Securing a Wireless World

Hao Yang[1], Fabio Ricciato[2], Songwu Lu[1], Lixia Zhang[1]
[1]Computer Science Department, UCLA, Los Angeles, USA
[2]Forschungszentrum Telekommunikation Wien, Vienna, Austria
Email: [1]{hyang, slu, lixia}@cs.ucla.edu [2]ricciato@ftw.at

***Abstract*— Securing wireless networks poses unique research challenges. In this paper, we survey the state-of-the-art approaches to providing security for three popular wireless networking paradigms, namely IEEE 802.11 based WLANs, 3G cellular networks, and mobile ad-hoc networks. We identify the security threats as well as examine the current solutions. We further summarize lessons learned, discuss open issues, and identify future research directions.**

I. Introduction

Wireless networking has been experiencing an explosive growth in recent years, which resembles the rapid growth of the Internet itself in mid 1990's. Wireless networks offer attractive flexibility and coverage to both network operators and users. Ubiquitous network coverage, for both local and wide areas, can be provided without the cost of deploying and maintaining the wires. Mobility support is another salient feature of wireless networks that grant the users not only "anytime, anywhere" network access, but also the freedom of roaming while networking. Recent advances in wireless communication technology have offered ever increasing data rates, in some cases comparable to their wired counterparts.

Despite their promising future, security has become one major concern in wireless networks, with the risk of hampering or delaying the migration of value-critical services (e.g. e-commerce, e-banking) towards wireless platforms. In this article we assess security threats in wireless networks and survey countermeasures along the following two dimensions:

- *Information Security*, i.e., to provide confidentiality, integrity, authentication, and non-repudiation for two entities that communicate through the network.
- *Network Security*, i.e., to protect the networking system as a whole and sustain its capability to provide connectivity between the communicating entities.

Although most, if not all, security threats against the TCP/IP stack in a wired network are equally applicable to an IP-based wireless network, the latter possesses a number of additional vulnerabilities that make it more challenging to secure:

- *Open Wireless Access Medium*: The security threats of message eavesdropping and injection are universe in any network; however they are particularly severe in wireless networks due to the open wireless medium. With off-the-shelf hardwares and little efforts, an attacker can intercept and inject traffic through a wireless channel. There is no physical barrier to separate the attacker from the network, as is the case in wired networks.
- *Limited Bandwidth*: Wireless networks are particularly vulnerable to Denial-of-Service (DoS) attacks due to their limited bandwidth and in-band signaling. Although the wireless channel capacity is continuously increasing, the spatial contention problem poses a fundamental limit on network capacity. One can deploy redundant fibers, but everyone must share the same wireless spectrum.
- *System Complexity*: Generally speaking wireless networks are far more complex than their wired counterparts due to the special needs for mobility support and efficient channel utilization. Each piece of complexity added into the system can introduce potential security vulnerabilities, especially in systems with a large user population and a complex infrastructure, such as 3G networks.

Recent years have witnessed a plethora of efforts on wireless security, with the outcome of a rich body of proposed solutions. In this article we assess security threats and summarize representative proposals for three popular wireless networking paradigms, namely wireless Local Area Networks (WLANs), 3G cellular networks, and ad-hoc networks. The IEEE 802.11 WLANs use stationary Access Points (APs) to extend network connectivity by one-hop wireless links, and are widely deployed in campuses, corporations and homes. The 3G networks are the next-generation wireless telecommunication systems providing wide-area data services for global subscribers. Since 2003, several 3G networks has become operational in Asia, Europe, and North America. In the absence of a deployed infrastructure, multiple wireless devices can self-organize into an ad-hoc network and forward data through multihop wireless links to enable peer-to-peer communication or further extend the network coverage. As we shall see, each type of these wireless networks has its own set of vulnerabilities that need to be addressed.

The WLAN is perhaps the simplest form of wireless networks among the above three, since it involves only one-hop wireless access from a small number of local users. The WLAN security solutions focus on applying cryptographic techniques to enhance the wireless link with data privacy and integrity. The network infrastructure, e.g., the APs, is assumed to be trusted, and the network security is achieved mainly through authentication that prevents unauthorized access in the first place. We discuss these security issues in Section II.

Similar to the WLAN, information security in 3G networks can be achieved through cryptographic encryption and authentication. However, the large network scale, increased system complexity, and heavy signaling interactions bring additional risks for the security the 3G network infrastructure. These aspects have not yet been adequately investigated, partially due to the quite recent commercial launch of 3G services, and considerable research efforts are required to display hidden problems and potential solutions. These are discussed in Section III, together with an overview of the existing security mechanisms in 3G networks.

The self-organized nature of ad-hoc networks present additional security challenges. Because a malicious entity can readily participate as a router that forwards packets for peer nodes, it can attack both the control plane (ad-hoc routing) and the data plane (multi-hop forwarding) in the network. These security issues are addressed in Section IV.

After surveying the security threats and proposed solutions in these wireless networks, we summarize the lessons learned and shed light on future research directions in Section V.

II. Security for Wireless LAN

In this section we describe the security threats and solutions in an IEEE 802.11 WLAN. We start with a brief overview of the WLAN architecture, then analyze its security vulnerabilities, followed by detailed descriptions of the WLAN security standards, including WEP, WPA, and 802.11i.

A. Background

1) WLAN Architecture: In a typical WLAN the wireless devices, also called Stations (STAs), communicate with a centralized, stationary Access Point (AP) through the wireless channel. The AP is connected to a wired network and functions as an Ethernet switch that extends network connectivity to the wireless medium. The IEEE 802.11 standard [23] is a group of specifications that define the Physical (PHY) and Media Access Control (MAC) layers for WLANs. The first 802.11 standard was adopted in 1997, which defined 1 and 2 Mbps data rates in the unlicensed 2.4 GHz radio frequency band. Since then the 802.11 standard family has been extended several times to offer higher data rates. For example, 802.11b supports a maximum data rate of 11 Mbps, and 802.11a and 802.11g enable data rates up to 54 Mbps.

2) Security Threats: The 802.11 standard family faces a common set of security vulnerabilities due to the open wireless medium. We focus here on the security threats related to the wireless link between the stations and the AP, which is in many cases the last hop in the end-to-end path. We do not consider the security compromise of an AP nor the attacks on the wired network portion. The security threats in WLAN can be roughly divided into two categories based on their scope and impact. The first category includes attacks targeting the network infrastructure:

- *Channel Jamming*: The attacker can jam the wireless channel in the physical layer and effectively deny network access to legitimate users, independent from whether the network is secured.
- *Unauthorized Access*: When authentication is not turned on, as is the case in many deployed networks, the attacker can not only gain free network usage but also use the AP to bypass the firewall and access the internal network.
- *Traffic Analysis*: The attacker can analyze the overheard wireless traffic to obtain useful information, such as the network usage pattern.

The second category includes attacks against the communication between the station and the AP.

- *Eavesdropping*: When the wireless link is not encrypted, the attacker can eavesdrop all nearby communication. With advanced antennas it is possible to monitor wireless traffic from a few miles away.
- *Message Forgery*: When the wireless link is not protected for message integrity, the attacker can inject forged messages into both directions of the communication.
- *Message Replay*: Even when message integrity is enforced, the attacker can replay previously recorded messages, including authentication data.
- *Man-in-the-Middle Attack*: The attacker can manage to reside between the station and the AP, and intercept and modify the messages on-the-fly. For instance he can set up a rogue AP, or forge Address Resolution Protocol (ARP) replies that maps himself to the AP's IP address.
- *Session Hijacking*: The attacker can hijack an established session in two steps. He first breaks the session through wireless contention, then masquerades the legitimate station and replays the previous authentication messages.

The implementation of these attacks is not sophisticated and requires only off-the-shelf hardware and little system knowledge. In fact, several hacker toolsets are publicly available (e.g., Aerosol [1], AirSnort [2], WEPCrack [4]).

3) Solution Overview: The basic approach is to devise link-layer security mechanisms that enhance the open wireless links with the following features:

- *Access Control*, which prevents network access from unauthorized users.
- *Data Confidentiality*, which prevents revealing the content of the transmitted data.
- *Data Integrity*, which prevents tampering with the content of the transmitted data.
- *Mutual Authentication*, which allows two communicating parties to authenticate each other.

These link-layer mechanisms can provide strong information security by encrypting and integrity-checking every message. They also reduce network security threats by preventing unauthorized access. However, they do not address the jamming and traffic analysis attacks which require physical-layer solutions.

Data communication over WLAN can also be protected at the network layer and above through end-to-end mechanisms (e.g., IPSec, VPN). However, these solutions cannot address wireless-specific attacks, such as unauthorized access or man-in-the-middle attacks. They can be used to complement link-layer mechanisms and further enhance end-to-end data security. Due to space limits, we do not elaborate on this further.

B. WEP

The Wired Equivalent Privacy (WEP) protocol [23] was the first link-layer security mechanism introduced in 802.11 to provide a security level comparable to that with a physical wire. After its release, the hardware products supporting this

		► RC4 Encrypted ◄	
802.11 Hdr 4 bytes	IV/Key ID 4 bytes	Data (MPDU) >= 1 bytes	ICV 4 bytes

Fig. 1. WEP-encoded Data Frame

standard rapidly dominated the market. Unfortunately, several critical flaws in WEP were soon identified which can be exploited to defeat its security goals [12], [16], [19], [41].

1) Basic Primitives: WEP was designed to enforce data confidentiality, data integrity, and access control through the following primitives:

- *Encryption*: WEP encrypts data using a RC4-based stream cipher to achieve data confidentiality.
- *Integrity Checksum*: WEP uses Cyclic Redundancy Check (CRC) to compute integrity checksums for the messages.
- *Authentication*: WEP uses a challenge-response handshake based on pre-shared keys to authenticate the stations. The AP enforces access control by discarding all frames that are not properly encrypted.

Putting them together, the data transmission in WEP works in the following way. A secret key k is shared between two communicating parties. Given a message M, the sender (either the station or the AP) first computes a CRC checksum $c(M)$, then concatenates them into a plaintext

$$P =< M, c(M) > .$$

The sender chooses an *Initialization Vector* (IV) and uses the RC4 algorithm to generate a keystream $RC4(IV, k)$, which is a long sequence of pseudorandom bits. The length of IV is 24 bits. The key length has two popular choices, 40-bits or 104-bits keys, in the so-called 64-bits and 128-bits versions respectively (the difference in the notations can be explained by the 24-bits IV). The sender XORs the plaintext with the keystream into the ciphertext:

$$C = P \oplus RC4(IV, k)$$

Finally, the sender transmits the IV and the ciphertext C. The WEP-encoded data frame is depicted in Figure 1.

2) Insecurity of WEP: At the first glance, WEP seems to have well addressed the security needs in WLANs by encrypting and checksumming each message. However, subsequent cryptanalysis has shown otherwise, mostly due to the security flaws in the WEP design. In what follows we provide a sketch of these cryptanalysis results. Interested readers should refer to the literature (e.g., [16], [19], [12], [41]) for more details.

The first security flaw in WEP is keystream reuse, i.e., the same keystream being used to encrypt multiple messages. In such cases, the XOR-based stream cipher used in WEP can be easily broken to decrypt data traffic [16]. Because k is fixed, the same keystream is derived when IVs collide. Unfortunately, the fairly short length (24 bits) of IV poses a fundamental limit on the keystream space size, regardless of the key length. The chance of keystream reuse is further increased by sharing the key among multiple stations and the AP. Whenever two entities pick the same IV, the corresponding keystream is reused.

Linear checksum is the second security flaw in WEP, which can be exploited to modify messages in arbitrary ways [16]. In addition, because the checksum is unkeyed, the attacker needs only one valid keystream to inject forged messages. This further defeats the authentication mechanism, because the attacker can now successfully complete the challenge-response handshake without knowing the key.

The third security flaw in WEP is the weak RC4 keys [19]. With such weak keys input to RC4, a few initial bytes in the output contain recognizable patterns which can be exploited to recover part of the input key. The usage of RC4 in WEP is particularly vulnerable to weak keys, allowing the attacker to recover the entire key quickly [41]. Real implementations [2] show that it requires only 20,000 packets to recover the key, which takes less than one minute in a fully loaded AP.

C. WPA

In response to the security flaws in WEP, a new security standard for WLANs, called Wi-Fi Protected Access (WPA) [6], was released by Wi-Fi Alliance [5] in Oct. 2002. Today most Wi-Fi products in the market are WPA-compliant, or can be easily upgraded to support WPA.

1) Basic primitives: The primary goal of WPA is to amend the known security flaws in WEP yet retain backward compatibility with legacy WEP devices. Thus WPA is still based on the RC4 stream cipher to reuse the specialized hardwares that off-load the computation-intensive RC4 functions from CPU. By keeping the underlying cryptosystem intact, the new features in WPA can be incorporated into legacy WEP devices through software or firmware updates. WPA addressed the security flaws in WEP through the following primitives:

- *Temporal Key Integrity Protocol (TKIP)*, a new data encryption protocol that defeats the keystream reuse and weak key attacks.
- *Message Integrity Codes (MIC)* that defeats the message forgery attacks.
- *802.1x Authentication* that achieves strong authentication, authorization, and key management.

The details in TKIP and MIC are described below. The 802.1x authentication is presented in another article [40] in this issue.

2) TKIP: Similar to WEP, TKIP also XORs the plaintext with a random keystream to obtain the ciphertext. However, it derives the keystream in a way different from WEP, as shown in Figure 2. TKIP uses a 128-bits Temporal Key (TK) and a 48-bits IV. IV is reset to 0 whenever TK is changed, then incremented by one after each transmission. The 48-bits length guarantees that IVs will not be reused with the same TK, as it takes 600+ years to exhaust the IV space even at 54 Mbps.

As shown in Figure 2, TKIP uses a two-phase key mixing operation to derive the per-packet keystream, and each phase fixes one particular flaw in WEP. Phase 1 mixes TK with the first 4 bytes of IV and the sender's MAC address, and generates an intermediate key $P1K$. This prevents keystream reuse due to cross-station IV collision. Phase 2 takes input $P1K$ with TK and the last 2 bytes of IV to generate a unique 128-bit RC4 key. This decouples the known association between IV and the key, thus preventing exploiting weak keys

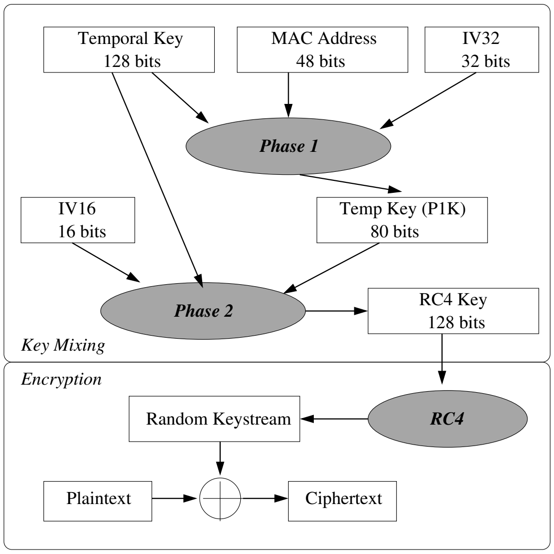

Fig. 2. Key Mixing and Data Encryption in TKIP

to recover TK. Finally, the RC4 key is used to generate the keystream, which is then XORed with the plaintext.

3) MIC: To protect message integrity, WPA uses cryptographic Message Integrity Codes (MIC) to replace the CRC checksum in WEP. The specific algorithm to compute the MIC is called Michael. Given a message, it first partitions the message into a sequence of 32-bits chunks and pads the last chunk, if not full, with $0x5A$ and enough zeros. An iteration is performed over the sequence. In each step, one chunk is mixed with the key using XORs, rotations, bit swaps, and little-Endian additions. The output of the algorithm is a 64-bit tag that serves as the MIC. One major concern in the design of Michael is to reduce the computational overhead. As a result, its defense against message forgery is weaker than one would expect. Although the MIC is 64-bit long, the best known attack using differential cryptanalysis can reduce its security level to 29 bits, that is, the attacker can forge any message using only 2^{19} MICs [25].

D. 802.11i

The IEEE 802.11 Task Group i (TGi) has recently proposed 802.11i [24], a new security standard for WLANs (ratified in June 2004). In fact, WPA was based on an earlier 802.11i draft, and all its essential features, such as TKIP/Michael, are retained in 802.11i. Wi-Fi Alliance has also adopted 802.11i as the next-generation WPA, so-called WPA2 [6]. One may view WPA as an interim step in the evolution from WEP to 802.11i. Products that are compliant with 802.11i are expected to be available by the end of 2004.

1) Basic primitives: The new cryptosystem used in 802.11i is the Advanced Encryption Standard (AES) that is provably secure against differential and linear cryptanalysis. The benefits of using AES is increased security in the long run. However, AES operations typically require a 64-bit co-processor to improve the performance. As a result, the legacy WEP/WPA devices, especially the APs, can hardly be upgraded to 802.11i without hardware upgrade.

The basic primitives in 802.11i include:

- *TKIP/Michael*: TKIP and Michael are retained in 802.11i for data encryption and MIC computation, respectively.
- *AES-CCMP*: AES in Counter mode with CBC-MAC Protocol (AES-CCMP) is a new protocol for data encryption and MIC computation.
- *802.1x Authentication*: 802.1x is used to authenticate the stations and distribute the keying materials.

2) AES-CCMP: AES-CCMP uses a single 128-bit AES key for both encryption and MIC computation (the stations and the AP acquire the key through 802.1x authentication [40]). AES is a block cipher that treats a message as a sequence of 128-bits blocks, as opposed to a stream cipher such as RC4.

Data encryption in AES-CCMP uses AES in Counter mode, which maintains a counter and increments it by one after one block is encrypted. For each block, the current counter is input to AES, and the output is XORed with the plaintext to generate the ciphertext. To decrypt the ciphertext, the receiver must know the initial counter value used in encryption. Therefore, ither the sender and receiver have implicit agreement on the initial counter value, or the sender should prepend its initial counter value to the ciphertext.

The MIC computation in AES-CCMP uses AES in CBC-MAC mode. The first block in the plaintext is encrypted by AES. The encryption output is XORed with the second block, then encrypted by AES again. Such iteration continues until the last block is XORed and encrypted. The final encryption output (more exactly, its first 64 bits) serves as the MIC of the message.

E. Summary

So far we have described several WLAN security solutions, namely WEP, WPA and 802.11i. They share the same goal of securing a single-hop wireless link and the same underlying approach: use cryptographic ciphers to achieve data privacy, data integrity, and access control. Their main difference is the specific ciphers and key management methods in use. By fixing the security flaws in WEP, WPA and 802.11i provide not only strong information security for individual stations, but also authentication and access control in the entire network. As a result, they can address most of the attacks listed in Section II-A, except the jamming and traffic analysis attacks, which clearly require solutions at the physical layer.

III. SECURITY OF 3G NETWORKS

In this section we examine the security aspects of 3G cellular networks. We first describe the network architecture, then discuss the security threats and their practicality. Finally we summarize the existing security mechanisms in 3G.

A. Background

1) From 2G to 3G: Public wide-area wireless networks are now migrating from the second-generation systems (2G), developed for low-bandwidth circuit-switched services, towards third-generation (3G) systems, designed to support higher data rates and packet-switched services. Several 3G systems are

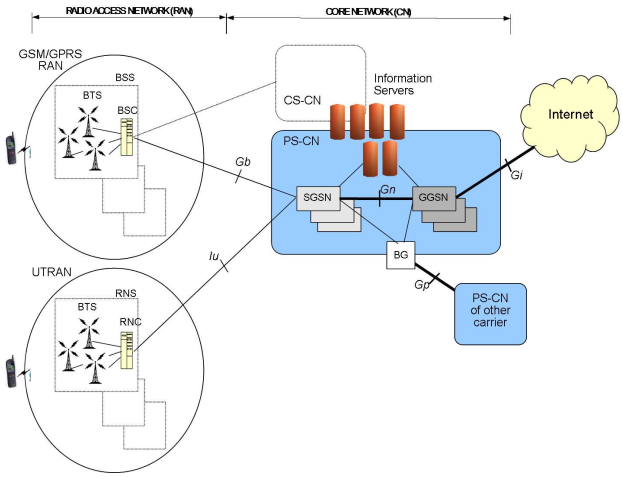

Fig. 3. 3G Network Architecture: UMTS

being developed evolving from different 2G roots and with different radio technologies. For the sake of simplicity we focus here on the the Universal Mobile Telecommunication System (UMTS), developed by 3GPP as an evolution of GSM. However, since all 3G systems share the same fundamental structure and functionalities, most of the security concepts presented here are common to other 3G platforms as well [17], [39].

During the migration path from GSM to UMTS, an intermediate phase is General Packet Radio Service (GPRS), a so-called 2.5G technology. With GPRS, the existing GSM Radio Access Network (RAN) is augmented with packet-switching capabilities for data services, and a new packet-switched core network (PS-CN) is added in parallel to the legacy circuit-switched core network (CS-CN) to carry data traffic. Besides the evolved GSM/GPRS RAN, the PS-CN will eventually connect to the new UMTS Radio Access Network (UTRAN) based on WCDMA. It is expected that for many operators GSM/GPRS and UTRAN will coexist for a long while, resulting in a mixture of 2.5G and 3G technologies with a common PS-CN.

2) UMTS Network Architecture: The network structure is depicted in Figure 3. The UTRAN is divided into *subsystems*, each consisting of one Radio Network Controller (RNC) connected to several Base Transceiver Stations (BTS). The BTSs maintain the air interface in the cells, while the RNC controls the radio connections with the Mobile Stations (MS) and the wired interface to the CN. The GSM/GPRS RAN has a similar structure.

The PS-CN embeds several elements: SGSN, GGSN, and multiple information servers. Each SGSN interconnects one or more RNC to the PS-CN, and performs functions like access control, mobility management, paging, route management [17]. The GGSN is the logical gateway between PS-CN and any external packet networks (e.g., the Internet, private intranets) and is endowed with a full IP-stack. It also handles the IP-level connectivity with the MS. The SGSN and GGSN of the same operator communicate through the Gn interface. In addition, the PS-CNs of different operators are interconnected through the Gp interface to support roaming.

The information servers play an important role in the control plane in 2.5G/3G networks. Among them, the Home Location Register (HLR) maintains all subscriber informations, including SGSN-level location tracking, while the Authentication Center (AuC) is responsible for subscriber authentication. Additionally, a number of traditional IP-based servers (e.g., DNS, DHCP, RADIUS) reside in the PS-CN for control and management purposes and interact with the SGSN/GGSN [14].

Each Mobile Station (MS) embeds two components that are physically and logically distinct: a software/hardware *terminal* (e.g. cellphone, smartphone, PDA, laptop) and a *Subscriber Identity Module* (SIM), which is a tamper-resistant smart-card storing a unique identifier and associated secret keys. The UMTS SIM (USIM) is capable of internal processing, and the cryptographic algorithms involved in authentication are executed directly on it. In fact, it is the USIM to be authenticated rather than the terminal. The USIM is issued by the network operator. Its secret keys are known to the home AuC, and a trust relationship is in place between the USIM and the AuC. This makes the administrative separation between the terminals and the network less sharp than in other networks such as public WLANs.

B. Security Threats

1) Threats to Information Security: The information security threats discussed in the WLAN context (e.g., eavesdropping, message forgery) are also applicable to 3G networks. These attacks can be attempted on either the radio link or the wired core network. Because the USIM is typically associated to a single subscriber, eavesdropping the signaling messages may reveal the subscriber's identity and location, menacing the user privacy beyond the content of the data communication.

2) Threats to Network Security: The 3G networks have a far more complex architecture than WLANs, a larger scale and heavyer signaling interactions between the MS and the network. These aspects result in additional potential threats to the network security and stability. The attacks against a 3G network can be grouped based on their source direction (see Figure 3):

1) Attacks from external wired networks, typically from the Internet (Gi interface)
2) Attacks from other interconnected CNs (Gp interface)
3) Attacks from the user plane of the RAN
4) Attacks from the signaling plane of the RAN

Attacks from the Internet (Group 1) are not unique to 3G networks, but a successful attack on an internal element of the CN might have a dramatic impact on a large portion of the network. In principle all traditional attacks against the TCP/IP stack can be attempted against the MS and/or some internal IP-based elements. Even in a simple case when the attacker injects massive unsolicited traffic towards the terminals, the damage is significant because:

- The radio capacity is scarce and shared. Massive traffic to one MS impacts the service of all other MSs in the same cell since it consumes physical and logical resources (e.g. bearer channel).

- Data traffic might induce an additional load on the signaling plane. For example, an incoming packet towards an attached yet idle MS triggers a paging procedure over a vast area that is iterated several times if the MS is not responding.
- The 3G users are typically billed per-volume, thus unsolicited traffic causes billing problems resulting in a lower level of perceived service reliability.

Attacks through the Gp interface (Group 2) can be launched via either signaling or data traffic. While the Border Gateway on Gp can firewall the traffic from foreign CNs, as noted in [43] the neighboring networks are often reciprocally semi-trusted and an attacker that has gained access to a foreign CN might from there attack the local CN.

Attacks from the user plane of the RAN (Group 3) might be critical since the terminals communicate with internal CN elements with IP-based protocol stack (e.g. GGSN, proxies). Malicious traffic like malformed packets or intrusion attempts from a terminal might aim at crashing or taking control over some internal element. From it, the intruder can attempt to gain access to even more critical elements (e.g. AAA system, OAM system). Such attacks, which ultimately exploit loopholes or other software flaws, have been demonstrated in laboratory at least for 2.5G systems [42], [43].

Another threat is the Distributed-DoS (DDoS) attacks that send massive amount of IP packets from the terminal side (e.g. TCP SYN, malformed packets), aiming at overloading the network elements or other terminals. More generally, the network stability might be threatened by macroscopic volumes of unwanted traffic even if the network elements are not directly targeted. For example, large-scale worm infections targeted to terminals might generate large volumes of unwanted traffic (e.g. TCP-SYN probes and backscatter ICMP, see [33]) that collectively build up a traffic aggregate deviating from the "typical" traffic characteristics along several dimensions - e.g. packet size, address distribution, burstiness. As a result, the network is exposed to a traffic pattern that is macroscopically different from that it was designed and optmized for, without any *a priori* guarantee that all network elements will operate correctly in such conditions. The proof-of-concept was given in 2001 by the propagation of the Code-Red-II worm, which *indirectly* caused troubles to several routers in the Internet despite the worm was not targeting network elements but just hosts (see [46], [18]). In principle, similar incidents might occurr in a 3G network as well.

Another type of potential attacks are those launched via signaling from the RAN (Group 4). A salient feature of 2.5G/3G networks is the strong signaling interaction between a large population of terminals and a reduced number of network elements (e.g., BSC, SGSN), which is required primarily for mobility and resource management. The attacker might use malformed or iterated signaling procedures to launch DoS attempts against the CN or RAN elements. In fact, several procedures require a considerable amount of resources in terms of processing power and memory states, while others use intrinsically scarce resources (e.g. limited-capacity signaling channels in the radio interface). In the worst case they might evocate flaws, software bugs or misconfigurations in the network equipments and cause additional troubles.

3) Practicality of Network Threats: So far we have presented a number of potential security threats in 3G networks. In what follows we critically examine their practicality.

In practice a single misbehaving MS cannot impose a critical load unless hitting a severe loophole or triggering a cascade of failures. This is due to the large resource asymmetry between CN elements and MSs: the former are powerful machines, typically overprovisioned to face traffic concentrations like flash crowds. Instead, the maximum traffic that that a single MS can generate is limited by one or more of the following factors:

- capacity of the signaling or data radio channel;
- processing capacity of the handset;
- processing capacity of the USIM.

The last factor for example limits the rate of signaling procedures requiring authentication (see Section III-C).

To overcome the resource limitation of individual terminals, the attacker might set up a large pool of misbehaving terminals and attempt large-scale DDoS attacks. In order to access a larger uplink bandwidth such terminals should be spread over a large geographical area and attach to multiple cells. If required, distant attacking terminals can communicate and synchronize via other networks (e.g. Internet) as the new generation of terminals tend to have multiple interfaces (e.g. a laptop with a 3G interface plus wired access). In this way distant terminals could connect to a single USIM and remotely share a single identity, e.g. to emulate frequent mobility procedures.

DDoS attacks might also be launched from a number of legitimate terminals that have been corrupted by malicious code (viruses, worms, trojans, etc.) and whose unaware owners are victim themselves. The possibility to spread malicious codes in the mobile handsets has already been reported (e.g. Cabir worm[1], Mosquito trojan[2]), which cumulates to the viruses typically spread on laptops with 2.5G/3G interfaces. However, compromising a large set of terminals through virus or worm infection is more difficult in 3G than in the Internet, due to some side factors:

- The current handset market presents a high degree of platform heterogeneity, making it harder for a malicious code to spread over a very large set of handsets.
- Subscribers are often charged per-volume, therefore will take more care of the sanity of their terminals and react upon detection of unsolicited activities.
- In some cases the terminal misbehavior will cause service degradation or unavailability and therefore trigger reaction by the user.

There is yet another difficulty in launching DoS attacks via signaling: they generally require hacking the low-layer logics of the terminal to modify the control plane modules, which are often implemented in firmware. To date there is no concrete evidence that malicious code can take control of the low-layer logics and affect the terminal's signaling behavior. At most, it might indirectly trigger a high rate of legitimate procedures (e.g. attach/detach cycles, PDP-context activation).

[1]http://viruslist.com/eng/viruslist.html?id=1689517
[2]http://viruslist.com/eng/viruslist.html?id=2019351

Other obstacles arise if the attacker seeks to put in place his own set of malicious terminals, for instance the acquisition of identities. In principle, he might try to masquerade legitimate subscribers by acquiring their identity attributes (IMSI and authentication keys), but this would be prevented by the authentication and ciphering mechanisms discussed later.

In summary, it is currently difficult and costly to instrument attacks against a 3G network due to features like resource asymmetry between terminal and CN elements, device heterogeneity, and terminal access. However, the security of 3G networks should not rely on such factors, which might eventually change in the future. For instance the recent widespread of 3G datacards for laptops launched in fall 2004 will inevitably import inside the 3G networks all kinds of malware currently present in the Internet on top of popular operating systems. In the mid-term future new software platforms might make it easier to compromise the signaling behavior of a terminal, while a higher level of device homogeneity will extend the potentials of large virus infections to handsets. In a longer term, the advancements in software defined radio [3] might make it possible to build (malicious) terminals by coupling some general-purpose transceiver and some (malicious) protocol stack publicly downloadable from the Internet. Ultimately, the cost of an attack - whether it lies in the cost of setting up a suitable attacking hardware or in the cost of acquiring knowledge about internal network features - is not an obstacle any more in front of an economic motivation for the attack itself, which is likely to grow together with the economic value of the 3G services. As a final remark, since often 3G networks coexist side-by-side with legacy 2G and 2.5G insfratructure, it should be noted that attacks to one component might cause troubles to the other as well.

C. UMTS Security Mechanisms

We highlight here the main cryptographic features in UMTS. The algorithmic details can be found in the overview in [40], [27], [17], or directly in the specifications - freely available from http://www.3gpp.org. As specified in [9] the security mechanisms for UMTS are built on top of those adopted in GSM for backward compatibility, with improvements to address known limitations and weaknesses of GSM. For instance, ciphering algorithms in 2G were not robust enough and could be cracked [15], due to key lengths too short and lazy key reuse. The cipher strength was already improved in GPRS by adopting the GEA algorithms [7], and in fact no crack is available in the public literature for it. However, these algorithms are kept secret and did not pass the open testing by the cryptanalysis community, therefore there is no evidence of their real strength - remarkably, the history of cryptanalysis is instructive about the failure of the "security-through-obscurity" model. A major improvement is introduced in 3G with the adoption of public and provably robust ciphering algorithms, with longer cipher keys (up to 128 bits) which are frequently refreshed.

The central component of the UMTS security architecture is the Authentication and Key Agreement (AKA) procedure. The AKA serves to mutually authenticate the MS (i.e., the USIM) and the network and at the same time exchange the session keys that will be used for encryption (Cipher Key) and integrity check (Integrity Key). The AKA procedure is initiated by the SGSN whenever the network needs to verify the identity of the MS, typically at each connection setup. It is based on a long-term pre-shared secret key and on a set of operator-specific cryptographic functions that are stored in the USIM and in the AuC of the subscriber's home network (i.e., the operator issuing the USIM). Besides the trust relationship between the USIM and its home AuC, a trust relationship is assumed between the AuC and the SGSN. Note that in case of roaming the AuC and SGSN belong to different operators, therefore they must have a trust agreement in place.

The AKA is a two-stage procedure. In the first stage the SGSN requests an Authentication Vector (AV) for the MS to its home AuC. The second stage consists of a one-pass *mutual* authentication between the SGSN and the USIM based on the AV. In case of successful authentication the cipher keys will be passed from the SGSN to the RNC. A detailed description of the AKA procedure and the involved cryptographic functions is reported in [40, Sec. III]

In order to protect the subscriber's identity and location privacy, a temporary identifier (Temporary Mobile Subscriber Identity, TMSI) is assigned by the SGSN to the MS. The TMSI is used for subsequent identification in place of the primary subscriber identifier (i.e., the IMSI), which makes it harder to track a specific subscriber.

In GSM all critical information (cipher keys, authentication data, signaling messages) were transported without protection in the CN on the assumption that external access to the network components is intrinsically restricted. In UMTS security mechanisms will be extended to the wired CN. In the 3GPP specifications it is foreseen from Release 4 to protect the signaling and data exchange within the wired CN by means of IPsec and MAPsec, a secure version of the SS7-based MAP protocol defined in [10]. This protects for example the exchange of the AVs between the AuC and the SGSN. From Release 6 secure communication is extended to the Iu interface between the RNC and the SGSN.

D. Summary

To date the existing cryptographic mechanisms in 3G networks are believed to adequately preserve the information security. Nevertheless, the security of the 3G network infrastructure has not yet received adequate attention. For instance, it has not yet been quantified the real exposure of 3G networks to certain types of incidents, including data-plane or signaling-plane attacks from the terminals, DDoS attacks, large-scale worm infection etc.

Additionally, in the near future the introduction of new services, new types of terminals and the further evolution of the 3G architecture (e.g. IMS and 3G/WLAN interworking [11], [8]) will likely introduce new threats for the security of 3G networks. The design of appropriate countermeasures requires a ready understanding of the threats and a concrete assessment of the risks. The prominent key factor shaping the success of these efforts will be the availability of measurements and experimental data from real operational networks. It is likely that experimental investigations are being carried on within industry laboratories (e.g. [32]), however to the best of our knowledge no results have been made public so far.

IV. Security for Mobile Ad-hoc Networks

In this section we describe the security issues in a mobile ad-hoc network. We first present the network architecture and routing protocols, then discuss their unique vulnerabilities, followed by an overview of existing solutions for control- and data-plane security in such networks.

A. Background

1) Ad-hoc Network Architecture and Routing: Mobile ad-hoc networks (MANETs) enables wireless communications among mobile nodes when a network infrastructure, such as the WLAN or 3G, is unavailable. In a MANET, any node may function as both a data source and a router that forwards packets for other nodes. Packets from a source are typically forwarded through multiple wireless hops to reach the destination. Thus an ad-hoc routing protocol is needed to build and maintain a routing table at each node.

There are mainly three families of routing protocols, namely distance vector, link state, and source routing. In distance vector routing, local neighbors exchange their distance, measured by a given routing metric (e.g., hop count), to each destination. A node selects the neighbor with the shortest distance as its next hop to forward data traffic. In link state routing, each node floods the information about its direct links to the entire network and collects updates from all other nodes to build a complete topology, it then executes a shortest-path algorithm (e.g., Dijkstra) to find a route to the destination. In source routing, each data source specifies the complete path in its data packets; more details can be found in [28].

Each routing approach may have two instantiations: proactive or on-demand. In proactive routing, each node maintains a full routing table for all destinations, and routing updates are exchanged periodically or whenever a topology change occurs. However, this may consume a large portion of limited wireless bandwidth, while only a few routes are actually used. An on-demand approach discovers a route only when needed. The route discovery is initiated by the source, typically through flooding a Route Request (RREQ). Routing states are established at intermediate nodes when RREQ is propagated. Finally the destination sends back a Route Reply (RREP) packet, and data traffic can start to flow.

The three most popular routing protocols for MANETs are DSDV [36] (proactive, distance vector), AODV [37] (on-demand, distance vector), and DSR [26] (on-demand, source routing).

2) Security Threats and Goals: Compared with WLANs, the MANETs face a new set of security threats, particularly at the network layer, due to their infrastructure-less nature. Because the core network elements, e.g., routing and forwarding engines, are provisioned by peer nodes, the attacker can readily become a router and disrupt the network operations by attacking the control or data planes. As such, the security vulnerabilities of MANETs present not only in each single-hop wireless link, but also the multi-hop forwarding mechanism that glues these links together as a network.

The threats against data security (e.g., data privacy and integrity) inherent in all wireless networks has been well studied in the WLAN context, and the countermeasures (e.g., encryption and MIC computation) discussed earlier also apply to MANETs. In what follows we focus on the unique network-layer security threats in MANETs, which can be divided into two main categories:

- *Control Plane Attacks*: an attacker can announce false routing messages to disrupt the discovery and maintenance of routes between two nodes multi-hop away from each other. The implementation is specific to the ad-hoc routing protocol in use.
- *Data Plane Attacks*: Regardless of which routing protocol is in use, an attacker can drop the data packets passing through it, replay the previously recorded packets, or inject forged packets into the network.

To protect its basic functionality of delivering packets from one node to another, the MANET needs to secure both the control-plane routing and the data-plane forwarding operations. Accordingly, a complete solution to achieve this goal has at least three pieces: control-plane security, data-plane security, and supporting components such as key management, as we will describe later in details.

B. Control Plane: Secure Ad-hoc Routing

The control-plane security design typically secure routing protocols by associating various authentication techniques with critical fields (e.g., hop count, source route) in the routing message, thus prevent even both insider and outsider nodes from disrupting the routing functionality.

1) Authentication Primitives: There are three popular message authentication primitives. The first one is *Message Authentication Codes (HMAC)*. If two nodes share a secret key, they can generate and verify a HMAC for any message using an efficient one-way hash function. However, the HMAC can be verified only by an intended receiver, thus unappealing for authenticating broadcast messages. In addition, it is non-trivial to establish network-wide pairwise keys, as $\frac{n\cdot(n-1)}{2}$ keys have to be maintained in a network with n nodes.

One-way key chain is another way to use such one-way functions to authenticate messages. By applying the one-way function $f(\cdot)$ repeatedly on an initial input x, one can obtain a chain of keys $f^i(x)$. The sender can gradually reveal the key chain in the *reverse* order, and use an unreleased key to generate HMAC for its message. This way, when the key is revealed later, the receiver can use it to verify the HMAC. With time synchronization and careful key release schedule, the one-way key chain can be used to efficiently authenticate broadcast messages [38].

The third authentication primitive is *digital signature* which is based on public-key cryptography, e.g.,RSA. Because the message is signed by the sender's secret key, it can be verified by any node given that the public keys have been distributed.

Thus digital signature scales well to large numbers of receivers, as in the broadcast cases. However, it involves heavy computation, which presents a new DoS vulnerability. The key revocation is also difficult in a self-organized MANET.

2) Distance vector routing: To secure distance vector routing protocols such as DSDV and AODV, the main challenge is to ensure that each node advertises the routing metric correctly. For example, when hop count is used as the metric, each intermediate node should increase it exactly by one when the routing updates are propagated in the network.

The hop count hash chain [20], [45] scheme can prevent an intermediate node from *decreasing* the hop count. Assuming the maximum hop count (i.e., the network diameter) is n, a node generates a hash chain of length n each time it initiates a routing update (in DSDV) or a Route Reply (RREP) message (in AODV):

$$h_0, h_1, h_2, \cdots, h_n$$

where $h_i = H(h_{i-1})$ and $H(\cdot)$ is a well-known one-way hash function. The node then adds $h_x = h_0$ and h_n into the routing message, with Hop_Count set to 0, and broadcasts it.

When an intermediate node receives such an update, it first check if

$$h_n = H^{n-Hop\_Count}(h_x)$$

where $H^m(h_0)$ denotes the result of applying $H(\cdot)$ m times on h_x. Then the node updates h_x with $H(h_x)$, increments the Hop_Count by 1, and re-broadcasts the routing update.

This way, the attacker can never decrease the hop count in an routing update, which provides authentication for the lower bound of the hop count. However, it does not prevent an attacker from advertising the *same* hop count as the one it has received. In [22], a more complicated mechanism called hash tree chain is proposed to ensure a monotonically increasing hop count as the routing update traverses the network. One general limitation of the above approaches is that they are only applicable for *discrete* routing metrics, while ineffective for continual metrics that take non-integer values.

Note that non-cryptographic techniques can also be used to secure distance vector routing protocols. For example, in the context of RIP [30], the proposed solution in [35] exploits simple geometry of triangle theorem as follows: For any set of three nodes A, B, and C, the distance between A and B should be no more than the sum of the distance between A and C, and the distance between B and C. A node can use the above fact to detect the inconsistency among the received routing updates, and further use TTL-controlled ICMP probe messages to verify the suspicious distances.

3) Link state routing: To secure link state routing protocol such as OSPF, the main challenge is to prevent the forgery of non-existent links. This is achieved in Secure Link State Routing (SLSP) [34] through digital signature based authentication. In SLSP, each node periodically broadcasts *hello* messages for local neighbor discovery, and floods *Link State Update* (LSU) packets to advertise its links. Both *hello* messages and LSU packets are signed by the node's private key. A link is accepted into the global topology if and only if it is advertised by both end-nodes through valid LSU packets. Thus the attacker cannot forge any link that involves a legitimate node.

The DoS vulnerability that exploits the high computation overhead of digital signature is addressed through rate control mechanisms. Each node measures how frequently its neighbor sends the digitally signed control packets, and discards such packets without verification if the rate exceeds a threshold.

4) Source routing: To secure source routing protocols such as DSR, the main challenge is to prevent malicious manipulation of the source routes (i.e., an ordered list of intermediate nodes) by an intermediate node, e.g., addition of new nodes, removal of existing nodes, or order switching. This is typically achieved via a per-hop authenticator associated with the route.

Ariadne [21] is a secure extension of DSR. It uses one-way HMAC chain, i.e., TESLA [38], to authenticate the source routes. It assumes time synchronization and pre-distribution of the last key in each node's TESLA key chain. Take the following example as an illustration: the source node S has a route towards the destination D through three intermediate nodes A, B, and C. When the Route Request (RREQ) packet is propagated, each intermediate node appends itself to the source route, together with a hash value for the entire packet, and a HMAC keyed by its next unreleased TESLA key. When the destination receives RREQ, it verifies whether the content matches the hash value. If so, it appends the cascaded HMACs in a Route Reply (RREP) packet, which traverses the reverse path to the source. An intermediate node delays the RREP packet until it released the previously used TESLA key, so that the next hop node can verify its TESLA HMAC.

The per-hop hash prevents a malicious node from modifying the RREP packet that it has received. Thus all it can do is to append new nodes to the route. The per-hop TESLA HMAC further prevents it from adding any nodes other than itself, because it does not know the unreleased keys of other nodes. This way, the source route discovered by Ariadne is secure.

C. Data Plane: Protect Packet Forwarding

The data-plane security should ensure that each node forwards packets according to its routing table. Unlike the control plane, the data plane cannot be proactively secured by cryptographic primitives because several attacks on forwarding cannot be prevented: an attacker may simply drop all packets passing through it, no matter how well they are protected. Thus the security solution takes a reactive approach, at the heart of which are a detection technique and a reaction scheme.

1) Detection: The open wireless medium enables localized detection in MANETs, in which each node overhears the channel and monitors the behavior of its neighbors. However, its accuracy is limited by a number of factors such as channel error, mobility, hidden terminals, etc. A malicious node may even abuse the detection mechanism and intentionally accuse legitimate ones. To address such issues, the detection results at individual nodes can be synthesized in a distributed manner to achieve consensus among a group of nodes. An alternative detection approach relies on explicit acknowledgment from the destination, and/or intermediate nodes, to the source, so that the source can figure out where the packet was dropped.

- *Localized detection*: The *watchdog* technique [31] takes the localized approach to detecting misbehaviors in the

context of DSR. It assumes symmetric links, i.e., if A can hear B, then B can also hear A. Since the entire path is specified, when node A forwards a packet to the next hop B, it knows B's next hop C. It then overhears the channel for B's transmission to C. If it does not hear the transmission after a timeout, a failure tally associated with B is increased. If the tally exceeds a threshold bandwidth, A reports B's misbehavior to the source.
This concept is extended in [44] to work with distance-vector protocols such as AODV. It adds a *next_hop* field in AODV packets so that a node can be aware of the correct next hop of its neighbors. Independent detection results are authenticated and further synthesized to reach consensus among local neighbors. It also considers more types of attacks, such as packet modification, duplication, and jamming attacks.
- *ACK-based detection*: The detection mechanism in [13] is based on explicit acknowledgments. The destination acknowledges each received packet. Based on the delivery quality, the source can initiate a fault detection process on a suspicious path. It performs a binary search between itself and the destination, and sends out data packets piggybacked with a list of intermediate nodes, also called "*probes*", which should send back acknowledgments. The source shares a key with each probe and the probe list is "onion" encrypted. Upon receiving the packet, each probe sends back an ACK, encrypted with the key shared with the source. The source in turn verifies the encrypted ACKs and attributes the fault to the node closest to the destination that sends back an ACK.

2) Reaction: Once a malicious node is detected, the network should be protected by the reaction scheme to prevent future attacks from it. The reaction scheme is typically related to the prevention component in the overall security system. For example, the malicious node may be revoked of its certificate, or have lower chance to be chosen in future forwarding paths. Based on their scope, the reaction schemes can be categorized as network-wide reaction and end-host reaction.

- *Network-wide reaction*: The network-wide reaction in [44] is based on the URSA certification framework [29]. Once multiple nodes have independently detected that one of their neighbors is malicious, they collectively revoke its current certificate. Consequently, the malicious node is isolated in the network as it cannot participate in neither routing nor packet forwarding operations any more.
- *End-host reaction*: The *pathrater* in [31] is an end-host reaction scheme that allows each node to maintain its own rating for another node. A node slowly increases the rating of well-behaving nodes over time, but dramatically decrease the rating of a malicious node that is detected by its *watchdog*. Based on the rating, the source always picks up a path with highest average rating. Clearly each node may have different opinion about whether another node is malicious, and make its independent reaction accordingly.

D. Summary

In contrast to WLAN and 3G networks, a MANET does not have a pre-deployed and trusted infrastructure. Therefore, the security solutions are mainly concerned with securing the operations of distributed network protocols, and establishing trust among peer nodes. Proactive approaches are commonly used to secure the control plane, especially the routing protocols, by authenticating the signaling messages. On the other hand, the data plane is protected through reactive approaches that detect and react to occasional intrusions. The complete security solution should encompass both aspects and manage the required keying materials in a self-organized manner.

V. Conclusion

A. Lessons Learned

To this end, we have surveyed security threats and existing security mechanisms for WLANs, 3G, and ad-hoc networks, respectively. There are several general observations that can be drawn from this study. First, the cryptographic techniques are an essential ingredient in providing information security, and can serve as the first line of defense against network attacks (e.g., through authentication). However, cryptography alone does not suffice to secure a networking system. The flawed WEP design shows that, like all other human endeavors, cryptographic designs are subject to human errors. To date, given a specific security requirement, there is neither a systematic process to develop a suitable security design nor to gauge its vulnerability.

Secondly, one major challenge in network security design is to address various dimensions of performance tradeoff including cryptographic strength, execution speed, computational overhead, communication cost, energy consumption, operational and configuration complexity, to name a few. A feasible solution must balance among these conflicting goals, yet a systematic way to evaluate these tradeoffs is still missing. Unfortunately, many state-of-the-art solutions still do not possess the properties that networking protocols deem necessary. For example, most of them cannot scale well as the network size grows, and rely on centralized components to bootstrap or operate the security protocols. As a result, they may work well in a small-scale setting but cannot function effectively or efficiently in large-scale networks, such as the emerging sensor networks or metropolitan/community mesh networks.

Finally, the current security solutions are typically based on specific threat models, and operate explicitly or implicitly with a number of assumptions made on the networks. For example, the 3G network security designs assume that the core network is reliable and resource-rich. When unexpected behaviors or unanticipated traffic patterns occur, the current mechanisms might be not sufficient to ensure the required network security.

B. Future Research

Looking ahead into the future, we would like to identify two directions that need more research and development efforts to build a truly secure wireless networking system:

- *Critical evaluation*: While many security solutions have been reported in the literature, most of them have not been thoroughly evaluated in terms of security strength and system performance. In fact, we lack systematic evaluation methods and efforts in the following aspects: *(1) Vulnerability analysis of the current solutions/standards*. While the cryptographic strength of individual ciphering algorithms is relatively well understood, we have no formal analytical tools to assess a system security proposal. In particular, the analysis on the inter-dependency among various system components and security operations poses a major research challenge. *(2) Measurements and emulations*. To date most solutions have been evaluated for their network and system performance via simulations. However testbed measurements and large-scale emulations based on measurement traces are critically needed for a deeper understanding.
- *Resilient security*: Most current solutions make idealistic assumptions on the network and individual components. A truly resilient security solution needs to possess both robustness and resiliency. It must be robust against wireless channel errors, transient/permanent network connectivity and topology changes, user mobility, changes in user and traffic behavior. It must also be resilient against unanticipated attacks, operational errors such as misconfigurations, and compromised/stolen devices. In addition, both dimensions of goals have to be achieved with acceptable cost.

The history of security has taught us that a perfectly secure system does not exist. Instead, security is an evolving process, as we have seen in the context of WLANs and 2G/3G networks. New system vulnerabilities continue to be identified, and new security threats continue to arise. Accordingly new solutions must be developed and integrated into existing systems. We need continued development of newer and stronger ciphers, but more fundamentally we also need a better understanding of how to architect a secure system that can embrace the security evolution in a flexible, non-intrusive, and efficient manner.

REFERENCES

[1] Aerosol. *http://www.stolenshoes.net/sniph/aerosol.html*.

[2] AirSnort. *http://airsnort.shmoo.com/*.

[3] GNU Software Radio. *http://www.gnu.org/software/gnuradio*.

[4] WEPCrack. *http://sourceforge.net/projects/wepcrack*.

[5] Wi-Fi Alliance. *http://www.wi-fi.org/*.

[6] Wi-Fi Protected Access (WPA). *http://www.wi-fi.org/wpa/*.

[7] 3GPP. TS 01.61. GPRS Ciphering Algorithm Requirements.

[8] 3GPP. TS 23.234. 3G Security. 3GPP Systems to WLAN Interworking: System Description.

[9] 3GPP. TS 33.120. 3G Security. Security Principles and Objectives.

[10] 3GPP. TS 33.200. 3G Security. MAP Application Layer Security.

[11] K. Ahmavaara, H. Haverinen, and R. Pichna. Interworking Architecture Between 3GPP and WLAN Systems. *IEEE Communications*, 14(11), Nov. 2003.

[12] W. Arbaugh, N. Shankar, Y. Wan, and K. Zhang. Your 802.11 Wireless Network Has No Clothes. *IEEE Wireless Communications*, 9(6), Dec. 2002.

[13] B. Awerbuch, D. Holmer, C. Nita-Rotaru, and H. Rubens. An On-Demand Secure Routing Protocol Resilent to Byzantine Failures. In *Proc. WiSe*, 2002.

[14] J. Bannister, P. Mather, and S. Coope. *Convergence Technologies for 3G Networks: IP, UMTS, EGPRS and ATM*. Wiley, 2004.

[15] E. Barkan, E. Biham, and N. Keller. Instant Ciphertext-Only Cryptanalysis of GSM Encrypted Communications. In *Proc. Crypto*, 2003.

[16] N. Borisov, I. Goldberg, and D. Wagner. Intercepting Mobile Communications: The Insecurity of 802.11. In *Proc. MOBICOM*, 2001.

[17] J.-C. Chen and T. Zhang. *IP-Based Next-Generation Wireless Networks*. Wiley, 2004.

[18] Cisco. Dealing with mallocfail and High CPU Utilization Resulting From the "Code Red" Worm. *http://www.cisco.com/warp/public/63/ts_codred_worm.pdf*, 2001.

[19] S. Fluhrer, I. Mantin, and A. Shamir. Weaknesses in the Key Scheduling Algorithm of FCC4. In *Proc. Eighth Annual Workshop on Selected Areas in Cryptography*, 2001.

[20] Y. Hu, D. Johnson, and A. Perrig. SEAD: Secure Efficient Distance Vector Routing for Mobile Wireless Ad Hoc Networks. In *Proc. IEEE Workshop on Mobile Computing Systems and Applications (WMCSA)*, 2002.

[21] Y. Hu, A. Perrig, and D. Johnson. Ariadne: A Secure On-demand Routing Protocol for Ad Hoc Networks. In *Proc. MOBICOM*, 2002.

[22] Y. Hu, A. Perrig, and D. Johnson. Packet Leashes: A Defense against Wormhole Attacks in Wireless Networks. In *Proc. INFOCOM*, 2003.

[23] IEEE Computer Society. Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications. IEEE standard 802.11, 1999.

[24] IEEE Computer Society. Wireless Medium Access Control (MAC) and Physical Layer (PHY) Specifications: Specifications for Enhanced Security. IEEE standard 802.11i, June 2004.

[25] Jessie Walker. 802.11 Security Series. Part II: The Temporal Key Integrity Protocol (TKIP). Intel Technical Report, 2004.

[26] D. Johnson, D. Maltz, and J. Jetcheva. *DSR: The Dynamic Source Routing Protocol for Multi-Hop Wireless Ad Hoc Network*, chapter 5. Ad Hoc Networking. Addison-Wesley, 2001.

[27] G. Koien. An Introduction ro Access Security in UMTS. *IEEE Wireless Communications*, 11(1), February 2004.

[28] J. Kurose and K. Ross. *Computer Networking: A Top-Down Approach Featuring the Internet*. Addison-Wesley, 2002.

[29] H. Luo, J. Kong, P. Zerfos, S. Lu, and L. Zhang. URSA: Ubiquitous and Robust Access Control for Mobile Ad-Hoc Networks. *IEEE/ACM Transactions on Networking (to appear)*, 2004.

[30] G. Malkin. Routing Information Procotol Version 2. RFC 2543, 1998.

[31] S. Marti, T. Giuli, K. Lai, and M. Baker. Mitigating Routing Misbehavior in Mobile Ad Hoc Networks. In *Proc. Mobicom*, 2000.

[32] METAWIN project. *http://www.ftw.at/projects*.

[33] R. Pang, V. Yegneswaran, P. Barford, V. Paxson, and L. Peterson. Characteristics of Internet Background Radiation. In *Proc. IMC*, 2004.

[34] P. Papadimitratos and Z. Haas. Secure Link State Routing for Mobile Ad Hoc Networks. In *IEEE Workshop on Security and Assurance in Ad Hoc Networks*, 2003.

[35] D. Pei, D. Massey, and L. Zhang. Detection of Invalid Routing Announcements in RIP Protocol. In *Proc. IEEE Globecom*, 2003.

[36] C. Perkins and P. Bhagwat. Highly Dynamic Destination-Sequenced Distance-Vector Routing (DSDV) for Mobile Computers. In *Proc. SIGCOMM*, 1994.

[37] C. Perkins and E. Royer. Ad Hoc On-demand Distance Vector Routing. In *Proc. WMCSA*, 1999.

[38] A. Perrig, R. Canetti, D. Tygar, and D. Song. The TESLA Broadcast Authentication Protocol. *RSA CryptoBytes*, 5(2):2–13, 2002.

[39] G. Rose and G. Koien. Access Security in CDMA2000, including a Comparison with UMTS Access Security. *IEEE Wireless Communications*, 11(1), February 2004.

[40] M. Shin, J. Ma, A. Mishra, and W. Arbaugh. Wireless Network Security and Interworking. *Proc. IEEE, Special Issue on Cryptography and Security Issues*, Fall 2005.

[41] A. Stubblefield, J. Ioannidis, and A. Rubin. Using the Fluhrer, Mantin, and Shamir Attack to Break WEP. In *Proc. Network and Distributed System Security Symposium (NDSS)*, 2002.

[42] O. Whitehouse. GPRS Wireless Security: Not Ready For Prime Time. *Report by Atstake Inc. http://www.atstake.com/research/reports*, June 2002.

[43] O. Whitehouse and G. Murphy. Attacks and Counter Measures in 2.5G and 3G Cellular IP Networks . *Report by Atstake Inc. http://www.atstake.com/research/reports*, March 2004.

[44] H. Yang, X. Meng, and S. Lu. Self-Organized Network Layer Security in Mobile Ad Hoc Networks. In *Proc. WiSe*, 2002.

[45] M. Zapata and N. Asokan. Securing Ad Hoc Routing Protocols. In *Proc. WiSe*, 2002.

[46] C. Zou, W. Gong, and D. Towsley. Code Red Worm Propagation Modeling and Analysis. In *Proc. CCS*, 2002.