Research Proposal for CERIAS 2002

Trusted Routing and Intruder Identification in Mobile Ad Hoc Networks

Bharat Bhargava: Principal Investigator (CS Department)
Michael Zoltowski: Co-Principal Investigator (ECE Department)
Pascal Meunier: Co-Principal Investigator (CERIAS)
Purdue University, West Lafayette, IN 47907, USA
E-mail: bb@cs.purdue.edu mikedz@ecn.purdue.edu pmeunier@purdue.edu

We have definite plans to explore external funding for this project. We have read the policies for CERIAS-funded projects and agree to abide by them. We plan to seek funding from National Science Foundation, Army Research Lab, CISCO and INTEL. We plan to submit proposals in FALL 2002. A University Research Program (URP) proposal has been submitted to CISCO and we are finalizing research tasks with INTEL. We are working closely with ITT to develop a proposal for DoD.

1 Introduction

A Mobile Ad Hoc Network (MANET) is a collection of wireless hosts that can be rapidly deployed as a multi-hop packet radio network without the aid of any established infrastructure or centralized administration [14]. Such networks can be used to enable next generation of battlefield applications envisioned by the military [29], including situation awareness systems for maneuvering war fighters, and remotely deployed unmanned micro-sensor networks. Ad Hoc networks can also provide solutions for civilian applications such as disaster recovery and message exchanges among safety and security personnel involved in rescue missions. Several special properties lead to the uniqueness of MANET:

- Wireless media is used for communication
- Network topologies and memberships are constantly changing
- No predefined trust exists between communication partners
- Limited bandwidth, battery lifetime, and computation power prohibits the deployment of complex routing protocols or encryption algorithms

While these characteristics are essential for the flexibility of a MANET, they introduce specific security concerns that are unknown or less severe in wired networks. The proposed research will address these concerns by investigating cross-layer security as described below.

- Smart antennae will be applied to physical layer of the wireless communication to provide better performance and protection against eavesdropping.
- A new routing protocol will be designed to discover, evaluate and choose trusted routes based on multiple security metrics and to support these smart antennae.
- An intrusion detection and intruder identification system based on distributed trust suited for MANET will be designed to provide security against malicious attacks to the networks.

These mechanisms will be integrated into a system that provides secure and trusted routing for MANET. This research combines the concepts of smart antenna, intrusion detection, distributed trust, and obfuscation of relationships. The results of the proposed research will contribute to homeland security, military communications, and disaster recovery.

2 Statement of the Problem and its Importance

The deficiencies in existing security mechanisms give rise to the following research problems and the proposed research tasks in wireless Ad Hoc networks.

Routing with Smart Antenna: Most Ad Hoc networks are based on omnidirectional antennae with uniform emission in all directions. The emissions enable adversaries to eavesdrop the communication, analyze the pattern of traffic, and locate the sender. One solution to this problem is the usage of smart antennae [11] [31]. Since transmissions are directed, remote stations can be

reached with lower power consumption and eavesdropping becomes more complicated. Despite the advantages on security and power consumption, using smart antennae introduces challenges for routing, which are summarized as follows:

- How to efficiently detect the changes of neighbors? Smart antennae do not cover all directions simultaneously and have delay in detection of neighborhood changes
- How to route the traffic using smart antennae? The sub-problems are: How to choose from multiple paths? How to schedule between different directions?

Solving these problems will enable the usage of smart antennae, thus decreasing information leakage and increasing the safety of physical layer and channel access.

Intrusion Detection: Existing solutions for wired network Intrusion Detection Systems (IDS) do not suit the wireless Ad Hoc networks. The difficulties are discussed in [33]. To utilize either misuse detection or anomaly detection to monitor any possible compromises, the IDS must be able to distinguish normal from anomaly activities. To enable intrusion detection in wireless Ad Hoc networks, the research problems are:

- How to efficiently collect normal and anomaly patterns of Ad Hoc networks? The lifetime of the hosts is short and Ad Hoc networks do not have traffic concentration points (router, switch).
- How to detect anomalies? The lost of traffic could be caused by host movement instead of attacks. Unexpected long delay could be caused by unreliable channel instead of malicious discard.

Our experiments have shown that the anomaly pattern extracted through simulation can be used to detect attacks to destination sequence of AODV [26] effectively. The patterns could also be applied to detect similar attacks to other protocols that use destination sequence.

Intruder Identification and Isolation: The intruders in Ad Hoc networks are more difficult to identify than in wired networks because the topology is constantly changing and the malicious hosts do not have fixed attach points. However, intruder identification must be adopted to protect the networks from following attacks. The research problems in intruder identification in wireless Ad Hoc networks are:

- How to identify the source of an attack?
- How to restrict the attack effect within a certain vicinity?

Solving these problems will heighten the security fence of Ad Hoc networks a step further than current IDS. Our preliminary study shows that it is difficult for a single host to tell the source of the attack [32]. It poses the challenge of identifying intruders in MANET.

Trusted Routing: To provide connectivity in a MANET, every host participates with other hosts to deliver packets to their destination. Since the communication safety of a host solely depends on a proper choice of the path used to reach the destination, it is important for a host to know the reliability of a route. The research problems in discovering trusted routes in wireless Ad Hoc networks are:

- How to evaluate the trustworthiness of an individual host? The trust value is used to describe the ability of a host to forward packets or choose secure path.
- How to evaluate the trustworthiness of a route through the trust value of the hosts along the path?

Our research on trust and evidence formalization [8] provides insights to designing the trust model, propagating trust values among hosts, and assessing the trustworthiness of routes.

Relationship obfuscation: Although the increase of battery lifetime enables basic encryption in mobile devices, encrypted communications hide only the contents of messages, but not the relationships. This is a reason why eavesdropping technology such as Carnivore is useful even in the presence of unbreakable communications [12]. Therefore, preferred targets can be identified, and attacks can be concentrated on nerve centers. The research problems of relationship obfuscation in wireless Ad Hoc networks are:

- What information can be gathered as to the relative authority (e.g., command center) or importance of the members?
- What can be done to obfuscate this information while keeping the efficiency of the communication?

Solving these problems will protect the hosts from traffic analysis attacks, thus decreasing the possibility of exposing the importance of a host.

3 Related Work

Because of the special environments (e.g., battlefield) under which Ad Hoc networks are applied, the vulnerabilities and protection of routing topologies have been paid attention since the very beginning. The difficulties to apply current IDS to Ad Hoc networks are discussed in [33] and a multi-layer integrated IDS for Ad Hoc environments is proposed. The security problems in wireless LAN and Ad Hoc networks are first investigated in [10] and [34]. In [13], different methods for query location for on-demand routing in Ad Hoc networks are analyzed. The latest Ad Hoc network security analysis and IDS structure for Ad Hoc networks have been presented in [30] [9] [25] [6]. This work provides a basis for further research on protecting the Ad Hoc infrastructure.

Several projects [29] [16] [5] [18] have been funded by NSF and other organizations to develop secure Ad Hoc networks or build intrusion detection systems. A central issue of these projects is to protect Ad Hoc networks against denial of service (DoS) attacks. So far researchers focus on using two main principles (redundancy in networking topology and distribution of trust) to solve these problems. Less efforts are put on detecting, and protecting MANET from, other kinds of attacks (host impersonation, false routing, etc.).

In contrast to the previous work, our research combines protection, detection and reaction of attacks to provide a complete security solution for MANET, which integrates smart antennae, secure routing, intrusion detection and intruder identification. A sophisticated trust model will be developed as the basis for these components.

4 Research Tasks and Proposed Solutions

We summarize the research tasks to address the problems presented in section 2 as follows:

1. Exploit the characteristics of smart antennae and the impacts of these characteristics to routing topology. We focus on the design and simulation of neighbor discovery and channel access protocols.

2. Identify normal and anomaly patterns and develop algorithms for intrusion detection and intruder identification in wireless Ad Hoc networks.

3. Design a trusted route discovery and maintenance protocol using the distributed trust model.

4. Study the importance of parameters other than contents and how they can be used to find out the originator of messages. Examine effectiveness and cost of obfuscation strategies against the detectors.

The proposed solutions are briefly outlined in the following subsections.

4.1 Channel Access with Smart Antenna

Smart antennae are available in several forms: sectorized, phased-array and adaptive array. Sectorized antennae consist of individual sector elements aimed in different directions, where only one sector at a time is energized with Radio Frequency (RF). Phased-array antennae can steer a main lobe in any direction, but are not capable of forming intentional nulls. Adaptive arrays can form not only multiple main lobes, but also steerable nulls in the direction of interferers. We propose to investigate the following problems by conducting the proposed experiment A, considering each variety of smart antennae in conjunction with either a CSMA/CA or a TDMA-like protocol.

- Discovering active neighbors. One approach is periodic neighbor discovery, the other is to enable the antenna to work in omnidirectional mode under special circumstances. An optimization for the discovery approach is to apply movement prediction [28]. The impact of other parameters (moving speed, density of hosts, etc.) on the discovery procedure will also be examined.

- Routing in Ad Hoc networks using smart antennae. Fairness is required to avoid hosts in a certain direction occupying the antenna too long. When the antenna is serving a connection, it must be able to monitor routing requests and change its serving object if a new request has higher priority. A routing protocol achieving both fairness and efficiency will be designed and examined.

4.2 Intrusion Detection and Intruder Identification

Intrusion detection and intruder identification are two continuous steps of the response to attacks. The IDS will examine local knowledge and collaborate with other hosts to detect an on-going attack. The identification procedure is used to help the system recovering from previous attacks and preventing further ones.

- Both misuse detection and anomaly detection are based on the pattern collection and matching process. Wired network routing protocols (RIP, OSPF, etc.) and Ad Hoc network routing protocols (AODV, DSR, ZRP, etc.) share a lot of common methods (e.g., distance vector, link state, source routing, destination sequence). The work on protecting the wired networks [7] has shown that it is these common methods that determine the security aspects of the routing topology. The similarity of attacks targeting at these methods in different protocols will be examined and anomaly patterns of these attacks will be extracted. The relationship between normal patterns of the Ad Hoc networks and the metrics (packet delay, user traffic load, density of hosts, etc.) that impact these patterns will be investigated. The completion of experiment B will provide deep understanding of these methods and guide the design of IDS.

- Intruder identification and isolation is triggered when the Ad Hoc network is aware of an attack. The network topology (connectivity history, distance vector) will be used to trace back to the source of the attack. Local knowledge about misbehaved hosts must be shared in a secure way. The information about suspicious host identified by a quorum should also be distributed in a secure way. To decrease the possibility that a normal host is marked as malicious by mistake, the behavior of a suspicious host should still be monitored. Intruder isolation could be achieved by identifying not a single, but a group of suspicious hosts. As long as the performance of the whole system and the benefits of a majority of the hosts are protected, the cost below a threshold is acceptable. Experiment C will provide guidelines for the design of intruder identification and isolation algorithms.

We have analyzed the security aspects of AODV Ad Hoc routing protocol [32]. Four kinds of attacks caused by these aspects have been investigated and simulated in ns2 (network simulator) [2]. A reaction protocol - Reverse Labelling Restriction (RLR) [32] - used to detect and isolate the intruders has been developed. This work will provide insights for collecting normal patterns of Ad Hoc networks for intrusion detection and identifying intruders through collaboration.

4.3 Trusted Route Discovery

When a host A chooses another host B to forward a packet, it takes some risk. Thus a trust relationship between A and B must be established. We use the degree of trust to estimate the risk [8] and to help making rational decisions. A trusted route is a route that only involves trustworthy hosts. Sending packets through trusted routes will decrease the probability of malicious attacks and information leakage. We plan to investigate the following issues via proposed experiment D:

- Applying trust metric to a single host, designing schemes to dynamically update the trust value, and assessing the trustworthiness of a route based on the involved hosts. The host's behaviors, such as forwarding, choosing proper routes, etc., are parameters that comprise the metrics. Communication principles, such as Kalman filtering [17], can be applied to build the trust model as a multi-variable, time-varying state vector that utilizes past information to predict future performance. The assessment of trustworthiness will be based on our current research on trust formalization [8]. We plan to investigate how to propagate trust from one host to another and how trust on hosts affects the trustworthiness of a route with respect to different forwarding schemes (e.g. source routing, hop-to-hop).

- The design of an efficient trusted route discovery protocol for Ad Hoc networks. The protocol must be scalable and adaptive, and can operate in on-demand or proactive fashion. The protocol will be capable of identifying trustworthy hosts by using authentication, and filtering erroneous query, and routing information. We plan to design this protocol using the dynamic programming principle.

4.4 Dynamic obfuscation of relationships

To protect the secure routing information from attacks, we propose to use dynamic obfuscation of relationships. A project ("Packet Tracker") conducted at CERIAS has shown that the source of the messages could be followed through gateways [12] in wired networks. Presumably, even for onion-routed encrypted messages, the additional observation of parameters other than contents, such as timing and size of messages could be used to find the originator of messages [12]. We believe that such techniques could be used to derive relationships and be used to attack secure routing information in Ad Hoc networks. Traffic patterns (initiator, responder, size of packets, response time) may also betray dependency or authority relationships through data mining of a database of communications in a format similar to CISCO's NetFlows [1]. We propose experiment E to examine obfuscation strategies as solutions to protect mobile hosts from traffic analysis attacks.

4.5 Experimental Studies

Research questions, such as identification of anomaly patterns and evaluation of trustworthiness of a route, have to be investigated via experimental studies. We plan to conduct a series of experiments using OPNET [3] and ns2. We have extended ns2 with the implementation of a hierarchical routing protocol and a computation delay module. Attacks to AODV have been investigated. Analysis tools have been developed to extract the traffic in Ad Hoc networks. These will be used as supporting components. Five sample experiments are outlined below:

- **Experiment A:** Determine the tradeoff between the directional beam width and the channel access protocol efficiency.
- **Experiment B:** Extract the anomaly patterns of attacks targeting different routing protocols.
- **Experiment C:** Study the efficiency, accuracy and overhead of different intruder identification and isolation approaches.
- **Experiment D:** Identify the relationships between computation, bandwidth, communication cost and route trustworthiness requirements.
- **Experiment E:** Investigate the effectiveness and cost of dynamic obfuscation of relationships in Ad Hoc networks.

We briefly present experiment C and experiment D due to space limitation. The detail of other experiments is available at www.cs.purdue.edu/homes/bb/cerias02-exp.html.

4.5.1 Experiment C: Intruder Identification and Isolation

Purpose: Intruder identification and isolation are based on connectivity and topology histories. The purpose for this experiment is to examine the efficiency, accuracy and overhead of this scheme.

Input Parameters: The input parameters include attack type (attack to distance vector, attack to destination sequence, etc.) and routing protocol (AODV, DSDV, etc.).

Output Parameters: Average response time (the interval between the initiation of an attack and the successful detection), the goodput, the number of normal hosts that identify the compromised hosts, the number of normal hosts that are wrongly identified, and the number of routing packets.

Method: The identification and isolation approaches will be tested with ns2. We propose to use a reverse labelling method [32] to trace back to the source of false routing information. Both timers and counters coupled with every foreign host will be used to temporarily restrict suspicious host and remember their misbehaving histories. To enable distributed trust, a quorum based mechanism will be adopted throughout the system.

Analysis and Conclusion: We will identify the essential parameters for tracing information source in Ad Hoc networks through the analysis of the experiment results. Completion of this experiment will provide guidelines for the design of an efficient intruder identification mechanism that will protect the networks from continuous attacks from the same malicious host.

4.5.2 Experiment D: Trusted Routing

Purpose: Discovering the most trustworthy route requires extra computation and introduces more delay. The purpose of this experiment is to identify the tradeoff between the cost and the trustworthiness.

Input Parameters: The input parameters include the density of hosts, the mobility of hosts, which is determined by the moving speed and pause time between two movements, the traffic load, and the trustworthiness requirements.

Output Parameters: The output parameters include average end-2-end delay and the normalized protocol overhead (protocol overhead divided by throughput) [27].

Method: The trusted routing protocol will be tested with ns2. A random mobility model is used to generate the movement of mobile hosts. We will determine a high value and a low value for the density of hosts, the mobility, and the traffic load. Based on these values, different testing environments will be set up, i.e., high density, low mobility, and low traffic load. The network layer and MAC layer traffic data will be collected. We will use the supporting tools to extract the average end-2-end delay, the throughput, and the protocol overhead from the experimental data. The normalized protocol overhead is then obtained from the throughput and the protocol overhead.

Analysis and Conclusion: We consider the trustworthiness requirement as an independent variable, the delay and the protocol overhead as cost functions. We will use MATLAB [21] to analyze these functions for each testing environment. From the analysis we can find how the cost are affected by different environments. The results of this experiment will provide guidelines for the design of adaptable and efficient trusted route discovery algorithms.

5 Research Team

We have an interdisciplinary team with ongoing research in

- Wireless network architecture [19] [20] [4], attack to Ad Hoc routing protocols [32], and formalization of evidence and trust [8]. These will be used as building blocks for the proposed experiments and will provide basis for deploying trust and secure routing in Ad Hoc networks.
- Smart antennae for wireless communications, anti-jam protection for GPS, and reduced-rank adaptive filtering. Different jam resistant protocols [35] [23] [24] and methods will be applied to decrease the vulnerability of wireless channels.
- An incident response system (CIRDB) and system vulnerability in mobile networks. The investigation on vulnerabilities and wireless PDA security [22] [15] will become important components in our secure routing and intrusion detection system.

6 Tentative Schedule of Tasks

Design and implementation of directional antenna module in ns2 (3 months). Simulation and analysis of different combinations of antennae and other parameters (2 months). Analysis and extraction of common security features of Ad Hoc routing protocols and attacks design (3 months). Simulation of Ad Hoc network under normal condition in ns2 and normal pattern collection (3 months). Intrusion detection system design and implementation (2 months). Design, implementation, examination of intrusion identification and isolation algorithms (3 months). Construction of distributed trust model and evaluation of different security metrics (3 months). Design, implementation, and examination of secure routing protocol (3 months). Experiments for dynamic obfuscation of relationships in Ad Hoc networks (2 months).

7 Plans for Continuation of Research/Tech Transfer

Two Ph.D. students (Y. Lu and W. Wang) are working in this area and have selected this topic for their theses. A University Research Program (URP) proposal "Trusted Route Discovery in Ad Hoc Networks" has been submitted to CISCO. Terry Charbonneau from ITT is working closely with us to prepare a proposal for Army Research Lab on the research of applying smart antennae for providing secure communication. Collaboration with INTEL (Dr. Unni K Narayanan) on the development of mobile network simulation tools is continuing and the tasks for funding are being finalized. CISCO, INTEL and Hewlett-Packard have shown great interest in this research in the Research Symposium held by CERIAS in April, 2002.

References

[1] http://www.cisco.com/go/netflow/.

[2] http://www.isi.edu/nsnam/ns/.

[3] http://www.opnet.com/products/modeler/home.html.

[4] Presentation at The Third Annual Research Symposium on Security at CERIAS, Purdue University, 2002.

[5] D. Agrawal. On robust and secure mobile ad hoc and sensor netwroks. NSF funded proposal, http://www.ececs.uc.edu/ cdmc/, 2001-2004.

[6] P. Albers and O. Camp. Security in ad hoc network; a general id architecture enhancing trust based approaches. In *Proceedings of International Conference on Enterprise Information Systems (ICEIS)*, 2002.

[7] S. Bellovin. Security problems in the tcp/ip protocol suite. *Computer Communications Review*, 19(2):32–48, April 1989.

[8] B. Bhargava and Y. Zhong. Authorization based on evidence and trust. To appear in Data Warehouse and Knowledge Management Conference (DaWak), France, 2002.

[9] S. Bhargava and D. P. Agrawal. Security enhancementsin aodv pro tocol for wireless ad hoc networks. Vehicular Technology Conference, 2001.

[10] V. Bharghavan. Secure wireless lans. In *Proceedings of the ACM Conference on Computers and Communications Security*, 1994.

[11] T. Biedka, C. Dietrich, K. Dietze, R. Ertel, B. Kim, R. Mostafa, W. Newhall, U. Ringel, J. Reed, D. Sweeney, W. Stutzman, R. Boyle, and A. Tikku. Smart antenna for handsets. DSPS Fest, 2000.

[12] F. Buchholz, T. E. Daniels, B. Kuperman, and C. Shields. Packet tracker final report. Technical report, CERIAS, 2000.

[13] R. Castenada, S. Das, and M. Marina. Query localization techniques for on-demand routing protocols for mobile ad hoc networks. *ACM/Kluwer Wireless Networks (WINET) Journal, Vol. 8, No. 2, pages 137-151*, 2002.

[14] M. Corson and A. Ephremides. A distributed routing algorithm for mobile radio networks. MILCOM 89, 1989.

[15] J. Crane, S. Kamara, P. Meunier, D. Noland, and S. Nystrom. Progress report on the penetration analysis of windows ce and 802.11b wireless netwroks. Technical report, CERIAS, 2001.

[16] Z. Haas. Secure communication for ad hoc networking. NSF funded proposal, http://wnl.ece.cornell.edu/wnlprojects.html, 2000-2003.

[17] R. Kalman. A new approach to linear filtering and prediction problems. *Transaction of the ASME–Journal of Basic Engineering*, pages 35–45, 1960.

[18] W. Lee. Career: Adaptive intrusion detection systems. NSF funded proposal, http://www.cc.gatech.edu/ wenke/, 2002-2005.

[19] Y. Lu and B. Bhargava. Achieving flexibility and scalability: A new architecture for wireless network. International Conference on Internet Computing, 2001.

[20] Y. Lu, B. Bhargava, and M. Hefeeda. An architecture for secure wireless networking. IEEE Workshop on "Reliable and Secure Applications in Mobile Environment", 2001.

[21] W. Martinez and A. Martinez. *Computational Statics Handbook with MATLAB*. Chapman and Hall/CRC, 2002.

[22] P. Meunier and E. Spafford. Running the free vulnerability notification system: Cassandra. In *Proceedings of the 14th Annual Computer Security Incident Handling Conference*, 2002.

[23] W. Myrick, M. D. Zoltowski, and J. Sjogren. Low complexity anti-jam space-time processing for gps. IEEE International Conference on Acoustic, Speech and Signal Processing, 2001.

[24] S. Ozen and M. D. Zoltowski. A fading filter approximation to enable state-space modelling and joint data/channel estimation of time-varing frequency selective channels with antenna arrays. IEEE CAS-Notre Dame Workshop on Wireless Communication and Networking, 2001.

[25] P. Papadimitratos and Z. Haas. Secure routing for mobile ad hoc networks. SCS Communication Networks and Distributed Systems Modeling and Simulation Conference (CNDS), 2002.

[26] C. Perkins and E. Royer. Ad-hoc on-demand distance vector routing. In *Proceedings of the 2nd IEEE Workshop on Mobile Computing Systems and Applications*, 1999.

[27] C. Perkins, E. Royer, and S. Das. Performance comparison of two on-demand routing protocols for ad hoc networks. In *Proceedings of IEEE INFOCOM*, 2000.

[28] K. Plataniotis. Mobile position location in third generation cellular networks. Supported by Nortel Institute for Telecommunications, Conducted at University of Toronto, 2001-2003.

[29] R. Ramanujan and R. Edin. Tiara: Techniques for intrusion-resistant ad hoc routing algorithms. DARPA funded proposal, www.oracorp.com/projects/current/tiara.html, 2000-2003.

[30] P. Sinha, R. Sivakumar, and V. Bharghavan. Enhancing ad-hoc routing with dynamic virtual infrastructures. IEEE Infocom, 2001.

[31] W. Stutzman, J. Reed, C. Dietrich, B. Kim, and D. Sweeney. Recent results from smart antenna experiments–base station and handheld terminals. pages 139–142. IEEE Radio and Wireless Conference, 2000.

[32] W. Wang and B. Bhargava. On vulnerability and protection of aodv. Technical report, CERIAS Security Research Center, Purdue University, http://raidlab.cs.purdue.edu, 2002.

[33] Y. Zhang and W. Lee. Intrusion detection in wireless ad-hoc networks. In *Proceedings of ACM MobiComm*, 2000.

[34] Z. Zhou and Z. Haas. Secure ad hoc networks. *IEEE Networks*, 13(6):24–30, 1999.

[35] M. D. Zoltowski. Recent advances in reduced-rank adaptive filtering with applications to high-speed wireless communications. The International Society for Optical Engineering, 2001.