - 10. The SNMP MIB model is well suited for representing network-centric threats.

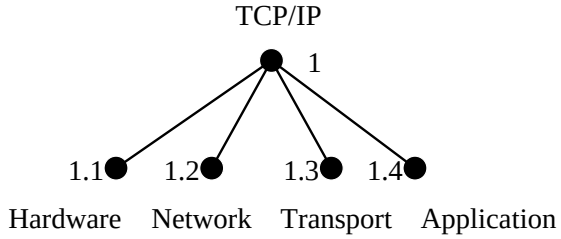

Fig. 8. Example TCP/IP Threat OID

Threats to TCP/IP at the physical layer are service disruptions due to natural disasters such as fires or flooding, cuts to cables, malfunctioning transceivers, and other hardware failures. From this construct, we turn our attention to the IP network layer and the TCP transport layer.

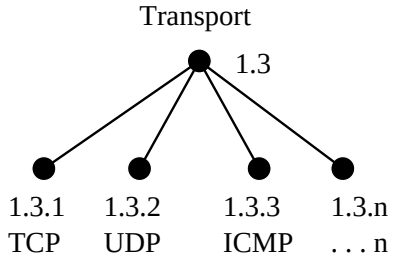

Fig. 9. Example IP Transport Threat OID

There are three primary data flows (services) which exist in the Internet; User Datagram Protocol (UDP), Transmission Control Protocol (TCP), and Internet Control Message Protocol (ICMP) [19]. Domain Name System (DNS) cache poisoning and UDP port-flooding denial of service attacks are examples of two vulnerabilities exploited using UDP services. The ping-of-death and ICMP redirect bombs are examples of Internet attacks based on ICMP. TCP vulnerabilities include TCP sequence number and SYN flood attacks, Fig. 10.

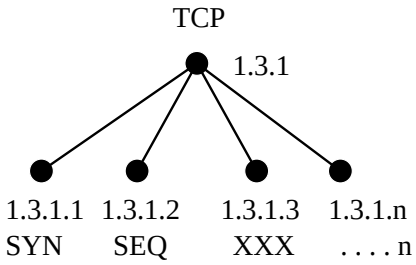

Fig. 10. Example TCP Threat OID

Security threats can be easily represented using the ASN.1 MIB notation. For example, a TCP SYN flood attack could be represented with the following OBJECT IDENTIFIER (OID);

tcpSYNFlood OID ::= { iso 3.6.1.5.1.3.1.1 }

Additional sub-object examples for *tcpSYNFlood* OID could be the source address or the target address of the malicious SYN packet:

tcpSYNFlood.source OID ::= { iso 3.6.1.5.1.3.1.1.1 }

tcpSYNFlood.dest OID ::= { iso 3.6.1.5.1.3.1.1.1.2 }

Developing an extensible TCP/IP security MIB would be a critical first step on the road to developing Internet IDS fusion systems. Using the example framework above as a starting point, intrusion detection local processing agents could be controlled from management systems. Sensor information should be stored locally on the sensor processing

agent as feasible, based on dynamic and static storage constraints.

VI. Concluding Comments

This paper builds on the multisensor IDS framework of [3] to begin the process of specifying Level 0 and Level 1 fusion requirements. The SNMP-style ASN.1 MIB model is recommended as the inter-IDS fusion database model. The TCP/IP threat-MIB should be further developed. However, these are only the a few first steps in the "long road" to the development of data fusion systems for cyberspace situational awareness.

A pilot on a mission understands the objectives, operating within concise rules on how to engage the enemy in a hostile environment. Commanders may return fire and destroy an enemy aircraft within well defined parameters and situations. The greater the situational awareness the more information a commander has to make difficult combat decisions [20].

> "When the battlespace is cyber, the attacks active and hostile, under what conditions does the communicator *return fire*?" [20]

Today, there are no well defined rules of engagement for network operators during cyberattacks [21]. Without high levels of cyberspace situational inference it is imprudent to execute counter-offensive operations unless the source of the attack is known with a very high probability; and the source address of hostile activities is easily masked in cyberspace. Therefore, the fidelity of counter information rules of engagement is directly proportional to the degree of cyberspace situational awareness and quality of knowledge inference.

This paper only offers small steps in the process of setting the engineering requirements to design and develop cyberspace situational awareness systems. The automated identification and tracking of dynamic network-centric subjects in cyberspace is a core technical competency required for the management of multiple cyberattacks. The identification tracking, classification, and assessment of both enabling and inhibiting network-centric activities in this complex infrastructure is possible using the art and science of multisensor data fusion as a design framework.

Each of the models and constructs offered in this paper require much further development. We hope that fusion engineers and scientists have found the areas of research and development suggested in this paper both interesting and motivational. It is also our hope that this paper contributes, in some small way, to forward the overall goals and objectives of the sensor fusion research community.

VII. Acknowledgments

I am very appreciative to members of the USAF/SC for all of our stimulating network-centric discussions; especially Lt. Gen. Bill Donahue, Lt. Gen. Jack Woodward, Brig. Gen. Dale Meyerrose, Brig. Gen. (select) Bernie Skoch and Lt. Col. Dave Gruber. Also, I would like to thank Ed Waltz for his inspirational life work on multisensor data fusion and information warfare.

References

[1] Silverman, R., *Intrusion Detection Systems Sniff Out Digital Attack*, The Wall Street Journal, pg. B6, February 4, 1999.

[2] Schultz, G., Chairman, *Detection of Malicious Code, Intrusions, and Anomalous Activity Workshop*, Department of Energy, National Security Council & Office of Science and Technology Policy, February 22-23, 1999.

[3] Bass, T., *Intrusion Detection Systems and Multisensor Data Fusion: Creating Cyberspace Situational Awareness*, Communications of the ACM (to appear), 1999.

[4] de Bony, E., *NATO reinforces against Net attack from Serbs*, InfoWorld Electric, Posted at 9:40 AM PT, Apr 2, 1999.

[5] Bass, T., Freyre, A., Gruber, D. and Watt., G., *E-Mail Bombs and Countermeasures: Cyber Attacks on Availability and Brand Integrity*, IEEE Network, pp. 10-17, Vol. 12, No. 2., March/April 1998.

[6] Denning, D., *An Intrusion-Detection Model*, IEEE Transactions on Software Engineering, Vol. SE-13, No. 2, pp. 222-232, February 1987.

[7] Mukherjee, ., Heberlein, L., and Levitt, K., *Network Intrusion Detection*, IEEE Network Magazine, Vol. 8. No. 3, pp. 26-41, May/June 1994.

[8] Denning, D. et al., *A Prototype IDES: A Real Time Intrusion Detection Expert System*, Computer Science Laboratory, SRI International, August 1987.

[9] Snapp. S. et al., *A System for Distributed Intrusion Detection*, Proceedings of IEEE COMPCON, pp. 170-176, March 1991.

[10] Bauer, D. and Koblentz, M., *NDIX - An Expert System for Real-Time Network Intrusion Detection*, Proceedings of the IEEE Computer Networking Symposium, pp. 98-106, April 1988.

[11] Hochberg, et al., *NADIR: An Automated System for Detecting Network Intrusion and Misuse*, Computers & Security, Elsevier Science Publishers, pp. 235-248, 1993.

[12] Heberlein, L. et al., *A Network Security Monitor*, Proceedings of the IEEE Computer Society Symposium, Research in Security and Privacy, pp. 296-303, May 1990.

[13] Waltz, E. and Llinas, J., *Multisensor Data Fusion*, Artech House, Boston, MA, 1990.

[14] Waltz, E., *Information Warfare Principles and Operations*, Artech House, Boston, MA, 1998.

[15] Hall, D., *Mathematical Techniques in Multisensor Data Fusion*, Artech House, Boston, MA, 1992.

[16] Varshney, P., *Distributed Detection and Data Fusion*, Springer-Verlag, New York, NY, 1996.

[17] Antony, R., *Principles of Data Fusion Automation*, Artech House, Boston, MA, 1995.

[18] Rose, M., *The Simple Book*, Prentice-Hall, Englewood Cliffs, NJ, 1994.

[19] Stevens, R., *TCP/IP Illustrated, Volume 1: The Protocols*, Addison-Wesley, Reading, MA, 1994.

[20] Bass, T., *Cyberspace Situational Awareness and Cyber Rules of Engagement*, Silk Road, December 8, 1998.

[21] Graham, B., *Cyberwar: A New Weapon Awaits a Set of Rules*, The Washington Post, pp. A1, A10, July 8, 1998.