Multi-objective Mobile Network Anomaly Intrusion

Kenneth S. Edge, Gary B. Lamont, and Richard A. Raines

Air Force Institute of Technology, Dayton, OH, USA

Summary—Mobile ad hoc networks have inherent vulnerabilities based on their very nature. Sarafijanovic and Boudec propose using an artificial immune system (AIS) approach to providing robust and reliable misbehavior detection. This paper builds upon that concept by framing the problem as a multi-objective problem attempting to balance efficiency and effectiveness of the detection. After mapping the algorithm to a symbolic representation and discussing the design of the multi-objective AIS, the testing results are discussed and a Pareto front depicting the results is depicted. A critique of selected current literature in the area of mobile network security is also included.

Key words: Intrusion Detection, Mobile Networks, Multi-objective, Artificial Immune System.

1. Introduction

By their very nature, mobile ad hoc networks (MANETs) are especially vulnerable to malicious attacks. In a wired network, an attacker must either gain physical access to the network or pass through a predefined set of nodes that can act as firewalls and/or gateways. In a wireless network, an attack can target any node and come from anywhere. Because of this architectural difference, a wireless network must ensure that every single node is prepared for an attack and protect them accordingly [2]. As wireless networks are rapidly developed, security is one of the greatest challenges for their implementation [5].

An intrusion detection system for a mobile network can be designed with features similar to the human immune system (HIS). The HIS is modeled with an artificial immune system (AIS) with two objectives. These two objectives are to find the intruders and to act quickly. The two objectives can be restated as efficiency versus effectiveness. With multiple objectives the problem becomes one of a multi-objective artificial immune system (MOAIS).

This paper discusses the problem of mobile network anomaly intrusion detection in Section II. It presents this problem symbolically in Section III. In Section IV, a specific MOAIS is outlined and discussed to solve this class of problems. Testing and evaluation techniques are discussed in Section V, and finally current literature on the subject is critiqued in Section VI.

The views expressed in this article are those of the author and do not reflect the official policy or position of the United States Air Force, Department of Defense, or the U.S. Government

Manuscript received March 23, 2006.

2. Background

MANETs are a network of individual mobile wireless nodes that can communicate with each other without any inherent network infrastructure or centralized control [3]. There are many applications for MANETs as they allow the exchange of information real time in a very mobile environment. A hypothetical military application is depicted in Figure 1. In this application, multiple entities such as unmanned aerial vehicles (UAVs), robots, and even humans on the battlefield can exchange the real time information they need in a dynamic environment in order to operate more effectively.

The major advantages of a MANET are unrestricted mobility and connectivity [3]. The most significant disadvantage of a MANET is its more complex security issues due to changing topology, limited capability of individual nodes, and its reliance on a trust relationship between nodes. These additional security issues are detailed in the following paragraphs.

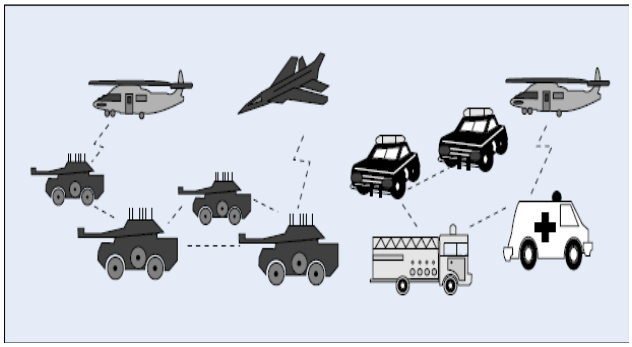

Figure 1 – Example MANET [3].

MANETs are vulnerable to attacks based on their fundamental characteristics of constant changing topology, lack of centralized control, required distributed cooperation, limited individual node capability, and open medium [3]. The changing topology presents challenges in routing as well as implementing any type of static security solution. Without centralized control, individual nodes must rely on other nodes in the network in order to communicate. If a malicious node fails to follow the correct protocols, it can wreak havoc to the system if the other nodes do not recognize the suspect node as malicious. Limited capability of the nodes opens up the vulnerability of a denial of service attack by exhausting limited resources such as battery life. It also makes detection

of a malicious node harder because nodes often disconnect from the network in order to conserve their resources during normal operation, not just because they are behaving badly [11]. Finally, the open medium of the network allows anyone to listen to communications and possibly enter the network as an imposter.

Many of the types of vulnerabilities that a wireless network is susceptible to are the same as those for a wired network. They might include eavesdropping, spoofing, replay attacks, and denial of service [1]. Because mobile network routing relies heavily on a trust relationship between nodes, mobile networks are especially susceptible to routing misbehavior as communication can be disrupted or even impossible when it occurs [10]. Routing behavior may be the result of a malicious node that was corrupted via an intrusion or a simple system failure. For the purposes of this paper we assume that the misbehavior is due to an intrusion.

Before trying to design a system to detect intrusion on a mobile network it is important to define an attack. [6] defines an attack as 'a violation of expectations of the agent programmer or owner caused by one or more than one intentional attacker(s).' It is important to note that this definition only refers to 'intentional' attacks. Thus an anomaly that is caused by a normal system failure is not covered in the scope of this paper. Due to the nature of MANETs, some attacks will be successful. Because MANETs are vulnerable, an intrusion detection system is vital so that operating nodes can ignore nodes that are malicious or have been compromised [2].

Due to the distributed nature of a MANET and the requirement to protect every node individually, an artificial immune system approach to intrusion detection for the network is a natural solution to the problem. The use of an AIS for intrusion detection allows the system to learn what normal behavior for the system is based on past patterns of activity and detect anomalous behavior from a malicious node much as the human immune system learns what types of cells are allowed and detects malicious cells that are trying to attack the body. Due to the lack of centralized control in a MANET, the IDS must be host based as shown in Figure 2.

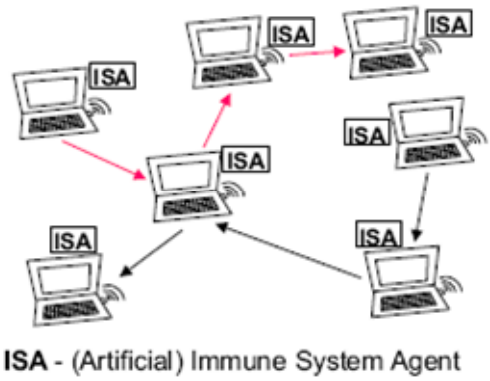

Fig. 2 – Host based agents in Mobile IDS [9]

3. Mapping to a Symbolic Representation

In order to map the problem of mobile network anomaly intrusions to an artificial immune system domain we must define how each element of the problem domain maps to the AIS domain. The following mapping follows the convention described in [9].

Antigens represent the observed protocol events

Antibodies are created randomly and trained but the format matches that of antigens.

Self cells represent non malicious nodes

Nonself cells represent malicious nodes

Bone marrow is represented as a protected environment for learning with certified well behaving nodes

Clonal Selection represents the process of creating new antibodies from ones that are performing well. Poorly performing antibodies are replaced with mutated versions of high affinity antibodies.

Further defining the above terms using the problem domain is described below:

Protocol events are mapped to a finite set of primitives to form an alphabet. The protocol events are recorded for a defined time and constrained to a maximum number of events [9]. If the protocol streams were not confined to just a sampling, the sequences would quickly become too large to handle computationally. It is important to remember that the events that are recorded are only a representative sample. This means that it could be possible to orchestrate a well crafted attack that could slip undetected between the recorded events. To combat this it is important to randomize when the time intervals that the events are recorded occur. For the sake of simplicity, we assume that this is correctly done and it would be infeasible to mask an attack by inserting it between recorded events.

A=RREQ sent B=RREP sent C=RERR sent D=DATA sent and IP source address is not of monitored node E=RREQ received F=RREP received G=RERR received H=DATA received and IP destination address is not of monitored mode

Table 1 – Alphabet of Primitives [9]

The following mapping is from [9].

A protocol trace may consist of the following sequence

$$l_1 = (EAFBHHEDEBHDHDHHDHD,\ldots)$$

A set of genes used for pattern matching is also defined to develop the antigen. Using the following list

Gene1=#E
Gene2=#(E*(A or B))
Gene3=#H
Gene4=#(H*D)

l_1 can be mapped to the antigen l_2

l_2 = (3 2 7 6)

To facilitate bit matching we encode the l_2 antigen to a string of ones and zeros where the value of the gene is represented by a one in the nth bit. For example, l_2 would map to the following

l_3 = (0000001000 0000000100 0010000000 0001000000)

l_3 is the final representation of a single antigen. Antibodies have the same representation except that they can have multiple ones in each gene string. We consider an antigen to match an antibody if the antibody has a one is every position that an antigen has a one.
For example the antibody a_1 = (1100001001 1000010110 0011001000 1001000100) would match antigen l_3 because it has a one in every position that l_3 does.

In order to prevent a false positive for simply matching an antigen to an antibody, a threshold equation is used to ensure that more than one detector matches the same misbehaving node. The equation for the threshold detection is:

$$\frac{Mn}{n} > \theta_{\max}\left(1+\frac{\xi(\alpha)}{\sqrt{n}}\sqrt{\frac{1-\theta\max}{\theta\max}}\right) \quad (1)\ [10]$$

Where M_n is the number of detectors that detected the node, n is the number of detectors that monitored the node, $\theta_{\max}$ is the maximum bound for false positive detection, and $\xi(\alpha)$ is the (1-α)-quantile of the normal distribution. If the equation is true, the node is considered malicious.

4. Design of MOAIS

In order to design the MOAIS, the symbolic notation of the problem is developed into a working algorithm. The best representation of the operation of the algorithm is shown in Figure 4. From this depiction, we see that a set of antibodies is randomly generated and then trained using both positive and negative selection in order to arrive at a useable set of detectors. It is important to note that this training must be done within a trusted environment. This is analogous to the HIS creating antibodies in the bone marrow of the human body.

Once the detectors are developed, they are able to detect both suspicious and malicious nodes in the network. The way that the IDS differentiates between the two is that a malicious node must be detected as suspicious by a threshold number of other nodes. If it is below the specified threshold, then it is labeled as only a suspicious node and no further action is taken.

Should a node be labeled as malicious, the IDS takes appropriate action and then runs through a clonal selection process which allows the IDS to increase the number of detectors that found the malicious node. These new detectors are created from a copy of the successful detector and then mutated to create small variations. These mutations are then run through a negative selection process to be sure that they do not detect non malicious nodes (self). The newly created detectors then replace detectors with low fitness values.

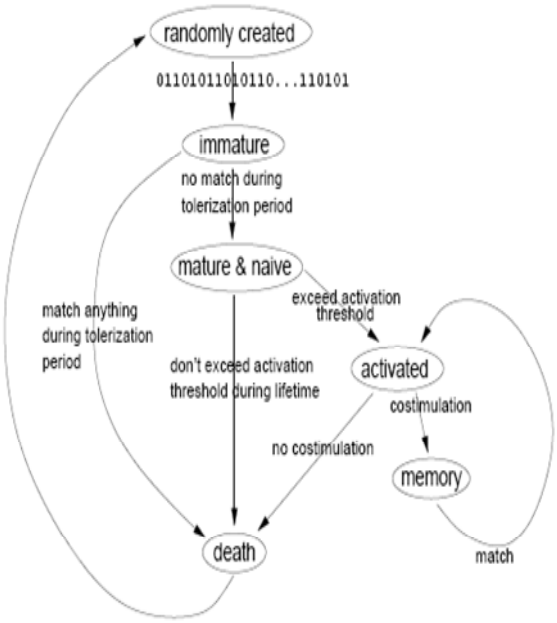

Fig. 3 – Lifecycle of Antibody [4]

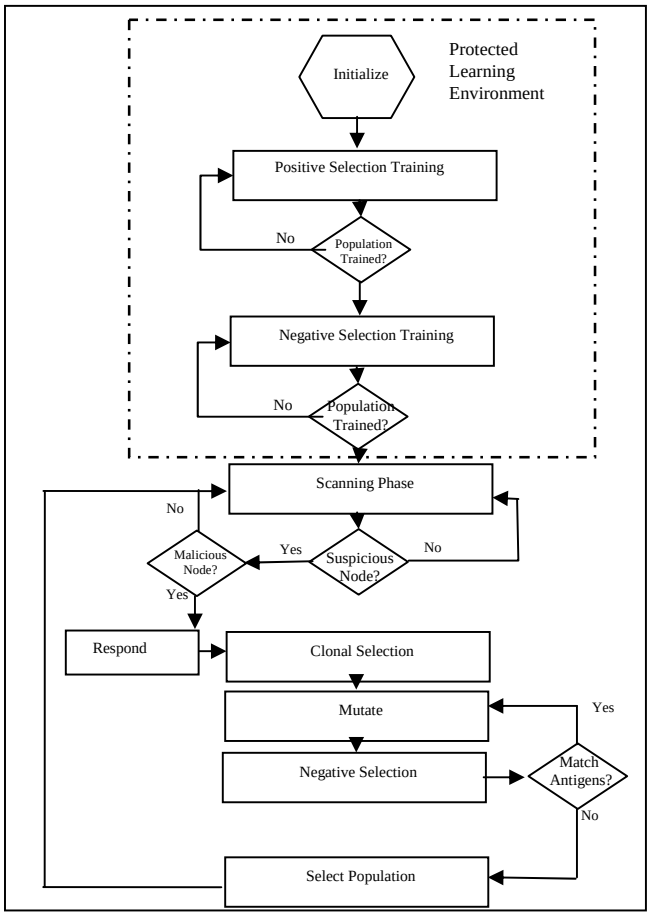

Figure 4 – Operation of MOAIS For IDS of MANET

As stated earlier, the algorithm is a multiobjective one with fitness functions based on effectiveness and efficiency.

$$F = w_1(f_{effectiveness}) + w_2(f_{efficiency}) \quad (2)$$

where $w_1 + w_2 = 1$ (3)

$f_{effectiveness}$ is measured in terms of the false positive rate and $f_{efficiency}$ is measured in time until classification.

In order to attain the desired performance metrics from the IDS, many parameters have to be determined. A partial list of tuning parameters includes learning time in the protected environment, number of antibodies, the size of the antibodies, false positive threshold, size of duplication in clonal selection, and rate of mutation [9].

5. Testing and Evaluation

The design of the MOAIS was tested using a simulation environment for MANETs called Glomosim [9]. By varying the targeted false positive classification rate, the authors were able to produce plots of false positive effectiveness ratios (effectiveness) and time until classification (efficiency). The plots have been combined to produce the Pareto plot shown in Figure 5. By minimizing the false positive classification rate, the results move down to the right of the line favoring effectiveness over efficiency.

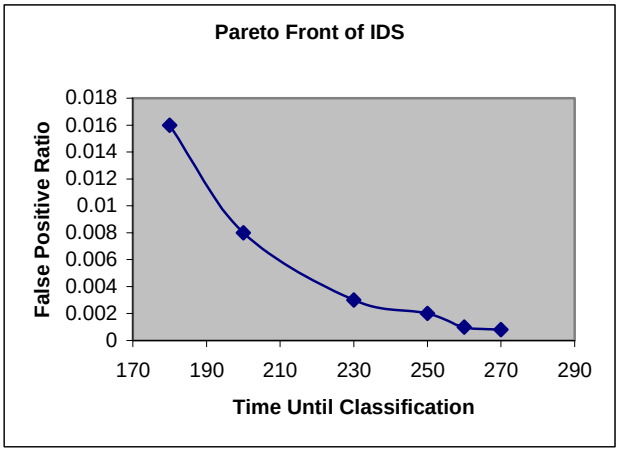

Figure 5 – Pareto Plot of IDS Results

The results also showed that the clonal selection function of the algorithm had significant effects in response time [9]. While decreasing the detection time, clonal selection also reduced the false positive rate. The rational explaining this was that if a node was exposed to a malicious node in the past then it would be easier to recognize another malicious node in the future by using clonal selection [9].

With the Pareto plot, a decision maker is able to objectively make decisions about the architecture of the IDS. Depending on the application, a low false positive rate might be required. In a different network, the time until classification is more important. The Pareto plot allows the decision maker to make informed trade offs with the knowledge of how such trade offs will affect the parameters of the IDS. If the Pareto plot shows unacceptable IDS behavior in all variables then the IDS may have to be redesigned in order to shift the plot to the left for a more acceptable response.

6. Critique of Current Literature

As mobile networks continue to grow in importance, the number and types of attacks also continue to grow. Intrusion detection for mobile networks has become an issue that also continues to grow and the amount of scholarly literature reflects it. This paper critiques selected articles that represent some of the most advanced concepts in intrusion detection on MANETs.

As is evident by the previous discussions, [9] most closely represents the concept of using a MOAIS to solve the problem of mobile network intrusion problems. The authors continued their research in [10] and improved the AIS described in this paper to include a virtual thymus to eliminate the need for the protected learning phase, added a danger signal to decrease false positives, used memory detectors to decrease the time until detection of malicious nodes, and added clustering to further reduce false positives. The journal article expands their work from [9] and presents promising results. As an

appendix, they include pseudo code of their AIS building blocks.

In [5], Karchirski and Guha propose a system that uses an agent type of intrusion detection system. Clusters of nodes use a protocol to select which nodes act as the agents and what their respective functions are. Although an interesting concept, there are some serious shortcomings in their work. First, their results indicate the system is not very scalable. After adding about 40 nodes, the number of packets that are dropped from analysis becomes unacceptable (See Figure 6). This makes the system an easy target of a coordinated denial of service attack using two agents. The first would flood the specific IDS agents with packets while the second would actually perform a specific attack which would go undetected with a high probability.

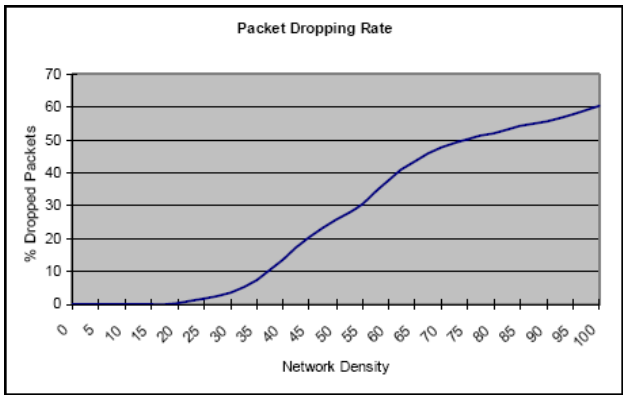

Figure 6 – Non-scalability of IDS [5]

The authors also stated that if any node was suspicious then the system would reissue security keys for the entire network. That is a tremendous amount of overhead for a large network with multiple keys for simply a suspicious node. Again, this shows the proposed IDS system is not very scalable.

Another shortcoming in [5] is that the authors do not address the issue of how to deal with a malicious node during their voting and selection protocols. Every node is not an IDS agent so every node does not monitor the network. Depending on the mobility of the nodes and where the agents are, a malicious node could remain undetected indefinitely. If the malicious nodes can influence the selection of the agents through rigged voting then they have an even greater chance of remaining undetected.

In [7], the authors present a sound design of using a statistical anomaly approach to a network IDS. They discuss the shortcomings of older IDSs in that they typically assume a normal distribution for events that may not actually follow that distribution. Their design uses neural nets and the Kolmogrov-Smirnov (K-S) test so they are more concerned with the cumulative distribution functions for their metrics which are much easier to develop empirically. This paper is applicable to the design presented here in that the method from [7] could possibly be used with the MOAIS in this paper to develop the gene patterns that are used for detection. Currently, these gene patterns are defined using a best guess methodology to try to attain the best detection capabilities [9]. The system could possibly be improved if some sort of dynamic statistical analysis were used in determining the genes.

A good background paper on the issue of IDS in MANETs is [11]. The authors described the unique vulnerabilities of MANETs thoroughly and what type of architectures for an IDS are needed. The problem of using current wired network IDS solutions in a wireless network was explained. They also discussed basic concepts of an IDS to include host versus network based as well as the differences between misuse and anomaly detection. The logical conclusion that the authors came to was that every node needs to have some form of IDS. This is a direct contrast to [5].

In order to keep their research manageable, the authors restricted the types of attacks used in their experiments to those only attacking routing protocols. They also used only three types of protocols in their research. They included Dynamic Source Routing (DSR), Ad-hoc On-Demand Distance Vector Routing (AODV0, and Destination-Sequenced Distance-Vector Routing (DSDV) [11]. Using these three protocols, they determined that it is important for the routing protocol to have some degree of redundancy for anomaly detection to work best [11].

Patwardhan, et al, proposed an IDS for implementation on handheld computing devices in a MANET [8]. To their knowledge, theirs was the first implementation of an IDS deployed on handheld devices. The protocol they used was SecAODV. The basic operation of their IDS relies on comparing ingoing packets to outgoing packets from a node's neighbors to determine if any neighbors are malicious. To do this, the handheld device must listen in promiscuous mode to catch its neighbors' packets. For a handheld device, this would seriously limit the battery life. This is an issue the authors failed to address. Although the authors argue that their solution is scalable, their experiments do not show this. They simply make the assertion but fail to show any results backing it up. Although it is important to develop an IDS for handheld type devices, in my opinion, the authors failed to show that their method was a better way.

7. Conclusion

This paper discusses the unique issues of MANETs in regards to intrusion detection. Although there are many successful implementations of IDSs in wired networks, due to the inherent differences between wired and wireless networks, these solutions fail for a wireless network. This paper explored the issue of using a MOAIS to solve this problem. Because a wireless ad-hoc network is structurally similar to cells roaming around in the human body, an artificial immune system type approach appears to be very promising in detecting malicious nodes. The AIS allows the IDS to be lightweight yet effective which is paramount within the limited capabilities of the devices that are typically in a wireless network.

In order to clearly understand the problem, this paper has defined the intrusion detection problem symbolically which eases the transition from the problem domain to the

algorithmic domain. The results of the current implementation of the MOAIS are discussed and current literature dealing with IDS in MANETs is critiqued.

References

[1] Albers, P., Camp, O., Percher, J., Jouga, B., Me, L., and Puttini, R. Security in Ad Hoc Networks: A General Intrusion Detection Architecture Enhancing Trust Based Approaches. 1st International Workshop WL Information Systems, 4th International Conference on Enterprise Information Systems, 2002.

[2] da Silva, A., Martins, M., Rocha, B., Loureiro, A., Ruiz, L., and Wong, H. Decentralized Intrusion Detection in Wireless Sensor Networks. Proceedings of the 1st ACM International Workshop on Quality of Service & Security in Wireless and Mobile Networks. 2005.

[3] Deng, H., Li, W., and Agrawal, D. Routing Security in Wireless Ad Hoc Networks. IEEE Communications Magazine (October 2002) 70–75.

[4] Forrest, S., Hofmeyr, S. Immunology as Information Processing. Design Principles for Immune System & Other Distributed Autonomous Systems. Segel and Cohen, eds. Oxford University Press, 2000. pp361-387.

[5] Kachirski, O., and Guha, R. Effective Intrusion Detection Using Multiple Sensors in Wireless Ad Hoc Networks. Proceedings of the 36th Hawaii International Conference on System Sciences. 2003.

[6] Man, M. and Wei, V., A Taxonomy for Attacks on Mobile Agent. Proceedings of International Conference on Trends in Communications, Volume: 2, 2001, pp. 385-388.

[7] Manikopoulos, C., and Papavassiliou, S. Network Intrusion and Fault Detection: A Statistical Anomaly Approach. IEEE Communications Magazine. October 2002. pp 76-82.

[8] Patwardhan, A. Parker, J., Joshi,A., Karygiannis, A., and Iorga,M. Secure Routing and Intrusion Detection in Ad Hoc Networks, Third IEEE International Conference on Pervasive Computing and Communications, Kauaii Island, Hawaii, March 8-12, 2005.

[9] Sarafijanovic, S. and Boudec, J., An Artificial Immune System Approach with Secondary Response for Misbehavior Detection in Mobile Ad-Hoc Networks. TechReport IC/2003/65, EPFL-DI-ICA, Lausanne, Switzerland, November 2003.

[10] Sarafijanovic, S. and Boudec, J., An Artificial Immune System for Misbehavior Detection in Mobile Ad-Hoc Networks with Virtual Thymus, Clustering, Danger Signal, and Memory Detectors. International Journal of Unconventional Computing, Vol 1, pp. 221-254. Feb 2005.

[11] Zhang, Y., Lee, W., and Huang, Y., Intrusion Detection Techniques for Mobile Wireless Networks. Wireless Networks Vol 9, pp 545-556. 2003.

Kenneth Edge received the B.S. and M.S. degrees in Electrical Engineering from The United States Air Force Academy, Colorado Springs, CO in 1993 and Wright State University, Dayton, OH in 1998, respectively. He is currently pursuing his PhD in Electrical Engineering at The Air Force Institute of Technology, Wright-Patterson AFB, OH. His research interests include software and network security, advanced algorithms, auto-immune systems, and VLSI design. He is a Student Member of the Institute of Electronics and Electrical Engineers (IEEE).

Gary B. Lamont received the B.S. degree in physics and the M.S.E.E. and Ph.D. degrees from the University of Minnesota, Minneapolis, in 1961, 1967, and 1970, respectively. He is currently a Professor of Electrical and Computer Engineering at the Air Force Institute of Technology, Wright-Patterson AFB, OH, where he directs the parallel and distributed computing and the evolutionary computation research groups. Previously, he was an Engineering Systems Analyst for the Honeywell Corporation for six years. He has authored or coauthored a book, several book chapters, and over 100 papers. His current research interests include parallel/distributed computation, evolutionary computation (genetic algorithms, evolutionary strategies), combinatorial optimization problems (single objective, multiobjective), formal methods, software engineering, digital signal processing, intelligent and distributed control systems, computational and numerical methods, and computer-aided design. Dr. Lamont is a Senior Life Member of the Institute of Electronics and Electrical Engineers (IEEE).

Richard A. Raines is Director, Center for Information Security Education and Research (CISER) and Associate Professor of Electrical Engineering, Graduate School of Engineering and Management, Air Force Institute of Technology (AFIT), Wright Patterson Air Force Base, Ohio. Dr. Raines earned a B.S. degree in Electrical Engineering from The Florida State University in 1985, with honors. He earned a M.S. degree in Computer Engineering from AFIT in 1987 and a Ph.D. in Electrical Engineering from Virginia Polytechnic Institute and State University in 1994. Dr. Raines has authored or co-authored more than 70 technical publications in the areas of computer and satellite communications, communications theory, vulnerabilities of communication systems, and communication protocol analyses. Dr. Raines is a Senior Member of the Institute of Electronics and Electrical Engineers (IEEE).