Security and Trust Management in Self-organizing Wireless Adhoc Networks

Ling Liu
Distributed Data Intensive Systems Lab
College of Computing, Georgia Institute of Technology
Lingliu@cc.gatech.edu

Ubiquitous connectivity and pervasive use of smart devices, powered by the emergence of cloud computing, are changing the way we live and work in the 20th century. We increasingly depend on the Internet, the computing infrastructure and the data networks for just about every aspect of our daily life. Consumers use the Internet to access information, manage finances, obtain wide range of products and services, communicate and share information with colleagues, friends, and families. Businesses use the Intern t to carry out transactions with their customers and with one another. Governments rely on the Internet to conduct federal and state government affairs and deliver services to their citizens.

With this increasing dependence on the Internet and the integration of the various computing and networked services, the disruption of the Internet connectivity and the availability of networked services may have profound impact on the lives of many individuals as well as the economic viability of businesses and organizations. Similarly, the security of nations is directly linked to the availability, survivability, and dependability of the Internet and the many Internet based data networks. Therefore, prolonged or unpredictable unavailability of networked services is unacceptable. One of the grand challenges in the 20th century is to devise approaches to ensure that networked services can survive unexpected security and availability challenges, such as attacks, large-scale natural disasters and faults, in a timely manner. Self-organizing networks and systems, especially self-managed wireless adhoc networks, powered with situational-aware proactive computing, will play an important role in meeting this grant challenge.

A self-organizing network is a network that can automatically extend, change, configure and optimize its topology, coverage, capacity, cell size, and channel allocation, based on changes in location, traffic pattern, interference, and the situation or environment. Wireless Ad-hoc networks is a special class of self-organizing networks, where capabilities or existence of links, capabilities or availabilities of nodes or network services are considered as a random function of time. An ad-hoc network has no fixed infrastructure or predetermined topology. No fixed centralized entity controls the network [10]. An ad hoc network is a (possibly mobile) collection of communications devices (nodes) that wish to communicate, but have no fixed infrastructure available, and have no pre-determined organization of available links. Individual nodes are responsible for dynamically discovering which other nodes they can directly communicate with. A key assumption is that not all nodes can directly communicate with each other, so nodes are required to relay packets on behalf of other nodes in order to deliver data across the network. A significant feature of ad hoc networks is that rapid changes in connectivity and link characteristics are introduced due to node mobility and power control practices. Ad hoc networks can be built around any wireless technology, including infrared and radio frequency (RF) [9,10,13,28].

The simplest Ad Hoc network can be seen as a wireless radio network between a collection of vehicles, ships, aircraft, or even people on foot, operating in a geographical area with no networking infrastructure. Many examples of such scenarios come to mind: Cars and trucks on country highways or freeways, Scientists on field outings, A group of school-children on an outing into a national park, all carrying laptops or PDAs, A meeting where all participants have a laptop. The range of possible situations in which Ad Hoc networking can be exploited is huge. A robust Ad Hoc networking scheme frees the individual from the geographical constraints of the fixed network. In this respect it is fundamentally different from established mobile wireless networking, in which mobile nodes need to remain within the coverage of a wireless base station, connected to the fixed network infrastructure.

The technological challenges of ad hoc routing are not trivial: The topology will vary because some nodes will move in and out of wireless link range of the other nodes in the network. Therefore the number of hops between source and destination will vary as well. Network throughput will also vary because the larger the number of hops, the greater the routing delay will be, and thus the throughput for a finite buffer size will decrease. When the distance between wireless nodes increases, the signal to noise ratio decreases and the achievable throughput is reduced. Routing problems fall into two categories: Route discovery and Route maintenance. The routing can also be divided into two different models: Proactive routing, where the routing tables in all nodes are continuously updated. Reactive routing, where the routing tables are only updated on demand. Proactive routing should be used when the node mobility is low and the utility traffic has real time demands. Reactive routing is used when the demand for real time transmission is low. Route discovery is only carried out when a new route is needed or when an old route is no longer in working order.

Another technical challenge is scaling. [5] shows a very interesting result based on a simple interference model. If there are N nodes in a bounded region, the total throughput capacity of an ad hoc wireless network grows at $\sqrt{N}$ which implies that the throughput per node decreases at $1/\sqrt{N}$. Thus, with a large number of nodes, the performance per node approaches zero. The number of route updates will also increase with the number of nodes. This is obviously a scaling problem [11].

The third challenge is the limited battery power supply of the mobile nodes. Forwarding packets for routing updates or other parties' utility packets may tempt users to turn off their equipment, and only turn it on when they want to communicate themselves.
This problem has both psychological side and technological side. Technological solutions may be to make the batteries last longer by making better batteries, making the transmitter power adapt to the wireless path length, and letting the equipment go into sleep mode when there is no traffic. A psychological solution may be to give the (owners of the) nodes some form of credit when other parties' packets are forwarded.

The most serious challenge is that of security. Some of the literature [1,11,14,15,22,23,24,28] has security in wireless ad hoc networks as its main theme. All of them describe principles and methods for adding security to existing ad hoc routing protocols, where security was not an issue from the beginning. A very limiting factor today is the capacity of the terminals. When n terminals, each having a capacity C work closely together to form an ad hoc network, the useful capacity C_U of each terminal (because of interference) [43] is $C_U = C/\sqrt{n}$. With 100 terminals in the network, the useful capacity of each terminal will be only 10% of its original capacity. The routing protocol may use 70 – 80% of this capacity if the terminals are highly mobile [44]. To make the ad hoc network secure, some form of authentication is necessary, which easily can use the rest of the capacity, especially if it is based on public key infrastructure and threshold cryptography.

Security in self-organizing networks is characterized by availability, integrity, confidentiality, authenticity, and accountability. The basic challenge of maintaining security and reliability of self-organizing networks is to handle trust and to have efficient and working security and networking mechanisms under ever changing conditions in ad-hoc networks, where nodes roam freely, communicate with one another via multi-hop, error-prone wireless communication, and may join, leave, or fail dynamically.

Availability is defined as the ability to deliver a set of resources or services at a given point in time, or continuously within a given time interval. Availability hence requires that the network can withstand denial-of-service attacks. Availability is probably the most important security attribute, as resources that are never available lose all utility. Much of contemporary computer security bases itself on the ability of a subject to contact a trusted entity somewhere in a given network. For a network with defined and reasonably stable links, this is usually not a problem. Link and node downstate are exceptions rather than the rule, and are usually caused by a fault somewhere. However, this is no longer the case for self-organizing ad-hoc networks, where the network is no longer a strongly connected graph, and arbitrary link or process behavior are considered normal.

Integrity deals with the detection of unauthorized operations on data in a system. The restoration of damage after unauthorized operations have occurred is usually considered a part of dependability, while the prevention of the unauthorized operations is typically taken care of by authentication and access controls. A message authentication code (MAC) allows the detection of some types of data modification with a reasonably high probability. It does not take care of fault-tolerance, such that provided by error-correcting codes, as it cannot supply. As an example, a MAC computed by the operating system kernel in its role as reference monitor, is well suited to detecting integrity breaches involving violation of processes' memory spaces, etc. The same MAC, however, cannot detect integrity violations carried out by an application misbehaving, because the application for all intents and purposes appears to be acting legitimately. Thus integrity borders closely on, or encompasses, legitimate usage.

Confidentiality is about controlling the ability of any given subject to extract information from an object. The types of data are relevant in a confidentiality context include (a) Secret content (such as offers during contract bidding); (b) Data that can identify a physical person; and (c) Data that can reveal preferences and habits of a physical person. Encryption is the fundamental method for protecting confidential data. The encryption in itself is not more challenging in a self-organizing network than in any other network. The challenge with data confidentiality is connected to the changing trust relationships, and thereby key distribution and management. Another challenge is to figure out what data to protect.

Protection of ***anonymity* and *privacy*** is another fundamental problem in self-organizing networks, as the self-organizing techniques are often based on collecting data about users and usage. Wireless multi-hop routing (intelligent relaying and ad hoc network), require information about neighbors, hence protection of anonymity and privacy is a major challenge in such networks. Anonymity is to conceal the identity involved in some process [12], whereas privacy is wider [7]: the right to control or influence what information related to them may be collected and stored by whom that information may be disclosed.

Authenticity in self-organizing wireless ad-hoc networks refers to three types of authentications: authenticity of origin, authenticity of identity, and authenticity of location. Authenticity of origin deals with proving or disproving the claimed identity of the creator of some data, be it art, code or something else. Authenticity of identity deals in general with proving or disproving the identity claimed by a subject. Authenticity of location deals with verification of claimed locations of a mobile node. Authentication is fundamental when providing users of a network with security. Without at least some degree of authentication, effective access control becomes impossible. In a distributed system, any implementation of an authentication system necessarily involves trust management. It is shown that the use of asymmetrical cryptography is computationally very intensive, compared to symmetrical cryptography; if hardware based cryptography about 100:1 and for software based cryptography about 1000:1 [29]. Therefore authentication based on software and unsymmetrical cryptography is so far considered out of the question for mobile hosts with limited processor power and battery life. For ad hoc networks, node-to-node message authentication should be used [22]. In general, due to rapid and frequent topology changes, security mechanisms for self-organizing networks need to be computationally and signaling efficient.

Key management service is required in ad-hoc networks [28]. It uses cryptographic schemes, such as digital signatures, to protect both routing information and data traffic. A public key infrastructure is the best way to distribute keys in the network and at the same time achieve integrity and non-repudiation. After authentication, shared secret keys schemes are used to obtain secure communication. In a public key infrastructure, each node has a private and public key pair. The public keys may be distributed to other nodes, while the private keys have to be kept confidential at the individual nodes. The public keys are usually bound to the individual nodes through a trusted third party, the certification authority, CA. The certification authority also has a public and private key pair. All nodes know the public key of the CA. The CA can therefore sign certificates binding public keys to nodes. The trusted CA has to stay continuously on line because the nodes enter and leave the network at all times, requiring new certificates. If a node is no longer trusted, its certificate has to be revoked.

It is problematic to base an ad hoc network on a single CA. If the CA is off line, it is impossible to establish trust between nodes. The CA will be the most vulnerable part of the network and will be the target for attacks or can be taken over by an adversary, leaking all the secret keys. To improve the availability of the CA, it may be replicated, but straightforward replication of the CA will make the service even more vulnerable. If any of the replicas is compromised, the whole network is compromised. A solution to this dilemma is threshold cryptography [41]. The certification authority is distributed between *n* nodes in such a way that if less than *r* servers are compromised, it is possible to trust the remaining *(n-r)* servers to sign certificates. It is also impossible for an adversary to obtain the secret keys if less than *r* servers are available to him. (*r* is the threshold number of servers in the scheme, *n* is the total number of CA servers.). [26] evaluated an ad hoc network with public key infrastructure and a threshold based certification authority through computer simulations. They found that the scheme was working well, but certification, authentication and routing messages used about 80% of the network's capacity. The nodes with CA functionality were provided with additional processing capacity.

Research community in self-organizing networks is exploring alternatives to PKI and threshold cryptography. One example is the scheme described in [22], using the principle of *the resurrecting duckling* and *secure transient association*. This solution requires considerably less processing and battery power. This research can also benefit from exploring and extending the research results in link-spam analysis [2,3], securing publish-subscribe networks [17], secure broadcast [16,19], and peer to peer trust [25].

To sum up, the main challenges with securing self-organizing networks are:

- How to balance between cryptography-centric design and network performance centric design?
- How to provide attack-tolerant solutions for securing self-organizing networks?
- How to device security guards in a collaborative networking environment without trusting each individual?
- How to protect privacy and anonymity of both message content and message source and destination?
- How to build a self-organizing secure network in a dynamic topological mobile ad-hoc network?

Reference

1. Dirk Balfanz, D.K. Smetters, Paul Stewart, and H. Chi Wong. *Talking to strangers:Authentication in ad hoc wireless networks*. In Symposium on Network and Distributed Systems Security (NDSS '02), San Diego, California, February 2002. http://www.citeseer.nj.nec.com/balfanz02talking.html
2. James Caverlee and Ling Liu. ``A Parameterized Approach to Spam-Resilient Link Analysis of the Web'', IEEE Transactions on Parallel and Distributed Systems (TPDS).
3. James Caverlee, Ling Liu, Steve Webb. ``SocialTrust: Tamper-Resilient Trust Establishment in Online Communities'', Proceedings of the International Joint Conference on Digital Libraries (JDL 2008), June 16-20, 2008 - Pittsburgh, Pennsylvania.
4. Ali Fessi, Heiko Niedermayer, Holger Kinkelin, and Georg Carle. A cooperative sip infrastructure for highly reliable telecommunication services. In ACM conference on Principles, Systems and Applications of IP Telecommunications (IPTComm), New York, July 2007.
5. P. Gupta and P. R. Kumar, *The Capacity of Wireless Networks*, IEEE Trans. Info. Theory, Mar. 2000. http://citeseer.nj.nec.com/cache/papers/cs/11809/http:zSzzSzblack.csl.uiuc.eduzSz~piyushzSz.zSz.zSzcapacity.pdf/gupta99capacity.pdf
6. Bugra Gedik, Ling Liu, and Philip Yu. ``ASAP: An Adaptive Sampling Approach to Data Collection in Sensor Networks'', IEEE Transactions on Parallel and Distributed Computing (TPDS).
7. Bugrg Gedik and Ling Liu. ``Protecting Location Privacy with Personalized k-Anonymity: Architecture and Algorithms''. IEEE Transactions on Mobile Computing. (This article was featured in PHYSORG.com Technology Section, December 2007).
8. Bugra Gedik and Ling Liu. ``Quality-Aware Distributed Data Delivery for Continuous Query Services'', ACM 2006 International Conference on Management of Data (ACM SIGMOD), Chicago, June 26-29, 2006.
9. J. Hubaux et al. *Toward Self -Organized Mobile Ad Hoc Networks: The Terminodes Project*. IEEE Communications Magazine, January, 118-124, 2001. http://www.comsoc.org/ci/private/2001/jan/pdf/hubaux.pdf
10. Carlo Kopp, *Ad Hoc Networking*, Monash University, Australia, Background Article, Systems, June, 1999. http://www.csse.monash.edu.au/research/san/AdHocNetworks.pdf.

11. J Kong, H Luo, K Xu, D L Gu, M Gerla, S Lu: *Adaptive Security for Multi-layer Adhoc Networks*, Special Issue of Wireless Communications and Mobile Computing, 2002, Wiley Interscience Press.
12. A. Menezes, P. Oorschot, S. Vanstone, *Handbook of Applied Cryptography*, CRC Press, Boca Raton, London, New York, Washington, D.C. 1997.
13. Ram Ramanathan and Jason Redi. *A Brief Overview of Ad Hoc Networks: Challenges and Directions.* IEEE Communications Magazine, May, 20-22, 2002. 26 J. Freebersyser and B. Leiner, *A DoD Perspective on Mobile Ad Hoc Networks, Ad Hoc Networking*, ed. C. E. Perkins, Addison-Wesley, 2001, pp. 29–51. 27 IETF, *Mobile Ad -hoc Networks (manet), Charter* http://www.ietf.org/html.charters/manet-charter.html
14. R. Ramanujan, A. Ahamad, J. Bonney, R. Hagelstrom, and K. Thurber. *Techniques for intrusion-resistant ad hoc routing algorithms (TIARA).* MILCOM 2000. 21st Century Military Communications Conference Proceedings, Volume: 2 , 2000, Pages 660 –664.
15. T. Schaefer, P. Smith, M. Schoeller, A. J. Mohammad, J. P. Rohrer, D. Hutchison, and J. P. G. Sterbenz. Towards a Decision Engine for Self-Remediating Resilient Networks. In Second International Workshop on Self-Organizing Systems (IWSOS) pages 12~14, September 2007.
16. Mudhakar Srivatsa, Arun Iyengar, Jian Yin, Ling Liu. ``Scalable Key Management Algorithms for Location Based Services", IEEE/ACM Transactions on Networking.
17. Mudhakar Srivatsa and Ling Liu. "Secure Event Dissemination in Content-Based Publish-Subscribe Networks". Proceedings of 27th IEEE International Conference on Distributed Computing Systems (ICDCS 2007).
18. Mudhakar Srivatsa and Ling Liu. ``Securing Publish-Subscribe Overlay Services with EventGuard", Proceedings of ACM Computer and Communication Security (CCS 2005),November 7-11, 2005, Hilton Alexandria Mark Center, Alexandria, VA, USA.
19. Mudhakar Srivatsa, Arun Iyengar, Jian Yin and Ling Liu. ``Access Control in Location-based Broadcast Services", Proceedings of The 27th IEEE International Conference on Computer Communications (INFOCOM 2008), Phoenix.
20. Mudhakar Srivatsa, Arun Iyengar, Jian Yin and Ling Liu, "A Middleware System for Protecting Against Application Level Denial of Service Attacks" , Proceedings of 7th ACM/IFIP/USENIX International Middleware Conference (Middleware 2006)
21. Mudhakar Srivatsa and Ling Liu. "Key Derivation Algorithms for Monotone Access Structures in Cryptographic File Systems" , Proceeding of 11th European Symposium on Research in Computer Security (ESORICS 2006) be held in Hamburg (Germany), 18-20 September 2006.
22. Frank Stajano and Ross Anderson. *The Resurrecting Duckling: Security Issues for Ad-hoc Wireless Networks*. In Security Protocols, 7th International Workshop, volume 1796 of Lecture Notes in Computer Science. Springer Verlag, 1999. http://www-lce.eng.cam.ac.uk/~fms27/papers/duckling.pdf
23. Frank Stajano. *The resurrecting duckling -- What next?,* In Proceedings of the 8th International Workshop on Security Protocols, Lecture Notes in Computer Science. Springler-Verlag, Berlin, Germany, April 2000. http://citeseer.nj.nec.com/stajano00resurrecting.html
24. F. Stajano and R Anderson, *The Resurrecting Duckling: Security Issues for Ubiquitous Computing*. Security & Privacy 2002 - Supplement to COMPUTER, 22-26, 2002. http://www.computer.org/security/supplement1/sta/print.htm
25. Li Xiong and Ling Liu. "PeerTrust: Supporting Reputation-Based Trust for Peer-to-Peer Electronic Communities", IEEE Transactions on Knowledge and Dat a Engineering, Vol.16, No. 7 (July 2004). Special issue on Peer to Peer Based Data Man agement. pp 843-857.
26. Panlong Yang and Shaoren Zheng. *Security management in hierarchical ad hoc network*. 2001. Proceedings. ICII 2001 - Beijing. (2001 International Conferences on Info-tech and Info-net), Volume: 2 , 2001. Page(s): 642 -649 vol.2
27. Seung Yi, Robin Kravets, *Practical PKI for Ad Hoc Wireless Networks*, University of Illinois at Urbana-Champaign, Department of Computer Science, 1304West Springfield Avenue, Urbana, IL 61801-2987 USA, August, 2001. http://www-old.cs.uiuc.edu/Dienst/Repository/2.0/Body/ncstrl.uiuc_cs/UIUCDCS-R-2002-2273/pdf
28. L. Zhou and Z Haas. *Securing Ad Hoc Networks*. IEEE Network, November/December, 24-30, 1999. http://www.cs.cornell.edu/home/ldzhou/adhoc.pdf
29. Mullender, Sape (ed.): *Distributed Systems*, second edition, Earth, ACM Press, 1993.