IEEE-International Conference on Signal processing, Communications and Networking
Madras Institute of Technology, Anna University Chennai India, Jan 4-6, 2008. pp167-172

Who is Listening? Security in Wireless Networks

Mudhakar Srivatsa
IBM T.J. Watson Research Center, Yorktown Heights, NY-10562, USA
msrivats@us.ibm.com

Abstract[1]

Wireless networks have significantly impacted the world as far back as World War II. Through the use of wireless networks, information could be sent overseas or behind enemy lines easily and quickly. Since then wireless networks have continued to develop and its uses have significantly grown. This rapid proliferation of wireless networks has been closely accompanied by an increasing number of security threats. This paper describes an overview of security issues in wireless networks. Security issues in wireless networks span multiple layers including physical layer, network layer and application layer and encompass cross-layer attacks based on identity management and side channels. This paper discusses some prominent security issues in the context of wireless networks and presents qualitative arguments that demonstrate the infeasibility of building unbreakable security mechanisms under a bounded resource model. Hence, it is becomes crucial to identify trade-offs between attack and defense strategies and their cost structures (such as performance overhead). The paper concludes with a discussion on an emerging paradigm for achieving a quantifiable level of security using a risk analysis approach that captures the notion of risk and pricing.

1 Introduction

Wireless communications offer organizations and users many benefits such as portability and flexibility, increased productivity, and lower installation costs. Wireless technologies cover a broad range of differing capabilities oriented toward different uses and needs and can be categorized along the following dimensions: fixed Vs mobile network, single hop Vs multi-hop network, device type (sensor motes, handheld PDAs, laptops), etc. Wireless local area network devices (Wi-Fi 802.11x [5]) that operate up to a range of 150 feet, for instance, allow users to move their laptops from place to place within their offices without the need for wires and without losing network connectivity. Emerging wireless metropolitan area network devices (WiMAX [15]) operate within a range of 3-10 miles and allow users to commute at 60 mph while sustaining high data rates. Such technologies enable a large number of location-based services (e.g.: Find the cheapest gas station within a 5 mile radius?). Ad hoc networks, such as those enabled by Bluetooth [10], allow data synchronization (e.g.: personal databases on PDAs and cell phones) with network systems and application sharing (e.g.: printing service) between devices.

Emerging technologies have extended single hop wireless networks (or last hop wireless networks) that do not use wireless technologies for packet routing and forwarding to multi-hop wireless networks. For instance, sensor networks are used to monitor physical or environmental conditions (e.g.: weather monitoring, pH-level monitoring in a river) and route the collected data to a base station using a multi-hop wireless network. Mobile ad hoc networks (MANET) [17] is a self-configuring network of mobile devices; mobile devices are free to move randomly and organize themselves arbitrarily, thus, the wireless network topology may change rapidly and unpredictably. Unlike the sensor networks there may be no pre-designated data sink (base station) in a MANET. MANETs (see Figure 1) find a wide variety of military applications (audio/video surveillance), coordinating an emergency response team from command & control and intelligent vehicular routing applications.

The ubiquitous growth of wireless networks has been closely followed by a splurge of security attacks. Unfortunately, security risks are inherent in any wireless technology. Some of these risks are similar to those of wired networks; some are exacerbated by wireless connectivity; some are new. First, the most significant source of risks in wireless networks is that the technology's underlying communications medium, the airwave, is open to intruders. Second, mobile and handheld wireless devices are resource constrained (e.g.: battery life); hence such devices have limited transmission power and may use weaker cryptographic mechanisms for saving power, thereby making them easy targets for powerful adversaries. Third, the lack of trusted third party (TTP) or a certification authority (CA) in ad hoc wireless networks pose serious

[1]This research was sponsored by the U.S. Army Research Laboratory and the U.K. Ministry of Defense and was accomplished under Agreement Number W911NF-06-3-0001. The views and conclusions contained in this document are those of the author(s) and should not be interpreted as representing the official policies, either expressed or implied, of the U.S. Army Research Laboratory, the U.S. Government, the U.K. Ministry of Defense or the U.K. Government. The U.S. and U.K. Governments are authorized to reproduce and distribute reprints for Government purposes notwithstanding any copyright notation hereon.

challenges to identity and trust management. Fourth, a multi-hop wireless network inherently assumes cooperation between nodes for packet routing and forwarding, whereas a compromised node may refuse to cooperate (by being greedy or malicious). Fifth, handheld mobile devices cannot afford the same level of physical security as an enterprise server and thus, may be easily stolen.

A direct consequence of these risks is the loss of data confidentiality and integrity and the threat of denial of service (DoS) attacks to wireless communications. Unauthorized users may gain access to agency's system and information, corrupt the agency's data, consume network bandwidth, degrade network performance, launch attacks that prevent authorized users from accessing the network, or use agency's resources to launch attacks on other networks. Specific threats and vulnerabilities to wireless networks include the following:

Physical Layer Attack: DoS attacks may be directed at wireless connections or devices. Resource constrained mobile devices are susceptible to radio frequency jamming and interference attacks from powerful adversaries. Such attacks can target wireless devices that operate on a narrow frequency band (e.g.: 2.402-2.48GHz in Bluetooth).

Network Layer Attacks: Malicious entities may deploy unauthorized equipment (e.g., mobile devices and access points) to surreptitiously gain access to sensitive information. Malicious entities may, through wireless connections, connect to other agencies or organizations for the purposes of launching attacks and concealing their activities. Further, in a multi-hop wireless network, a malicious entity may falsely route packets, drop packets, advertise incorrect routes (e.g.: routing loops, routing black holes), incorrectly code and aggregate packets, etc.

Mobile Device Attacks: Sensitive information that is not encrypted (or that is encrypted with poor cryptographic techniques) and transmitted between two wireless devices may be intercepted and disclosed. Handheld devices are easily stolen and can reveal sensitive information, especially in the absence of tamper resistant hardware. Viruses or other malicious code may compromise a wireless device and subsequently be introduced to a wired network connection.

Identity Attacks: Malicious entities may steal the identity (MAC address) of legitimate entities and masquerade as them on internal wireless networks. The absence of a certification authority in ad hoc wireless networks allows a malicious node to masquerade any identity and assume any number of identities. Such identity spoofing attacks can adversely affect commonly used leader election and redundancy control protocols.

Side Channel Attacks: The open nature of the wireless medium makes wireless devices vulnerable to side channel attacks. A side channel attack uses information gained from the physical implementation of system, rather than theoretical weakness in its algorithms. A malicious entity may use RF localization, power estimation, traffic analysis, etc to infer position, movement and activity level even in a *secure* wireless network.

The rest of this paper describes security threats and solution methodologies in the most general form of wireless networks, namely, mobile ad hoc wireless networks. We show that while it is infeasible to build unbreakable security mechanisms, one can exploit trade-offs between attack and defense strategies and their cost structures to achieve pragmatic security. The arguments presented in this paper steer towards a new and emerging approach based on quantitative risk analysis.

2 Physical Layer Security

The physical layer communication medium used in wireless networks (the airwave) is open to jamming (interference) and eavesdropping attacks from intruders. Eavesdropping at the physical layer refers to hiding the very existence of a node or the fact that communication was even taking place from an adversary. A common solution to achieve physical layer security is to use spread spectrum codes. Spread spectrum (SS [18, 11]) generally makes use of a sequential noise-like signal structure to spread the normally narrowband information signal over a relatively wideband band of frequencies. This is achieved using a spreading code or key, which must be known in advance by the transmitter and receiver(s). The codes are generated as keyed pseudo-random number (PRN) sequences that are long and appear as *noise-like* as possible for receivers that do not possess the key.

Resistance to jamming (interference): In narrowband systems where the signal bandwidth is low, the received signal quality will be severely lowered if the jamming power happens to be concentrated on the signal bandwidth. A narrowband jamming affects spread spectrum data transmission about as much as if the amount of jamming power is spread over the whole signal bandwidth, when it will often not be much stronger than background noise. However, a persistent and powerful adversary can *always* jam all data transmissions by transmitting high power white noise over the entire frequency spectrum.

Resistance to eavesdropping: The spreading code (in Direct Sequence SS systems) or the frequency-hopping pattern (in Frequency Hopping SS systems) is often unknown by anyone for whom the signal is unintended, in which case it *encrypts* the signal and prevents the adversary from making sense of it. Since the signal power is spread over a large bandwidth, the signal power spectral density (PSD) is much lower, often significantly lower than the noise PSD, making it hard for the adversary to

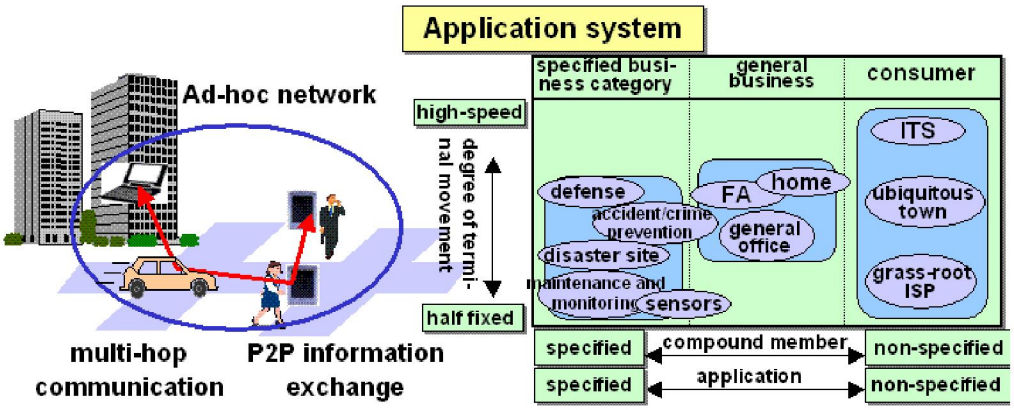

Figure 1: Mobile Ad Hoc Wireless Network (courtesy: Hitachi)

determine if the signal exists at all.

However, there is key difference between traditional cryptographic primitives (such as symmetric key encryption, public-key signatures, etc) and spread spectrum systems. Cryptographic primitives can assume a large key space (128 bits) and thus ensure that a successful attack is nearly infeasible under standard computational models. On the other hand, the key space in a spread spectrum system is limited by the range of carrier frequencies, which is typically no more than a few Giga-Hertz[2]. The carrier frequency range is usually quantized (in steps of 100 KHz) to accommodate background noise, low power interference and multi-path effects. This reduces the key space in spread spectrum systems to about 24 bits. Hence, a persistent and powerful adversary can jam and eavesdrop with high probability. However, the probability of a successful attack varies with the amount of resources *invested* by an adversary. A rational adversary with a bounded amount of resources is forced to analyze its return on investments (RoI) and thus spend its resources wisely. This observation consequently leads us to a quantitative risk analysis based approach to security (see Section 7).

3 Network Layer Security

In a single hop (or last hop) wireless networks, the nodes do not participate in network layer activities such as packet routing and forwarding. In this section, we address network layer security issues in a multi-hop wireless networks. Multi-hop wireless networks use nodes for three primary network layer functionalities: packet routing and forwarding, packet coding and packet data aggregation. An adversary may compromise one or more nodes in the wireless network and use them to falsely route packets, drop packets, advertise incorrect routes (e.g.: routing loops), improperly code packets, improperly aggregate packet data, etc. In the rest of this section we describe each of these three functionalities in detail and describe relevant attacks associated with them.

Packet Routing and Forwarding: In figure 2, a node S may send packets to a destination D through a path $\langle S, A, B, D\rangle$; here, nodes A and B perform packet forwarding function to deliver packets. Additionally, node S requires cooperation from other nodes to discover a route to node D (route set up and discovery). A malicious node can create a *black hole* by advertising low cost routes and drop all packets routed to it, destabilize routes, and create routing loops. There is an inherent trade off between the robustness and the communicating cost of packet routing and forwarding protocol. For instance, if each node uses a broadcast (flooding) protocol, it may maximize the probability that a packet from S reaches D; however, its packet forwarding cost is linear in the size of the network. In any event, if an adversary can partition the network (by compromising a *vertex cut*) then it can completely control all communications between the partitions. Fortunately, in a mobile network the topology changes dynamically and arbitrarily; and thus the vertex cut is not static. Hence, an adversary is forced to invest more resources in attempting to compromise new nodes as the topology changes. On the other hand, the network may invest more resources into increasing the mobility of nodes to defend against network partitioning attack. In the limiting case, if the network had infinite resources for mobility, then it does not have to use multi-hop routing protocols; the communicating parties can move closer to one another and correspond over a direct channel. In a realistic scenario, the network operating under a bounded security budget has to wisely spend its resources in a way that best defends adversarial attacks.

In a typically sensor mote, transmitting one bit expends as much energy as executing 800 instructions [8]. Hence, wireless networks use in-network data processing techniques (e.g.: packet coding techniques and aggregation) to reduce transmission costs. In-network data processing techniques introduce additional challenges (packet data confidentiality and integrity) as discussed below.

[2]Note that higher carrier frequencies draw more energy and thus drain battery life quickly

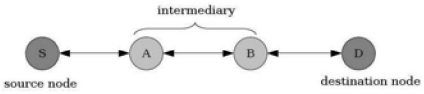

Figure 2: Packet Routing and Forwarding

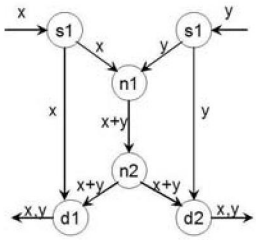

Figure 3: Network Coding

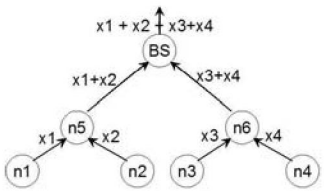

Figure 4: In-Network Aggregation

Packet Coding: Figure 3 shows a simple example of packet coding. Let us suppose there are two sources s_1 and s_2 each of which generate data streams x_i and y_i at the rate of one bit per second. All wireless channels can carry at most one bit per second. There are two destination nodes d_1 and d_2 both of which need the bit streams x_i and y_i. One can show that no packet routing and forwarding scheme can achieve the goal of delivering both x_i and y_i to both d_1 and d_2. On the other hand, this goal can be met if n_1 uses packet coding and transmits $x_i \oplus y_i$ (see Figure 3). In addition to packet forwarding and routing attacks, the node may improperly execute packet coding. One may use erasure coding techniques [19] to improve the robustness of network coding based routing protocols.

In-Network Aggregation: In a sensor network, the base station may not be interested in collecting all the raw data; but may require only some aggregates on the raw data such as `sum, average, count, variance, min, max, etc`. Hence, sensor nodes may perform in-network packet data aggregation (see Figure 4) to reduce transmission costs. In addition to packet forwarding and routing attacks, a malicious node may improperly execute the aggregation operator. However, one may exploit the statistical properties of aggregation operators and a data model (for raw data) to limit the extent of damage caused by malicious nodes [2].

We now argue that in-network processing techniques (and subsequent reduction in transmission costs) result in more security issues and/or performance overheads. We use packet data confidentiality and integrity as a sample security property. In a simple packet forwarding scenario a source S and destination D can protect packet data confidentiality and integrity using payload encryption (e.g: AES [14]) and keyed message authentication codes (MAC [9]) even if the packet forwarding nodes (A and B in Figure 2) were malicious. In network coding schemes, confidentiality from packet coding and forwarding nodes (n_1 and n_2 in Figure 3) can be achieved using payload encryption; however, it may not be possible to generate $MAC(x_i \oplus y_i)$ from $MAC(x_i)$ and $MAC(y_i)$[3]. One possible approach is to use a computation intensive Goldwasser-Micali [6] digital signature that is homomorphic on the $\oplus$ operator. In the aggregation schemes, it is hard to maintain both confidentiality and integrity data from forwarding and aggregating nodes (n_5 and n_6 in Figure 4). One possible approach is to use homomorphic encryption schemes (Benolah [1] and Paillier [16]); however, there is no known cryptosystem which preserves the ring structure of the plaintexts, i.e. allows both addition and multiplication on a group. In the absence of efficient cryptographic primitives, the network is faced with the challenge of effectively trading off efficiency (say, by turning off in-network aggregation) with the goal of improving its resilience to network layer attacks. If a resource constrained multihop wireless network wishes to take zero risk, then it is not useable; instead the network should operate under a bounded risk budget while maximizing its usability.

[3]One solution is to attach both $MAC(x_i)$ and $MAC(y_i)$; however, this increases packet size

4 Mobile Device Security

Unlike wired networks, mobile and handheld devices may be deployed in hostile environments that cannot afford physical security. Such devices may be stolen and subjected to physical attacks that attempt to tamper them with the goal of extracting sensitive data (such as private keys). Given physical access to the device the attacker can launch several attacks: (i) physical attack of various forms (micro-probing, drills, files, solvents, etc.), (ii) freezing the device, (iii) applying out-of-spec voltages or power surges, (iv) applying unusual clock signals, and (v) inducing software errors using radiation. Tamper resistant chips may be designed to zero their sensitive data if they detect penetration of their security encapsulation or out-of-specification environmental parameters (even after its power supply has been crippled). Nevertheless, it is practically impossible to totally eliminate tampering by a sufficiently motivated opponent.

However, an adversary has to take the risk of stealing the device and invest considerable resources (including time) to tamper it. Fortunately, all tampering mechanisms are not perfect either. Some mechanisms (like micro-probing) take longer; some of the data may get corrupted when attempting the physically tamper the device; corrupted portions of the data may be hard to recover. For instance, corrupted bits in a text file are easily recovered, while those in a randomly generated cryptographic key are much harder to guess; e.g.: corrupted

text: `komputer`; recovered text: `computer`; corrupted key: `0x1a35fd86`; recovered key: `??`. Hence, the goal of a tamper resistant device is to sufficiently increase the tampering cost, making the device invulnerable in practice.

5 Identity Management

One can have, some claim, as many electronic personas as one has time and energy to create.
–Judith S. Donath [4]

Naming service (e.g. domain name service (DNS)) is one of the core services offered by any network. In an open ad hoc network wherein arbitrary nodes can join the network, it is hard to verify the identity and the credentials associated with a new node in the absence of a common certification authority (CA). The worst case scenario manifests itself as a Sybil attack. In a Sybil[4] attack [4], a single malicious entity presents multiple identities and uses them to gain a disproportionately large influence, thereby undermining the outcome of de facto election algorithms and redundancy control algorithms. Theoretically, in the absence of a trusted authority, an arbitrarily powerful adversary can forge infinitely many identities without being detected by the network.

However, in practice, a network's vulnerability to a identity attacks depends on how cheaply identities can be generated, the degree to which the network accepts inputs from entities that do not have a chain of trust linking them to a trusted authority, and whether the network treats all entities identically. This observation opens up multiple research challenges in identity management:

Federated Identity: A federated identity represents a virtual union, or assembled identity, of an entity, stored across multiple identity management systems. Federated identity management extends the notion of a traditional identity to encompass contextual information about an entity; for example, a GPS service may additionally associate a spatial-temporal coordinate with an entity. A federated identity management system may exploit trust relationship between different identity management systems to constrain the number of identities spoofed by an adversary.

Resource Challenge: An orthogonal approach to mitigate identity attacks is to use resource challenges. An example of a CPU resource challenge is a cryptographic puzzle [7, 20]. A cryptographic puzzle ensures that if an adversary has ρ times as computationally powerful as the network nodes, then the adversary can spoof no more than ρ identities. Other challenge mechanisms focus on memory size (using matrix inversion test) and the number of radios available at a malicious entity (number of simultaneous conversations) and limit the number of spoofed identities.

RF Localization: The neighbors of a malicious entity may use RF localization techniques [13] to determine the physical coordinates of a malicious entity. In the event of a Sybil attack, the purported locations of all fake identities reported by a malicious entity would appear geographically clustered (within a small radius). Standard detection theoretic approaches (e.g.: hypothesis testing) can be used to analyze cluster size and cluster radius to detect spoofed identities.

Similar to previous security issues discussed in this paper, it is theoretically impossible to completely eliminate Sybil attack in the absence of a central trusted authority (say, in an ad hoc network setting). Solutions described above attempt to constrain the number of spoofed identities allowing the network to operate under a bounded risk setting.

6 Side Channel Attacks

The open nature of the wireless medium makes wireless devices vulnerable to side channel attacks. In particular we describe traffic analysis and power analysis attacks.

Traffic analysis allows an attacker, in a more subtle way, to gain intelligence by monitoring the transmissions for patterns of communication. Traffic analysis attack does not attempt to inspect the payload in a packet (payload may be encrypted), instead it attempts to infer the intentions and actions of the enemy by observing communication patterns. Example patterns include: (i) Frequent communications can denote planning, (ii) Rapid, short, communications can denote negotiations, (iii) lack of communication can indicate a lack of activity, or completion of a finalized plan, (iv) Frequent communication to specific stations from a central station can highlight the chain of command, etc.

Power analysis techniques allow an attacker to determine the distance to transmitter and the transmitter power level. The received power approximately decays with square of distance: $P_{rx} \propto \frac{P_{tx}}{d^2}$. Knowing the transmit power P_{tx}, three or more attackers can estimate the exact location of transmitter tx using simple geometric triangulation. Hence, the attacker can track the mobility pattern of a mobile device over a period of time. Knowing the distance d, the attacker can estimate the transmit power P_{tx}; a larger transmit power indicates long distance (and directional) communication, while a smaller transmit power indicates short distance communication. Hence, the attacker can use this information to infer the intended recipient of the transmitted message. In a military setting, such mobility patterns and 'who is talking to whom' patterns may reveal strategic information to the adversary.

[4]Named after the subject of the book *Sybil*, a case study of a woman with multiple personality disorder

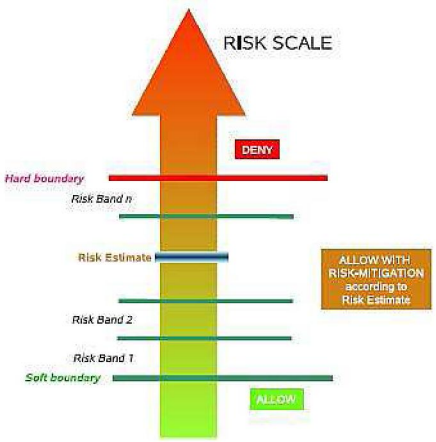

Figure 5: Risk-Adaptive Access Control on a Risk Scale [3]

7 Risk Analysis

Traditional security mechanisms adopt a 0/1 approach to security. For instance, the problem of breaking cryptographic protocols is reduced to NP-hard problems; thus, it would be infeasible to break an ideal implementation of the protocol. However, as pointed out in the earlier sections, a wireless network is vulnerable to a wide range of physical, network, application, identity and side channels attacks making it practically impossible to design secure protocols whose hardness properties can be reduced to NP-hard problems.

However, there are two crucial observations: (i) the ability of a network to defend itself is limited by its resources, and (ii) the ability of an adversary to launch effective attacks is limited by its resources. Under a bounded resource model, this problem may be formally studied using literature from quantitative risk analysis. This approach has gained lot of visibility in the security domain due to the JASON report on horizontal integration [12] which was commissioned to investigate barriers in information sharing and the risk of information leakage. Following the report, FuzzyMLS [3] proposed a risk based access control model that expands the well-known and practiced Bell-LaPadula model multi-level security (MLS) access control model. Fuzzy MLS (in a limited context) is used to quantify risk associated with information access. The ability to quantify risk makes it possible to treat risk that an organization is willing to take as a limited and countable resource. This enables the use of a variety of economic principles to manage this resource with the goal of achieving the optimal utilization of risk, i.e, allocate risk in a manner that optimizes the risk vs. benefit tradeoff.

8 Summary

In this paper, we have described an overview of security issues in wireless networks at different layers including physical layer, network layer and device layer and cross layer attacks based on identity management and side channels. We have argued in the context of wireless networks that on one hand, it may be hard to secure a mobile device to an extent that renders attacks infeasible and sophisticated defense mechanisms may be highly resource intensive; on the other hand, attacks are not guaranteed to be error-free and complicated attacks drain adversarial resources. Based on these observations, we have described an emerging paradigm under a bounded resource model whose goal is to maximize the usability and performance of the system while operating under a bounded risk budget.

Acknowledgements: This overview paper draws on a vast body of literature (too numerous to enumerate) in the general area of security in mobile ad hoc networks. In particular, the author benefited from discussion with several members held during the ITA program. The author extends special thanks to Pankaj Rohatgi, Pau-Chen Cheng, Dakshi Agrawal and colleagues from University of York for their insightful remarks.

References

[1] J. Benaloh. Dense probabilistic encryption. In *http://research.microsoft.com/crypto/papers/dpe.ps*.
[2] H. Chan, A. Perrig, and D. Song. Secure hierarchical innetwork aggregation in sensor networks. In *ACM CCS*, 2006.
[3] P. C. Cheng, P. Rohatgi, and C. Keser. FuzzyMLS: An experiment on quantified risk-adaptive access control. In *IEEE Symposium on Security and Privacy*, 2007.
[4] J. Douceur. The sybil attack. In *2nd IPTPS Workshop*, 2002.
[5] M. Gast. 802.11 wireless networks. In *O'Reilly Networking, ISBN: 0596001835*, 2002.
[6] S. Goldwasser and S. Micali. Probabilistic encryption and how to play mental poker keeping secret all partial information. In *14th ACM STOC, pp 365377*, 1982.
[7] A. Juels and J. Brainard. Client puzzle: A cryptographic defense against connection depletion attacks. In *NDSS*, 1999.
[8] C. Karlof and D. Wagner. Secure routing in wireless sensor networks: Attacks and countermeasures. In *Elsevier's AdHoc Networks Journal*, 2002.
[9] H. Krawczyk, M. Bellare, and R. Canetti. HMAC: Keyed-hashing for message authentication. http://www.faqs.org/rfcs/rfc2104.html.
[10] M. Miller. Discovering bluetooth. In *Sybex Inc, ISBN: 0782129722*, 2001.
[11] J. S. Min and H. Samueli. Analysis and design of a frequency-hopped spread-spectrumtransceiver for wireless personal communications. In *IEEE Transactions on Vehicular Technology Volume 49, Issue 5, pp: 1719 - 1731*, 2000.
[12] MITRE. Horizontal integration: Broader access models for realizing information dominance. In *Corporation Jason Program Office JSR04132, http://www.fas.org/irp/agency/dod/jason/classpol.pdf*, 2004.
[13] D. Nicelescu and B. Nath. Ad hoc positioning (APS) using AOA. In *Proceedings of IEEE Infocom, pp: 1734-1743*, 2003.
[14] NIST. AES: Advanced encryption standard. http://csrc.nist.gov/CryptoToolkit/aes/.
[15] F. Ohrtman. WiMAX handbook. In *McGraw Hill Communications, ISBN: 0071454012*, 2005.
[16] P. Paillier. Public-key cryptosystems based on composite degree residuosity classes. In *EUROCRYPT pp223-238*, 1999.
[17] Y. Pan and Y. Xiao. Ad hoc and sensor networks, wireless networks and mobile computing. In *Nova Science Publishers, ISBN: 1-59454-396-8*, 2005.
[18] R. Pickholtz, D. Schilling, and L. Milstein. Theory of spread-spectrum communications. In *IEEE Transactions on Communications Volume 30, Issue 5, pp: 855 - 884*, 1982.
[19] L. Rizzo and L. Vicisano. A reliable multicast data distribution protocol based on software fec techniques. In *4th HPCS*, 1997.
[20] X. Wang and M. K. Reiter. Defending against denial-of-service attacks with puzzle auctions. In *IEEE Symposium on Security and Privacy*, 2003.