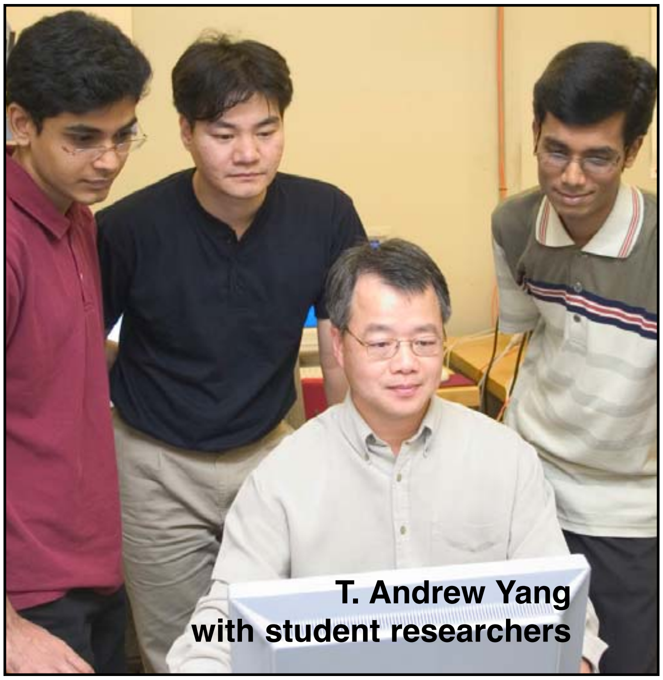
Development of Wireless Stations for Distributed Field Operations

T. Andrew Yang
Computer Science Department

Sadegh Davari



T. Andrew Yang
with student researchers

Abstract—Distributed field operations involve dispersed mobile units operating in a wide geographical area, such as battlefield operations or exploration on the moon. One or more wireless stations may be deployed for effective connectivity among the units. In this seed project, we investigate the security and performance issues of wireless stations in mobile ad hoc networks (MANET).

THE FIVE COMPONENTS OF A SECURITY MECHANISM ARE confidentiality, integrity, authenticity, availability and non-repudiability. Of these terms, authenticity is the most fundamental issue, since a breach of authenticity leads to a system-wide compromise. One of the widely used authentication mechanisms in conventional wired networks is the public key management system using certificates.

One of the main issues to consider in a certificate-based scheme is the secure distribution of the public keys to all the nodes in the network. The Public Key Infrastructure (PKI)[1] defines methods for handling public key management using X.509 certificates. In a wired network, there exists a centralized certificate server which handles the creation, renewal, and revocation of certificates. This is not feasible in mobile ad hoc networks (MANET), which are composed of mobile nodes that may be constantly moving in the geographical area and do not have a fixed infrastructure or centralized management. Because of the dynamic topology of the network, frequent link failures may occur, resulting in issues such as re-authentication and timely communication with the certificate server.

To overcome these limitations and to reap full advantages of the certificate-based authentication mechanism, several public key management mechanisms have been proposed for MANET.[2-5]

Goals of the Project

The overall goal of the project is the investigation of security and performance issues of wireless stations in distributed networks. At the current stage, we have focused on the area of wireless local area network security and certificate-based authentications in mobile ad hoc networks.

To devise a secure and effective certificate-based authentication scheme for mobile ad hoc networks, our immediate goal is evaluation of existing approaches by running network simulations to compare their respective strengths and weaknesses. Based on the results of our evaluation, the next step of the project is to design a secure an efficient authentication protocol for mobile nodes in a MANET.

Results

Our contributions so far include the following: (1) analysis of the requirements of a secure distributed authentication system for MANETs; (2) a survey of the existing certificate-based authentication mechanisms by analyzing their features, including pros and cons, in the context of distributed authentication; and (3) the design of a series of scenario-based simulation experiments and metrics to evaluate these features.

Requirements of Effective Certificate-Based Authentication for ad hoc Networks

Five requirements have been identified for any certificate-based authentication scheme to be considered secure and effective, with respect to authentication in a mobile ad hoc network.

R.1 Distributed Authentication: In ad hoc networks, due to issues such as frequent link failures, node mobility, and limited wireless medium, it is typically not feasible to include a fixed centralized certifying authority (CA) in the network. Further, in networks requiring high security, such a server could become a single point of failure. For example, consider a battlefield scenario where the troops are spread over a large area. In such a case, it might not be feasible to have a central server. An enemy attack on the server would bring down the whole network. One of the primary requirements of a certificate-based mechanism is to distribute the authentication amongst a set of nodes in the network.

R.2 Resource Awareness: Since the nodes in an ad hoc network typically run on batteries with high power consumption and low memory capacity, the authentication protocols must be resource-aware. That means that the time and space complexity of the underlying algorithms must be acceptably low. In this regard, symmetric-key-based cryptographic techniques are more suited, in contrast with public key methods, because symmetric cryptography in general incurs less consumption of resources. However, the issue of distributing the symmetric keys prevents their practical deployment in ad hoc networks. This is a tradeoff that must be dealt with at the application level. Since certificate-based authentication uses public key mechanisms, which are resource-intensive, the protocol itself must be efficient both in terms of memory and power.

R.3 Efficient Certificate M anagement Mechanism: The distribution of public keys and management of certificates have been studied extensively in the case of wired networks.[1] However, in applying these methods to MANETs, managing the certificates is a challenging issue. For example, most of the current mechanisms lack a robust certificate revocation scheme.

INDIA—Having earned his B.Technology degree in computer science and engineering at the Jawaharlal Nehru Technological University in Hydedrabad, India, Satheesh Kumar Ilu now pursues the M.S. in computer science at UHCL.

VIETNAM—Tuan Anh Nguyen currently serves as a research assistant in Computer Information Systems at UHCL where he is studying for a master's in computer information systems. He earned his B.S. in computer sciences at the Hanoi University of Technology in his native country Vietnam.

Table 1. Comparison of Certificate based Authentications

Requirements	*Self Organized Public Key Management*[2]	*Providing Robust and Ubiquitous Security Support for Mobile Ad hoc Networks*[4]	*Self Managed Heterogeneous Certification in Mobile Ad Hoc Networks*[3]	*Trust- and Clustering-Based Authentication Services in Mobile Ad Hoc Networks*[5]
R.1. Distributed authentication	Totally distributed certification method since every node acts as a CA	Totally distributed and scales well to large networks	Totally distributed and scales well to large networks	Distributed and self organized since every node acts as a CA
R.2. Resource awareness	Each node maintains two certificate repositories, which incurs a high overhead.	The generation and distribution of keys using complex polynomial functions is resource-intensive and time consuming.	Each node only maintains a list of its trusted CAs. Thus, it is more efficient than the method proposed in Capkun[2]	The maintenance of trust tables and the monitoring components are memory intensive.
R.3.(a) Creation	Self–signed certificates and more robust than a shared key based mechanism	Requires at least *k* neighbors which might be a bottleneck	Similar to *K*-threshold mechanism4	Across nodes, creation is based on trust values. The existence of introducing nodes may not be true at all times.
R.3.(b) Renewal	No explicit mechanism discussed	Same as issuance	Implemented through the DMCR algorithm	Not discussed
R.3.(c) Revocation	Explicit revocation causes delay between far-away nodes in the network.	System CRL table stored at each node and, hence, memory intensive.	Not discussed	Not discussed
R.4. Heterogeneous certification	Not implemented.	Not implemented.	Implemented using trust graphs.	Not implemented

R.4. Heterogeneous Certification: As in the case of wired networks, certifying authorities might be heterogeneous even in ad hoc networks. This means that two or more nodes belonging to different "domains" may try to authenticate each other. In such a case, there must be some kind of trust relationship or hierarchy among the CAs. In wired networks, this is accomplished through certificate chaining.

R.5. Robust pre-authentication mechanism: By pre-authentication mechanism, we mean the process of establishing necessary trust between nodes before the actual certificate creation and distribution. Though this is not a part of the certificate authentication process itself, it is pretty important in MANETs, because, in order to satisfy the requirement of distributed authentication (R.1), it is mandatory that nodes have prior trust between each other (by exchange of public keys, for example). Without this pre-established trust, the later mutual authentication and renewal of certificates would not be possible.

Survey of Related Work

Certificate-based authentication usually consists of three phases. During the first phase or the "bootstrapping" phase, the nodes are issued a certificate by a certifying authority. The certificate is created by the CA using the node's identity information, such as IP address, name, organization, and its public key. The certificate also consists of the issuing time and the expiration time besides other information. During the second phase, the certificate is "renewed" due to its expiration. The third phase involves revocation of the certificate by the CA, possibly due to compromise of the private key of the certificate holder or probably because the issuer believes that the user-key binding is no longer valid. We have surveyed four of the proposed mechanisms.[2-5] Their respective advantages and disadvantages are shown in Table 1.

Scenarios and Metrics

In order to study the effectiveness of these mechanisms, we propose a set of realistic "scenarios" for simulation. Before defining the scenarios, we first need to define specific parameters:

The *mobility model* represents the realistic movements of nodes in the network. They can be primarily classified as entity mobility models and group mobility models. Camp et al. give a broader classification of these models.[6] The most commonly used mobility model by the research community is the Random Waypoint Model (RWM), which uses pause times and random changes in destination and speed. However, the randomness does not suit well to certain scenarios, such as a

Table 2. Sample Scenarios

parameters	*I. Battlefield*	*II. Rescue Operation*	*III. City Traffic*	*IV. Event Coverage*
Mobility model	RPGM	RPGM	Manhattan Grid	Gauss Markov Model
Number of nodes	10 in each group 5 groups	5 in each group 10 groups	50	50
Area	2000 * 2000 m	1000 * 1000 m	1500 * 500 m	500 * 500 m
Speed	Node speed: 5 m/s Group speed: 1 m/s	Node speed: 2 m/s Group speed: 5 m/s	Node speed: 20 m/s	Node speed: 2 m/s Group speed: 5 m/s

battlefield where the mobility is more predictive. Further, the model also fails to provide a "steady-state" over a long simulation period.[7] Thus, mobility models should be chosen carefully while evaluating a certificate-based authentication mechanism. It must model the realistic scenario as closely as possible.

Node Density also varies according to a particular scenario. For example, an event coverage scenario may have a high density of nodes, whereas a disaster recovery scenario might have a low density as the nodes are spread out over a wide area.

Traffic rates vary according to the node linkage failures, congestion, and mobility.

The Sources and Type of Traffic

Normally, the traffic type used is Constant Bit Rate (CBR), although other types of traffic, such as TCP or UDP, must also be taken into account while defining the scenarios.

Sample scenarios and their respective parameters for simulations are listed in Table 2. Scenarios I and II are based on the Reference Point Group Mobility model (RPGM).[6] RPGM is a group mobility model where each group has a logical center (similar to a troop head) that determines the group behavior. The nodes within a group move randomly according to the RWM, but the group movement is determined by the leader overall. Scenarios III and IV are based on entity mobility models. The most commonly used entity mobility model is the Random Waypoint. However, for realistic scenarios, in scenario III the Manhattan Grid Model is used, and in scenario IV the Gauss Markov Model is utilized.

Having defined the parameters for the scenarios, we further identify the following metrics, based on which the authentication mechanisms can be evaluated.

Successful Certification Ratio (μ) measures the ratio of the number of successful certification services (including issuance, NC_{ISS}, and renewal, NC_{REN}, respectively) to the total number of requests for such services (NC_{TotIss} and NC_{TotRen}, respectively). It gives an idea about the efficiency of the mechanism in providing successful certification services. If we consider μ_{REN} as the successful certification renewal ratio and μ_{ISS} as the successful certificate issuance ratio, then their respective values can be calculated as follows:

$$\mu_{REN} = \frac{NC_{REN}}{NC_{TotRen}} \qquad \mu_{ISS} = \frac{NC_{TotRen}}{NC_{TotIss}}$$

Settling Time (*st*) measures the initial time taken for all the nodes in the network to be issued valid certificates. The value of *st* can be calculated as the difference between the time when all the nodes are issued valid certificates and the starting time when the process of certificate issuance begins. The settling time taken will depend on factors such as the number of malicious or non-cooperative nodes, the algorithms used for key generation and distribution, etc. If pre-authentication methods are efficient (R.5), the settling time will be less.

Frequency of Certification (f_{cert}) measures the number of certification services per time interval:

$$f_{cert} = \frac{N_{cert}}{T_{int}}$$

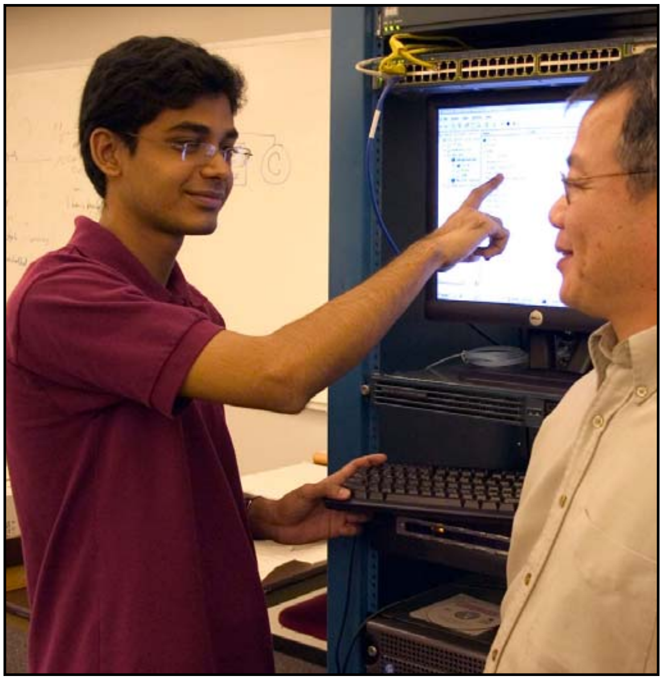
Here N_{cert} is the total number of certification services (issuance/renewal) by nodes in the network, and T_{int} is the simulation time. As the topology of the network changes, it is expected that there will be frequent certificate issuance and renewal processes. This incurs overhead, since each time a node wants to create or renew its certificate costly computations have to be carried out for the public key mechanism. We intuitively predict that a distributed and self-organized mechanism will have a lower frequency of certificate creation, renewal and revocation, and hence, a lower f_{cert}.

Average Certification Delay (*acd*) is measured as the time delay between the certificate service request (*CSReq*) and the certificate service reply (*CSRep*) averaged over the simulation time. This value estimates the efficiency of the algorithm and mainly depends on the time complexity of the algorithm.

$$acd = \frac{\Sigma_{i=1..n}(CS\,\mathrm{Re}\,p_i - CS\,\mathrm{Re}\,q_i)}{T_{\mathrm{int}}}$$

Summaries and Future Work

Successful authentication in mobile ad hoc networks is critical for ensuring secure and effective operation of the supported application, especially in distributed field applications where mobile nodes are spread over a large geographical area. Several certificate-based authentication mechanisms have been proposed for MANETs. We surveyed some of these mechanisms and charted the requirements for certificate-based authentication schemes for MANETs. We also pro-



MADRAS—Karthik Sadasivam, research assistant in computer science, earned his Bachelor of Engineering degree in computer science at the University of Madras in India. He is now a master's student in computer sciences at UHCL, conducting research under the direction of Dr. T. Andrew Yang.

posed a few experimental scenarios and metrics, based on which simulation study of these methods may be currently under way, using the network simulator ns-2.

In addition to authentication issues, our long-term goal is to develop a complete set of security protocols geared toward wireless networks in distributed environments. The set of protocols will address the whole spectrum of security components, including confidentiality, integrity, authenticity, availability, and non-repudiability.

Acknowledgments

Equipment used in this project is partially supported by the National Science Foundation (DUE-0311592) and the Division of Computing and Mathematics, UHCL. Karthik Sadasivam, completing his M.S. thesis at UHCL, has made major contributions to this project.

References

[1] Internet Engineering Task Force (IETF), "Internet X.509 Public Key Infrastructure Certificate and CRL Profile," RFC 2459.

[2] S. Capkun, L. Buttyan, and J.-P. Hubaux. "Self-Organized Public-Key Management for Mobile Ad Hoc Networks," IEEE *Transactions* on Mobile Computing 2.1 (2003): 52-64.

[3] W. Wang, Y. Zhu, and B. Li, "Self-Managed Heterogeneous Certification in Mobile Ad Hoc Networks," *Proc.*, IEEE Vehicular Technology Conference (VTC 2003), 2003.

[4] J. Kong, P. Zerfos, H. Luo, S. Lu, and L. Zhang, "Providing Robust and Ubiquitous Security Support for Mobile Ad Hoc Networks," *Proc.*, 9th International conference on Network Protocols (ICNP), 2001.

[5] E. C. H. Ngai and M. R. Lyu. "Trust- and Clustering-Based Authentication Services in Mobile Ad Hoc Networks," *Proc.*, 24th International Conference on Distributed Computing Systems Workshops, W4: MDC (ICDCSW'04), 2004.

[6] T. Camp, J. Boleng, and V. Davies, "A Survey of Mobility Models for Ad Hoc Network Research," *Wireless Communication & Mobile Computing*, special issue on *Mobile Ad Hoc Networking: Research, Trends and Applications* 2.5 (2002).

[7] J. Yoon, M. Liu, and B. Noble, "Random Waypoint Considered Harmful," *Proc.*, IEEE INFOCOM '03 (2003): 1312-21.

Publications

Yang, T. A. and Y. Zahur. "Security in WLANs," in *Handbook of Wireless Local Area Networks: Applications, Technology, Security, and Standards*. Eds. M. Ilyas and S. Ahson. Boca Raton, FL: CRC Press LLC, 2005. 429-250 (to be published April, 2005).

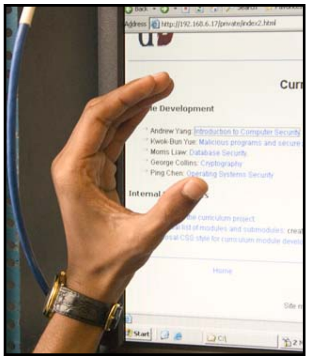
Yang, T. A., K. Yue, M. Liaw, G. Collins, J. T. Venkatraman, S. Achar, K. Sadasivam, and P. Chen. "Design of a Distributed Computer Security Lab," *J. Computing Sciences in Colleges* 20.1 (2004): 332-346.

Presentations

Sadasivam, K. and T. A. Yang. "Evaluation of Certificate Based Authentication in Mobile Ad Hoc Networks," IASTED International Multi-Conference on Networks and Communication Systems (NCS 2005), Krabi, Thailand. April 18–20, 2005.

Sadasivam, K., V. Changrani, and T. A. Yang. "Scenario Based Performance Evaluation of Secure Routing in MANETs," 3rd presentation, 2nd International Workshop on Mobile Ad Hoc Networks and Interoperability Issues (MANETII'05), in conjunction with the International Conference on Wireless Networks (ICWN'05), Las Vegas, NV, June 2005 (*accepted*).

Sadasivam, K., B. Samudrala, and T. A. Yang. "Design of Network Security Projects Using Honeypots," 2005 Consortium for Computing Sciences in Colleges (CCSC) South Central Conf., Lake Charles, LA, April 15–16, 2005.



Hands-on research in the laboratory