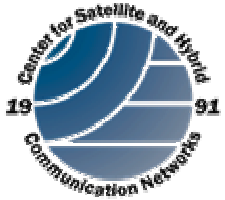


Center for Satellite and Hybrid Communication Networks

Distributed Immune Systems for Wireless Networks Information Assurance

John S. Baras

University of Maryland College Park

Kick-off Meeting CIP/SW URI
ARL
April 23-24, 2001

Overview/Summary

- **A program of:**

  theoretical and experimental investigation of the fundamental principles that should govern information assurance systems for large heterogeneous wireless networks, with changing topology and connectivity
- **Mobile wireless networks with**
  - high degree of **self-organization**
  - great variety of user **intermittent connectivity** profiles
  - **severe** communication link bandwidth, node processing capabilities, intermittent connectivity, and energy consumption **constraints**
- **Research Aim: produce 'robust' information assurance systems;**
  - maintain assurance even under high levels of noise and node capture or destruction

Theme

Theme of our research program:

- Development of innovative distributed methods and algorithms that can take advantage of the special characteristics of wireless networks and use them to improve assurance and security, while at the same time keeping their disadvantages inherent in wireless media to minimum
- As such our key ideas are often counter-intuitive
- Plan to use sophisticated analytical methods supported by selective experimentation and testbed validations to demonstrate and support our claims and results

Problems Addresssed

Plan to investigate following problems in an integrated manner:

- automated vulnerability assessment
- automated compromised subnetwork containment
- pro-active intrusion and anomalous behavior detection
- automated classification of intrusions and anomalous behavior patterns
- automated and distributed storage and distribution of intrusion and anomalous behavior patterns
- autonomous deployment of passive/active methods for intrusion defense
- autonomous deployment of schemes assuring continuous operation at acceptable assurance levels
- trade-off analysis between detection performance and false positives *vs* complexity and speed of response
- robustness and resilience of the proposed assurance schemes
- integration of transmission and traffic flow security with key generation/management and authentication

Integration Means

This integration will be achieved by innovative ideas and schemes that focus on the following principles:

- **Distributed automatic classification of intrusions in real-time**
- **Automatic generation of responses for containing and nullifying an intrusion faster than it spreads**
- **Attacking intrusions close to the 'network edge'**
- **Utilization of synergy between physical layer and network layer assurance schemes**
- **Hierarchical methods and schemes in both the physical and logical domain for efficiency and scalability**

Motivating Ideas

Motivation from:

- Operational principles of biological immune systems
- Recent successful development of 'digital immune systems' for the protection of commercial networks from virus attacks
- Recent advances in complex waveform generation which can be profitably utilized to secure wireless communications in a variety of yet unexplored ways

Cross-Disciplinary Research Team

Team of researchers covers a wide range of expertise and disciplines

- *John Baras* (ECE, CS, ISR): network security, pattern classification, intelligent systems and dynamic games, distributed detection and estimation under communication constraints, learning, neurodynamic programming, stochastic systems
- *Carlos Berenstein* (Math, ISR): complex variables, algebraic geometry, mathematical complexity, algebra and cryptography, algebraic number theory, network security
- *Anthony Ephremides* (ECE, ISR): wireless mobile networks, self-configuring networks, network security, energy efficient routing, information theory, multi-user detection
- *Virgil Gligor* (ECE): network security, cryptography, distributed systems
- *Ray Liu* (ECE, ISR): adaptive signal processing, smart antennas and array processing, multimedia signal processing, time-frequency signals
- *Babis Papadopoulos* (ECE, ISR): distributed signal processing algorithms, nonlinear and chaotic systems for signal processing and communications, physical layer algorithms for wireless communications, redundant and reliable communications
- *Nick Roussopoulos* (CS, UMIACS): database management, distributed databases, query optimization, object-relational databases, fast computation of aggregates, adaptive data broadcasting, network management

Principal Goals

Team of experts will undertake a concerted effort to achieve two goals

- **First:**

  develop the theoretical framework and to abstract the underlying principles of self-organizing network behavior and signal processing that can endow mobile wireless networks with an autonomous distributed immune system for information assurance

- **Second:**

  apply these principles and demonstrate them in realistic wireless network testbeds

Challenges and Opportunities

- **Wireless mobile networks are**
  - pervasive in the military
  - becoming ubiquitous in the commercial world
- **They now can carry multimedia and the available bandwidth is rapidly increasing. Internet-type services can now be offered over wireless networks**
- **Military mobile networks present major challenges because:**
  - they have typically rapidly changing topologies
  - intermittent connectivities
- **Traditional thinking suggests that network security and information assurance will be very weak over wireless mobile networks**
  - This is due to a great extent to the perceptions about the wireless medium
- **These problems become even more challenging in wireless environments with limited bandwidth, connectivity, energy**
- **Nevertheless, advances in signal processing, waveform design, network algorithms and architectures**
  - offer opportunities for the development of high quality information assurance and network security schemes for mobile wireless networks
  - This is the principal thesis of our research program

Exploiting Waveform Design

- Waveform design has produced advanced signal constellations, waveforms used in dense multi-user environments, and other signal construction methods that permit us to detect signals in very weak signal to noise environments and even more so if we have information about them that our adversaries do not have
- These developments allow the generation of signals that are practically undetectable, the creation and use of CDMA like schemes using large numbers of codes, and the rapid variation and distribution of these codes for adaptive operation and more importantly for our goals for dynamic security and assurance
- Furthermore the noise in the wireless channels can be effectively used to mask communications, routing information etc.
- Techniques such as OFDM, and its extensions into dynamic and adaptive waveform generation offer even more opportunities

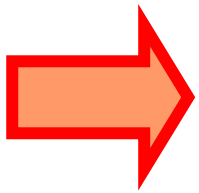
The vision is that through sophisticated signal design, and rapid and dynamic variation, we can "lock" the wireless channel for use only by designated users

Exploiting Network Architectures and Multicasting

- **Multicast and group communications are becoming pervasive in both military and commercial networks**
- **Wireless networks offer natural advantages and efficiencies when it comes to multicasting**
- **In addition wireless networks offer multiplicity of paths or diversity, which can be controlled and exploited for security and information assurance advantages**
- **Inspired by the operation of the human immune system, we propose to develop sophisticated techniques for intrusion detection and correction which exploit the advantages of wireless media**
- **For example corrective "vaccines" can be broadcast fast to numerous users in a wireless network, thus helping stop the intrusion at a boundary close to the network edge**
- **Similarly adaptive and dynamic routing and access schemes can be designed that exploit the nature of the wireless networks**

Research Program Organization

Combination of these two key motivating ideas



Variety of interconnected and integrated schemes for network security, authentication and information assurance

- Research program is organized along three closely interrelated thrusts:
  - (1) Distributed Autonomous Immune Systems
  - (2) Assurance Via Distributed Physical Layer Signal Processing and Routing
  - (3) Distributed Computing Formalisms and Systems
- Research on methods, algorithms, modeling and analytical methods will be supported by:
  - mobile wireless network simulation testbeds
  - real experimentation with mobile wireless network testbeds

Thrust (1) : Distributed Autonomous Immune Systems

- *Fast innate and adaptive immune systems*
- *Group authentication and multiparty key protocols in dynamic groups*

Fast Innate and Adaptive Immune Systems

- Develop systems for information assurance capable not only to provide authentication and security but also to detect and defend against information assurance attacks

- Principal objective for this research is to develop a distributed intrusion and anomalous behavior detection system that can detect such abnormal network behavior early on, and as close as possible to the first node(s) that has(ve) been attacked or compromised

- The system then will autonomously generate a response to either isolate temporarily the compromised components or to attack and nullify the effects of the intrusion attack and re-establish normal operations

Fast Innate and Adaptive Immune Systems

- **The proposed 'immune system' will in general have two components and the key properties outlined below:**
- **An 'innate immune' component which must be capable of detecting in a distributed manner the presence of a high proportion of intrusions that are unknown to it specifically**
  - The system should recognize previously unknown intrusions and attacks of all types, including file infectors, masquerading, denial of service, etc.
  - This innate component detects *broadly defined* components or parts of an intrusion attack or anomalous behavior
- **An 'adaptive immune' component which should be capable of automatically deriving from a single sample of anomalous behavior a 'prescription' for detecting and, if possible, removing or nullifying all instances of the intrusion or anomalous behavior**
  - The detections and classifications performed are of the type needed *to identify specific intrusions* or abnormal behaviors
  - The system must deliver this prescription to the afflicted node(s) and must also facilitate dissemination of the prescription to other nodes both in the neighborhood and in the entire network at large
  - The system must be capable of detecting an intrusion and deriving and disseminating prescriptions on a time scale faster than the intrusion or anomalous behavior can spread

Fast Innate and Adaptive Immune Systems

- Develop methods and algorithms for extracting key strings of bits that characterize various intrusion and anomalous behavior patterns
- Will be accomplished (as in modern virus detection and defense systems) by capturing fast instances of anomalous behavior, represented by sequences of events or program strings, and quickly perform simulation experiments in order to identify the minimum length digital signature of the intrusion attack
- Research in new parallel algorithms that can perform very large numbers of normal/abnormal tests and able to identify the common digital signature of polymorphic attacks
- Learning methods based on the powerfull and scalable Support Vector Machine (SVM) algorithms, which have proven very useful recently in DNA partial sequence matching and proteomics
- Innovative methods for learning and knowledge representation using techniques such as neurodynamic programming and Q-learning

Fast Innate and Adaptive Immune Systems

- Key steps in discovery, development and implementation of such a system :
  - (1) Fast discovery of a previously unknown intrusion pattern or anomalous behavior pattern on a network node
  - (2) Capturing a sample of the behavior or pattern and sending it to one of the distributed nodes capable of analyzing the sample
  - (3) Automatic classification and analysis of the pattern in order to identify its 'minimal' signature and a prescription for detecting it and removing or nullifying it from any host node
  - (4) Delivery of the prescription to the affected network node, updating the distributed databases which store such intrusion and anomalous behavior pattern information, and executing the strategy described in the prescription to detect and nullify all occurrences of the intrusion
  - (5) Disseminating the prescription to other nodes in the vicinity of the affected node and to the rest of the network

Group authentication and multiparty key protocols in dynamic groups

- Mobile wireless communication networks for the Army will offer communication services for collaborative applications of all kinds to so-called dynamic peer groups (DPG)
- In contrast to multicast groups, DPGs tend to be smaller (involving a hundred or a few hundred members), flat (*vs* the hierarchical groups often encountered in multicast communications), and employ many-to-many communication patterns (*vs* the one-to-many communication patterns prevalent in multicast communications)
- Key management and authentication for DPGs is a challenging open problem
- Investigate these problems under the additional requirement of good performance under rapid changes in the network topology, group membership and severe bandwidth and energy constraints

Group authentication and multiparty key protocols in dynamic groups

- **Develop distributed algorithms that do not rely on the existence of centralized completely trusted third parties: the so-called key agreement type of key management**
- **They involve two phases: an initial key agreement phase and an auxiliary key agreement phase**
- **Diffie-Hellman extensions to groups of any size, including authenticated key agreement protocols have been previously developed**
- **Principal advantages of DH are that they:**
  - do not need a trusted third party
  - work with ***adhoc*** mobile networks
  - provide fresh and random group keys
  - provide key independence
  - perfect forward secrecy
  - resistance to known-key attacks
  - key confirmation and integrity

Group authentication and multiparty key protocols in dynamic groups

- Main drawback: their computational complexity and inefficiency in dynamically changing groups
- Develop improvements of these promising schemes using techniques such as the ones we recently developed (fractional keys), which are efficient, low complexity and amenable to distributed implementation
- Investigate information assurance for both large multicast groups as well as smaller DGPs using these methods
- Key goal is to provide distributed, highly efficient key generation and management algorithms that can cope with rapidly changing group membership (handle the re-keying problem efficiently)
- Investigate logical tree keying, key multicasting and key caching

Thrust (2): Assurance via Distributed Physical Layer Signal Processing & Routing

- *Advanced signal processing for channel and communication assurance and authentication*
- *Wireless multimedia security, authentication, and dynamic key management*
- *Use of covert channels*
- *Simultaneous selection of access control and routing*
- *Securing mobile adhoc networks*

Advanced Signal Processing for Channel & Communication Assurance & Authentication

- Orthogonal frequency division multiplexing (OFDM) and other advanced time-frequency modulations offer an opportunity to secure wireless channels and at the same time authenticate users of these channels
- Analogy with CDMA: these waveform modulations provide a method to identify users by their code (or time-frequency pattern)
- Investigate such waveform techniques as means for channel security and user authentication.
- Develop distributed algorithms for authentication signaling
- Investigate combinations of such algorithms with secure routing (see below) for *adhoc* networks
- Dynamic re-distribution algorithms to prevent compromise of authentication
- Key challenge is reduction in computational complexity and achieving great efficiency under conditions of rapid group dynamics
- Investigate the combination of these algorithms with the use of position information (such as GPS) for improved and more robust authentication and identification

Wireless Multimedia Security, Authentication, and Dynamic Key Mngment

- Secure multicast communications: a common session key needs to be updated whenever there is member addition or deletion
- Scalable session key distribution techniques for dynamic groups has been a challenging problem
- Most such schemes do not make use of the special properties of multimedia signals
- Develop a new paradigm to multicast security by showing how secure multicasting may be established by exploiting the properties of the data that is being sent
- Rather than treating all data as generic, we consider the scenario where the data is for multimedia services
- We consider multimedia data as having special characteristics, which make it suitable for conveying the messages, associated with membership registration and deregistration
- Multimedia data is suitable for data embedding, which is the almost invisible hiding of extra information in the data structure

Wireless Multimedia Security, Authentication, and Dynamic Key Mngment

- By using data embedding, key updating messages associated with secure multicast key management schemes may be hidden in the data and used in conjunction with encryption to protect the data from unauthorized access
- The key message is seamlessly distributed in the encrypted bit stream, which makes it much more hard for the attacker to break the system
- Achieve improved scalability by employing a tree-based algorithm to update the SK and KEKs; map the scheme to a tree structure for scalable framework
- A non-balanced tree employing one-way functions can be used in a key management scheme allowing member joins and departures
- Consider the balance between computation, communication, and storage resources
- Need for using a tree-based key distribution scheme becomes more pronounced as the group size increases; the O(log n) communications needed by most tree-based schemes makes the use of a tree-based scheme essential when the group size is several thousand or more users
- Another issue that should be considered is the amount of storage needed by the GC and each individual user

Use of Covert Channels

- **Covert channels offer a powerful alternative for enhanced security**
- **The wireless medium provides new and natural opportunities for the implementation of covert channels; a wireless network can counter a variety of threats through covert message exchange**
- **Covert communication can be used in many ways**
  - can provide alternative means for authentication or message protection
  - can verify sensitive protocol information
  - can assist the reconfiguration of the network in post- or pre-attack conditions
  - can provide a totally secure, undetected means of message exchange.
- **Wireless medium offers unique opportunities for covertness (despite its ubiquitous availability to multiple users) example**
  - Suppose that a collision resolution algorithm is used for interference control in a contention-based media access control (MAC) protocol
  - requires an orderly schedule of retransmissions among cooperating users
  - result in a pattern of subsequent collisions, whose number diminishes gradually until all competing messages are successfully transmitted
  - a covert transmitter (in collusion with the covert receiver) can cause at will as many spurious collisions as it wishes
  - their total number in any given collision resolution period carries covert information that only the intended receiver can decipher

Use of Covert Channels

- As the covert communication process takes place, the apparent profile of the channel traffic is essentially the same as in a covert-free mode of operation
  - Thus, it becomes difficult to detect
- Implementation of a covert channel is only one of many aspects of the channel that must be examined
- Need to evaluate rate at which it can relay information, as well as its bit error rate
- These performance components of a covert channel are needed to establish its suitability for specific uses, that have their own requirements
- Our research will identify several alternative wireless covert channels and will evaluate:

  1) The quality-of-service they are capable of in terms of bit error rate and capacity

  2) The application for which they are appropriate

  3) The possibility of their detection by unauthorized users

Simultaneous Selection of Access Control and Routing

- When an intrusion or a threat is detected, one way to protect the information and the network and to ensure its delivery is to reroute or reassign resources in response to that threat
- Can define a very concrete measure that simply assesses the "state" of each packet transmission at each hop: a binary state (i.e. satisfactory or failed), or a more elaborate one
- Based on that measure, the assignment of resources to each link (say, the bandwidth) is adjusted up or down (at the expense or benefit of those assigned to other links that share these resources)
- As a result, the actual performance on that link (as measured, say, by delay) changes and forces a shift in the value of that link's metric as it is used in whatever routing algorithm is employed
- This results in a rerouting, which in turn yields different bandwidth needs for the original links, which are, in turn, adjusted appropriately

Simultaneous Selection of Access Control and Routing

- Problem can be formulated in a TDMA, FDMA or CDMA fashion
- Important for QoS-aware high-data-rate applications
- Simple model: *N* nodes that form a "clique" share an bandwidth *B*
- *B* can be thought of as a frame of *B* time slots, which recurs regularly, and that must be allocated according to some criterion to each of the *N* nodes
- The initial assignment of the slots to the flows are assumed to be in accordance to their rate and QoS requirements; i.e. the available bandwidth is sufficient for the demand and no bandwidth is left unassigned
- As time goes by, the successful transmissions do not equal the allocated slots and thus there will be throughput "lags" for some flows
- These can be compensated for at the next frame (at the expense, though, of other flows which will start "lagging" also as the compensated ones catch up or even "lead" over their required rates)
- Thus, an iterative, frame-by-frame, allocation will be assigning different numbers of slots to the different flows at each node based both on the required values and on the channel behavior during the preceding frame (which can be very uneven, affecting each flow differently)
- To effect a proper scheduling/allocation process, we will use a Link-Error-Adjusted-Rate (LEAR) measure

Simultaneous Selection of Access Control and Routing

- This allocation awards slots proportionately to the sum of the average need plus the encountered lag for each flow; alternative methods are possible
- Queues start building up at the buffers reserved for each flow at each node; these queues do not build up uniformly among all nodes and flows
- How to reroute the packets that are encountering long delays in their currently allocated routes?
- Potential arises not only to couple the layers (physical, link, and network) but also to resolve the fundamental issue of jointly solving the access and the routing problem in *adhoc* networks
- Consider the "clique" of the N nodes, that share the bandwidth B embedded in a large, multi-hop network, where each flow has a source-destination pair
- Must be able to organize the network in cliques of that type that are interconnected (and possibly overlapping) and to resolve the issue of how bandwidth is allocated among cliques in a non-interfering fashion
- Coupling access control and routing: "lag" values become natural measures of delay on link for each flow
- Based on this measure, a routing algorithm of any choice can re-compute routes

Simultaneous Selection of Access Control and Routing

- The recomputed routes provide new values to the rates in the clique: at the next iteration provide new target points or equilibrium in the allocation of the *B* slots
- This successive interaction, from frame-to-frame, between the route selection, that determines the required flow, and the bandwidth allocation, is at the heart of our methodology for a joint routing/access resolution
- This simple iteration cycle exemplifies an adaptive way of adjusting the network resource allocation in response to any changes whatsoever (i.e. jamming, channel fades, mobility, or whatever else)
- The end result is far-reaching: it permits an implementable solution framework for the the simultaneous choice of access control and routing
- All work to date has either assumed fixed routes and hence fixed traffic demands on each link and hence a solution to the access problem or, conversely, a fixed allocation of access, thereby defining a metric on the links and solving the routing problem
- To implement this idea, one needs to solve an associated problem of obtaining "cliques" of nodes in the *adhoc* network on which then to apply this iteration
- We will solve the clique problem (preferably in a distributed way) and resolve the issue of coordinating the allocations at each clique
- The resulting schemes will be evaluated in different threat scenaria

Securing Mobile *Adhoc* Networks

- The salient features of *adhoc* networks provide both challenges and opportunities for security and information assurance system design and implementation
- To achieve high survivability *adhoc* networks must have a distributed architecture with no central entities
- Trust relationships between nodes in an *adhoc* network change dynamically: security mechanisms must be able to adapt on the fly to these changes
- To balance these challenges *adhoc* networks offer the advantage of *redundancies* (i.e. multiple routes between nodes) and *distribution of trust* (i.e. collaborative trust establishment via a set of nodes using partial secrets to establish a common secret)
- The key generation and distribution systems we developed recently can be used in *adhoc* networks
- Develop new distributed security and information assurance systems for *adhoc* networks by combining techniques from: routing redundancies, secure routing, diversity coding (i.e. transmit redundant information through multiple paths for improved intrusion detection and recovery), key generation and management systems that are robust and individually confidential (common key is computed in collaboration from partial keys of members of the group, using combiners), frequent share refreshing as a means for proactive defense against mobile intruders, asynchronous operations

Thrust (3): Distributed Computing Formalisms and Systems

- *Formal methods for intrusion models*
- *Algebraic methods and complexity*
- *Dynamic topology discovery and network tomography*
- *Distributed trust models for mobile wireless networks*
- *Active distributed databases, caching and prefetching of intrusion pattern models*
- *Cooperative intrusion detection databases with aggregates on a shadow security network*

Formal Methods for Intrusion Models

- **Develop systematic techniques for categorizing/analyzing intrusions and abnormal behaviors**
  - plan substantial research in formal methods for the representation, testing and storage of intrusion patterns and anomalous behavior patterns
- **Within telecommunications community particular attention to three standardized formal description techniques: LOTOS, Estelle and SDL**
  - primary application has been protocol specification and validation
  - recently communication services were modeled using formal methods and models used with field data to validate service behavior and quality
- **Offer several advantages for problems of intrusion detection and information assurance; Plan to use formal methods to represent:**
  - security and assurance policies
  - communication protocols and processes
  - intrusion patterns
  - anomalous patterns
  - normal patterns
  - prescriptions for restoring normal operations
  - various strategies for defense against information assurance attacks

Formal Methods for Intrusion Models

- **Investigate these problems through formal method techniques such as:**
  - FSM (finite state machine)
  - SDL (specification and description language)
  - LOTOS (language of temporal ordering specification)
  - Estelle (extended finite state machine language (EFSM))
  - Esterel (a synchronous programming language)
  - Temporal Logic (a formal specification language for the description and analysis of time-dependent and behavioral aspects)
  - Linear time temporal logic (LTL)
  - Action-based temporal logic (ACTL*)
- **Combine use of formal models and parallel clustering algorithms of the Support Vector Machine (SVM) type, to develop fast distributed algorithms for identification of components of intrusions & abnormal behaviors**
- **Inspired from similar successful combination of formal (logic) models and SVM in genomics and proteomics, and in particular for the problem of partial identification using side logical information**

Algebraic Methods and Complexity

- **Investigate problems of complexity (i.e. feasibility) for several of the proposed key management schemes and other authentication protocols for dynamic peer groups, as well as for general networks**
- **Our approach: most reasonable schemes amenable to two types of analysis**
  - asymptotic methods
  - reduction to solvability of systems of algebraic equations in several variables, (Nullstellensatze)
- **Have unique experience and record in these areas**
  - completed complexity of Nullstellensatze; optimal estimates for solvability of systems of multivariable algebraic equations over fields with arbitrary characteristic
  - sharp estimates: every complexity problem with polynomial equations reduced to this
  - analytic methods, using multidimensional residues, to compute Arakelov measures and associated invariants (essential in algebraic factorization problems)
- **Provide mathematical tools to analyze the Diffie-Hellman key protocols or construct new ones: advances in key generating protocols**
- **Methods, being a combination of analytic and number theoretic tools, will provide sharp complexity estimates, and help find new algorithmic solutions**

Dynamic Topology Discovery and Network Tomography

- **Problem of understanding the topological nature of the *ad hoc* networks created by dynamic groups, and provide tools for the study of other large, variable configuration networks like the Internet or the Tactical Internet**
- **Purpose is to detect attacks on the integrity of the system early on**
- **Recent work indicates that this problem may be amenable to study using tools that were developed by members of our team in a different context**
- **Analysis of the behavior of the Internet and similar networks can be approximated by tomography on trees**
  - a line in a tree is the shortest path between two points; rules out closed circuits
  - the length of a "segment" is just the number of nodes between the initial point and the arrival point, plus one
- **Tomography is the use of the Radon transform in trees:**
  - a function f on the (nodes of the) tree; l a line
  - $Rf(l)$ is the sum of the values of f along the nodes of the line
- **There are inversion formulas for the Radon transform on trees: they involve the discrete analog of the Laplace operator**

Dynamic Topology Discovery and Network Tomography

- **Use boundary value problems for the discrete Laplacian to detect perturbations in signal traffic corresponding to intrusions or other attacks on system integrity**
- **Diagnosis of such perturbations of the network is akin to EIT (Electrical Impedance Tomography) in the context of a tree or more generally, graphs**
- **EIT an inverse problem: Find out the conductivity of a material plate from the boundary measurements of the voltage induced by currents introduced on the boundary, for instance, dipole patterns**
- **Our earlier work demonstrated relation between tomography and EIT**
  - EIT can be analyzed using the Radon transform in the hyperbolic plane, that is, the integration is performed along the geodesics of the hyperbolic metric
  - Harmonic analysis in the hyperbolic plane and harmonic analysis in trees are closely related
- **Plan to study this connection to obtain a method to monitor network traffic and produce early detection of hostile intrusions or disruptions**
  - Particularly interested in the development of fast distributed algorithms that can track network topology on-line
  - Also particularly interested in fast distributed algorithms that can monitor for partial intrusions in networks with rapidly changing topologies
- **Radon transform methods and their approximations are amenable to such distributed and fast implementations; setting here is completely nonconventional**

Distributed Trust Models for Mobile Wireless Networks

- **Original use of public key certificates was to securely bind a user's name to his public key: a means of authentication**
  - This use was adopted by X.509 Version 1, and PGP certificates
- **Components that provide authentication or confidentiality comprise not only the software, the hardware, and the network that enable the user nodes to communicate, but also the established security policies, procedures, and infrastructures used by the various parties**
- **Establishment of trust in the certification process, and through it between users can be established by the deployment of a trust model: PGP and PEM/X.509 are well-known trust models**

Distributed Trust Models for Mobile Wireless Networks

- **For mobile wireless networks there is great need for distributed trust models that have the following properties:**
  - **capable to operate without using certificates or CRLs**
  - **allow for the creation of security domains encompassing single individuals, multiple users, arbitrarily complex organizations**
  - **allow for organic growth among the users and organizations**
  - **allow security domains to grow, shrink or reorganize at any time**
  - **allow users and/or the administrator of a security domain to choose which other domains are to be trusted**
  - **the operation of the trust model as a whole should not depend on the existence and operation of any single part of the deployed infrastructure**

Distributed Trust Models for Mobile Wireless Networks

- **Investigate trust models formally and develop methods for designing trust models with these properties for mobile users connected through wireless networks**
- **These new trust models should**
  - incorporate the best features of the PGP, PEM and SPKI trust models
  - be capable for operation in a mobile tactical Internet environment
- **Investigate extensions of the IPsec suite of protocols, to mobile wireless networks employing at least clustered mobile-IP routing policies**
- **Investigate the extension of the Internet Key Exchange (IKE) protocol to mobile wireless networks**
- **Develop new IPsec models**
  - appropriate extensions of IKE/ISAKMP/OAKLEY/DOI (using both Diffie-Helmann, and algebraic-curve-based key exchanges)
  - defenses against flooding attacks & other well known vulnerabilities of the IPsec
- **Develop new distributed key negotiation, and key derivation algorithms for mobile networks**
  - Important part: development of efficient rekeying & retransmission strategies

Active Distributed Databases, Caching & Prefetching of Intrusion Pattern Models

- For efficient & fast intrusion detection the network has to employ reference models for various intrusion and anomalous behavior patterns
- Where in the network are these models stored?
- How are they moved around the nodes in response to the evolving intrusion or information assurance attack?
- Develop mechanisms for distribution of these reference models, and for efficiently moving them around the network
- Development of algorithms that can prefetch such reference models based on the past history of the algorithm and current estimates/detections from various nodes
- Develop databases of belief networks as distributed depositories of learned intrusion and anomalous behavior patterns
- These databases will be used via decision theoretic dynamic methods for the development of prescriptions to nullify intrusion effects
- These methods lead to systematic design and implementation of asynchronously operating software agents

Cooperative Intrusion Detection DBs with Aggregates on a Shadow Security Network

- **Intrusions follow well-defined patterns which can be detected using pattern matching techniques on audit-trail information stored in system**
  - E.g. series of attempts to login to a system or to "setid" inside a program can be detected by examining log messages resulting from system calls
- **Anomalous intrusions are detected by observing significant deviations from normal behavior**
- **Pattern matching approaches or techniques based on anomalous conditions detection using metrics determining normal from abnormal behavior have been applied for intrusion detection**
- **Although such techniques provide various degrees of security, in large heterogeneous wireless networks they fall short as there is no centralized audit-trail system that logs access and usage behavior that can be accessed in real-time to do the detection**
- **The logs are distributed, heterogeneous, and the intermittent connectivity prohibits real time access for such detection.**

Cooperative Intrusion Detection DBs with Aggregates on a Shadow Security Network

- **Develop a "shadow security network" (SSN):**
  - a substrate of wireless network for real-time delivery of log patterns, statistics, and control messages to the various nodes responsible for the security of a subnetwork
  - SSN is an independent orthogonal network channel that could either run on its own platform or can be multi-plexed with the normal data channels
  - Its whole purpose is intrusion detection and prescription (vaccine) for defending an attack.
  - SSN is a "broadcast" network delivering security data
- **A Cooperative Intrusion Detection Database (CID2) consists of patterns observed, statistics aggregated by individual nodes, statistics observed across multiple nodes, and prescription to remedy attacks**
  - CID2 will completely reside on the SSN and its pieces will continuously be distributed as a "broadcast" program

Cooperative Intrusion Detection DBs with Aggregates on a Shadow Security Network

- **Architecture of the SSN: each participating node consists of a Monitor, an Aggregator, a Broadcaster, and a Cache Storage**
  - Monitor observes statistics on the SSN channel and decides which of these are considered an intrusion
  - uses the Aggregator to compute new aggregates; specifically, the Aggregator combines the broadcast statistics received with local statistics from the node logs, updates the local cache, and passes them to the Broadcaster
  - The Broadcaster schedules them into its broadcast program along with possible prescriptions for the SSN
  - Broadcaster should have the ability to prioritize the SSN broadcast channel because its broadcasts have an impact on the global delivery of the SSN and the security it provides
  - The Monitor is also capable of executing prescriptions for either defending an attack or for invoking the Aggregator to start a new aggregation of statistics with a different accumulation point or even a totally new aggregate view of the network

Cooperative Intrusion Detection DBs with Aggregates on a Shadow Security Network

- **Two key technologies required and exploited in the SSN architecture are:**
- **Adaptive Data Broadcast**
  - new technology of broadcast channels using concept of "aircache": broadcast data program is a fast and very-wide network storage media which can scale to millions of clients
  - scalable and economical method for data dissemination under normal use of network storage
  - 1000 plus fold scalability for situations of "panic"
  - aircache channel is hierarchically organized: most important (or latest) have higher priority than those of less important (or stale)
  - channel division is configurable to the application's requirements
- **Rapid Aggregation of Data**
  - Intrusion detection will rely on rapid aggregation of data to be compared against patterns
  - Aggregation of the statistics are not complicated algorithms
  - Detection uses data mining algorithms which require an incredible number of aggregations
    - "restarts" of the aggregations- meaning new starting point of the aggregates
    - "on-the-fly" new views of aggregations- a different slice of the system logs
  - Logs are evolving at very high rates: aggregation has to be done "incrementally" and in "bulk" to keep up with the rate of updates
  - Cubetree Storage Organization offers this: "merge" operations instead of "in-place" updates
  - Merge of updates into the aggregates is the fastest possible algorithm as it is linear in the input that needs to be maintained

Cooperative Intrusion Detection DBs with Aggregates on a Shadow Security Network

- **A scenario of the SSN:**
- **Each node maintains its own aggregates on access, resource usage, picture of the status of the network, patterns of accesses that constitute normal behavior, intrusion patterns, etc.**
- **Aggregates which refer to other nodes are broadcast to the SSN**
- **Monitor monitors aggregates delivered by the SSN: if they involve resources of the received node, they are combined with the local log aggregates and broadcasts the result**
- **Although the local aggregates cannot detect an attack, the global ones will**
- **When a potential intrusion risk is detected, a prescription is broadcast through the SSN**
- **Prescription could degrade the access to a reduced level, or take additional actions or set up a "watch dog" to pay attention to potential intruder or completely shut off intruder**
- **Upon receipt of a prescription, the node protects its own resources by appropriate actions**
- **One of most frequent prescribed actions is that of dispatching a "watch dog aggregate"**
- **Upon suspicion of some anomaly, a number of new aggregates must be computed to determine whether it is a real danger or an artifact**
- **SSN does not carry complete logs: partial aggregates are computed by the node posting the threat using its own logs**
- **Priority broadcast pushed through the SSN allowing all the nodes to contribute their piece of knowledge and forward to others until puzzle is complete: proves a threat or an artifact**
- **Unlike agent and AI based classification techniques (fall short in performance and scalability) cooperative aggregation through the SNN substrate is a radically different technology; provides real-time performance and scalability for wireless networks**

Deliverables

- Technical reports
- Algorithms for network security
- Algorithms for network vulnerability assessment
- Algorithms for intrusion detection and correction
- Algorithms for information assurance
- Algorithms for signal construction
- Real-time prototypical implementations of algorithms
- Performance evaluation results
- Experimental and simulation results
- Guidelines for wireless network security systems
- Guidelines for wireless network information assurance
- Extensive simulation experimentations and performance benchmarks

Schedule and Milestones

Schedule (year of the URI)

For each item algorithms and real-time prototype implementations where applicable :

- **Distributed Autonomous Immune Systems** — **Y3, Y4, Y5**
- **Fast innate and adaptive immune systems** — **Y2, Y3**
- **Group authentication and multiparty key protocols in dynamic groups** — **Y1, Y2**
- **Assurance via distributed physical layer signal processing and routing** — **Y2, Y3, Y4**
- **Advanced signal processing for channel and communication assurance and authentication** — **Y2, Y3**
- **Wireless multimedia security, authentication, and dynamic key management** — **Y2, Y3**
- **Use of covert channels** — **Y1, Y2**

Schedule and Milestones

- Simultaneous selection of access control and routing — Y2, Y3, Y4
- Securing mobile adhoc networks — Y3, Y4, Y5
- Distributed Computing Formalisms & Systems — Y3, Y4, Y5
- Formal methods for intrusion models — Y2, Y3
- Algebraic methods and complexity — Y1, Y3
- Dynamic topology discovery and network tomography — Y1, Y3
- Distributed trust models for mobile wireless networks — Y2, Y3
- Active distributed databases, caching and prefetching of intrusion pattern models — Y1, Y2
- Cooperative intrusion detection databases with aggregates on a shadow security network — Y2, Y3, Y4
- Extensive experimental and simulation performance results — Y4, Y5

Expected Outcome and Impact

A research program in the discovery, design and evaluation of distributed autonomous systems for information assurance in large heterogeneous wireless networks

This focused research effort will yield:

- **Fundamental understanding of the general principles that can endow such information assurance systems with superior performance**
- **Methods and algorithms to evaluate trade-offs between intrusion detection, false positives, complexity, energy and bandwidth constraints, latency and processing capability**
- **Methods and algorithms for efficient key generation, management and authentication for group collaboration and communications**
- **Automatic schemes for isolating, diagnosing and nullifying intrusions on mobile wireless networks**

Impact on Academic Research & Education

- **Research Program will bring together:**
  - A leading team of experts on problems of wireless communication networks with rapidly changing topology and connectivity, network security, signal processing, pattern classification, distributed computing,
  - Army scientists and engineers
  - Industry engineers from leading defense companies
- **These interactions and collaborative efforts will increase substantially the ability of the University of Maryland College Park to contribute to DoD relevant research, education due to the increased awareness of interesting problems**
- **Large portion of the requested funds will be devoted to the support of graduate and undergraduate research students: some 14 graduate students will be involved in the proposed effort each year**

Complementary Research

- **URI research program very complementary to on-going research at the University of Maryland College Park**
- **Existing and on-going efforts include:**
  - Several single investigator ONR grants on wireless networks
  - an NSF group project on wireless networks
  - a DARPA project on network modeling and simulation (first year of three)
  - a DARPA project on integrated security of dynamic coalitions (first year of three)
  - a NASA Center project on modeling, performance evaluation and design of hybrid communication networks (second year of five)
  - an ARL Federated Lab project (ATIRP) on Telecommunications and Infrastructure Research (last year of five)
- **URI funds are heavily leveraged**
- **Substantial support from UMCP to the URI Program**
- **Two state-of-the-art Laboratories will support the research: *Hybrid Networks Laboratory (HNL)*, *Systems Engineering and Integration Laboratory (SEIL)***

Collaborative Environment

- **Center for Satellite and Hybrid Communication Networks (CSHCN) will host the URI Program; within the Institute for Systems Research (ISR)**
  - provides a unique environment for the conduct of multi-disciplinary research
  - pioneered innovative ways to structure academia-government-industry partnerships
- **Create an industry partners team consisting primarily from companies with leading expertise and interest in mobile wireless networks and network security: Lockheed Martin Global Telecommunications, Motorola, Hughes Network Systems, Network Associates Inc., others**
  - Partners will obtain experimental algorithms and design principles from the URI researchers, which will be tested, validated and evaluated at their network testbeds
- **Further strengthen our on-going collaboration with the Army Research Laboratory and the Naval Research Laboratory**
  - Collaboration will entail both research and educational components as we will systematically seek to transfer to ARL scientists and engineers the latest results of our understanding and the theoretical principles we will discover
- **Strengthen our collaboration in this area with CECOM, other DoD Labs**
- **Annual Review Conference and Exhibition**