Wireless Security Perspectives

Cellular Networking Perspectives

Editors: Les Owens, David Crowe. Email: Les.Owens@cnp-wireless.com Vol. 4, No. 10. November, 2002

In the News

Cyberdefense

A cooperative research and development project between the U.S. Department of Defense (DoD) and Lancope will integrate the Atlanta-based company's StealthWatch™ intrusion detection system (IDS) with NSA and DoD technology to develop an appliance to be known as "Therminator." Using advanced mathematics, researchers aim to convert the character of network traffic into imagery. System users (analysts) would "see" their network's cyber traffic, and the DoD intends to use information from this system for early detection of new (never seen before) cyber attacks. Therminator will be offered to both the public and private sectors.

In the event of an attack, Therminator would create an audit trail of network activity to help trace compromised servers and to help identify the source of the attack. In theory, new attacks would exhibit new signatures (patterns of imagery constructed from the advanced mathematics – reacting to actually data flow).

Read more about Therminator at the **Lancope** website.

Evolution of WiFi Security

Upcoming wireless local area network (WLAN) security improvements could give home and small-office WiFi users many of the security advantages enjoyed by large enterprises equipped with authentication servers or network infrastructure. In the next few months, watch for WiFi Protected Access (WPA), an evolutionary change in WiFi security. WPA is being promoted by the Wi-Fi Alliance as an interim standard. Two modes will be offered: A full-scale "WPA in Enterprise Mode" and a lesser version, "WPA in Home Mode". Industry experts are giving WPA only a luke-warm thumbs up – it is a band-aid attempt at fixing the gravely flawed Wired Equivalent Privacy (WEP).

For even greater security, within 14-18 months, the RSN (Robust Security Networks) will be available for the user. RSN is seen as a more robust, long-term solution for WiFi security.

Without question, WEP (Wired Equivalent Privacy) is troubled. Its faults may not bother WiFi network experimenters, but who would risk "high security" aspects of their organization to its vulnerabilities? Employees often simply side-step encryption, introducing major security holes (i.e., if they feel it is too much trouble). Systems using WEP are typically shipped without encryption enabled, and no one would dispute the encryption's inherent weaknesses.

About Wireless Security Perspectives

Price

The basic subscription price for *Wireless Security Perspectives* is $300 for one year (12 issues) for delivery by emailed PDF file or by first class mail within the US or Canada. International subscriptions are US$350 per year. The basic subscription allows for distribution to up to 10 people within one organization. Contact us for license fees to allow more readers.

We provide discounts to educational institutions and small businesses (less than 10 employees).

Back issues are available individually, or in bulk at reduced prices.

Delivery is by first class mail or by email (Acrobat PDF file).

Complete pricing information for both publications is available at:

www.cnp-wireless.com/prices.html

To obtain a subscription, please contact us at:

cnpaccts@cnp-wireless.com

Next Issue Due…

December 18th, 2002.

Future Topics

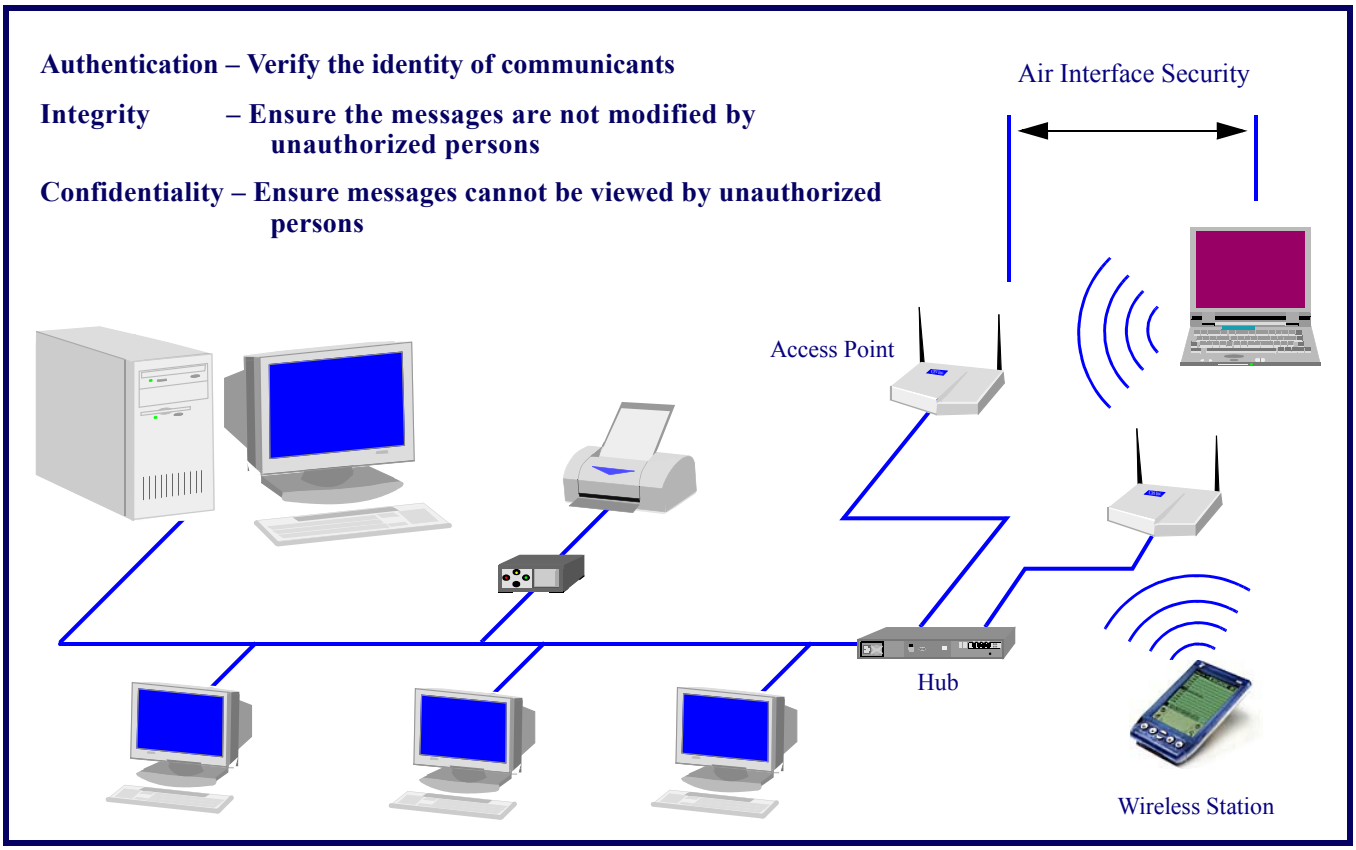
802.11 Wireless LAN "Hotspot" Roaming Security • Wireless VPNs • 3G Security • Public Keys & Wireless • Wireless Flash Memory Security • Radius for Wireless • Security Issues in Ad hoc Wireless Networks • Latest in Watermarking

Wireless Security Perspectives (ISSN 1492-806X (print) and 1492-8078 (email)) is published monthly by Cellular Networking Perspectives Ltd., 2636 Toronto Cresc. NW, Calgary, Alberta T2N 3W1, Canada. **Phone**: 1-800-633-5514 (+1-403-274-4749) **Fax**: +1-403-289-6658 **Email**: cnpsales@cnp-wireless.com **Web**: www.cnp-wireless.com/wsp.html **Subscriptions**: $300 for delivery in the USA or Canada, US$350 elsewhere. **Payment**: accepted by cheque, bank transfer, American Express, Diners Club, MasterCard or Visa. **Delivery**: Email or 1st class mail. **Back Issues**: Available individually for $35 in the US and Canada and US$40 elsewhere, or in bulk at reduced rates. **Discounts**: Educational and small business discount: 25% off any order. **Copies**: Each subscriber is licensed to make up to 10 copies of each issue or back issue. Call for rates to allow more copies.

Technical Editor and Illustrator: Les Owens.

Article Sourcing: Tim Kridel.
Production: Doug Scofield.
Distribution: Debbie Brandelli.
Accounts: Evelyn Goreham.
Publisher: David Crowe.

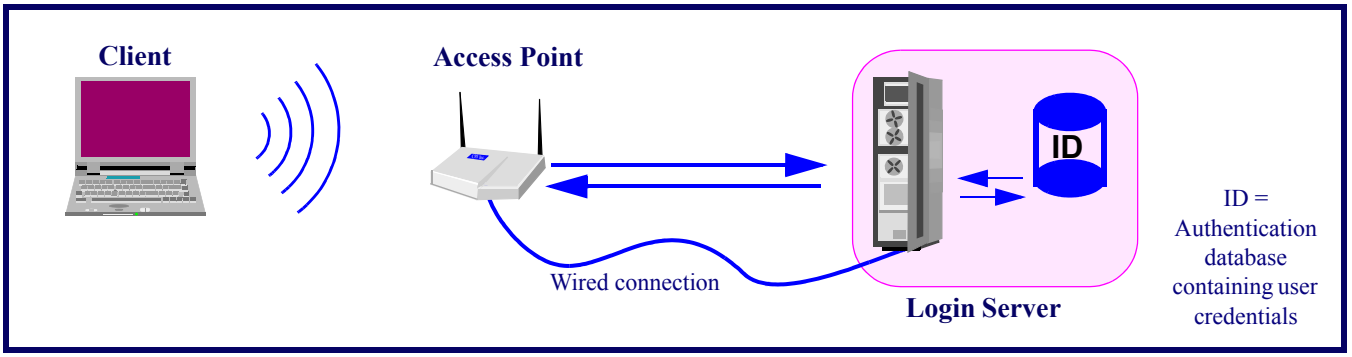
Figure 1: Typical WiFi Network – Three Important Security Requirements: Authentication, Integrity and Confidentiality



WiFi Protected Access (WPA)

WPA is a suite of interim solutions to address WEP problems with existing hardware. By incorporating the IEEE 802.1X port-based access control protocol – including Extensible Authentication Protocol (EAP) – into 802.11, WPA includes a more secure framework for authentication and encryption key distribution. Furthermore, it is designed with an automatic reset feature in response to Denial of Service attacks. With these features, WPA provides a more robust security solution than WEP, yet it requires basically the same hardware – operating within the typical WiFi configuration (as shown in **Figure 1**).

Figure 2: WPA Authentication in Enterprise Mode: (802.1X) Port-based Access Control



Authentication and Encryption Key Distribution

Port-based access control means WPA eliminates the shared and static key weaknesses of WEP. WiFi user communication is limited to an access point (AP) until all authentication and key distribution is completed. The AP delivers authentication data – a user-name and password keyed in by the user or, alternatively, biometric data or data from a smart card – from the user (client) to a special login server (RADIUS, for example), as shown in **Figure 2.** Both the host and the client are

authenticated under EAP. Failed authentication disallows encryption key distribution and network access – a definite improvement over WEP.

For the Enterprise Mode, authentication data is centrally stored at the login server. Those using this mode may find this aspect to be a down-side of WPA. It could become an IT management headache when many users, each with a unique login, must have their credentials stored in the login server.

The Home Mode version will not include all of the 802.1X Authentication features shown in Figure 2. Instead, no login server is needed – the access point completes authentication. The same password is used for all devices, and this password initiates encryption.

In either mode, the valid password initiates generation of the EAP master key for the Temporal Key Integrity Protocol (TKIP), which is then used to generate "base keys," which in turn is used for generating the per packet key. Thus, WPA offers more robust security on the radio link. The frequent key changing aspect of 802.1X, based upon TKIP, reduces the risk of cryptographic key theft. With TKIP, every 10 Kbytes of data transmitted over the network is encrypted using a new key.

TKIP enhances the WEP cipher engine, as illustrated in **Figure 3,** with four new algorithms:

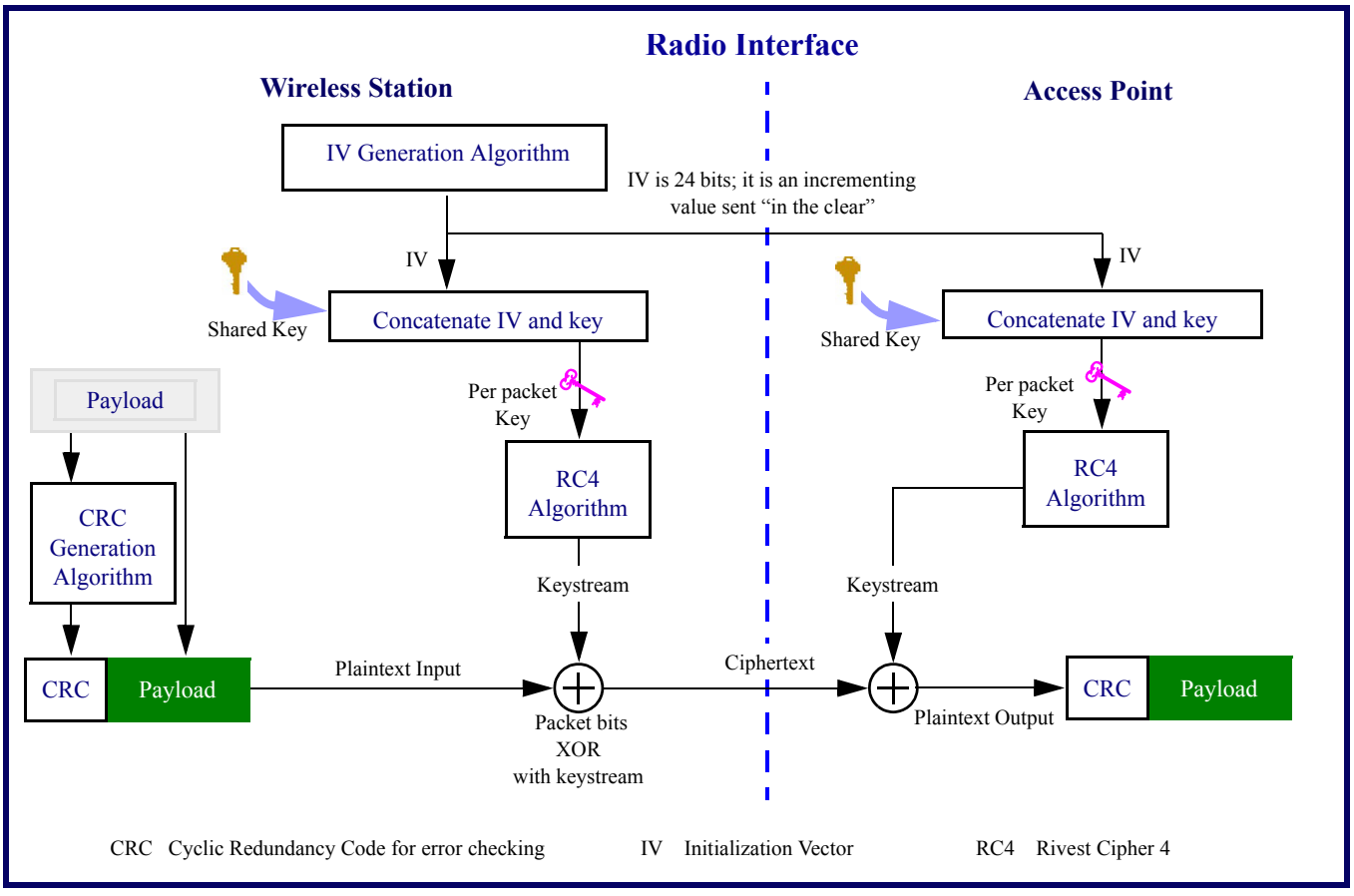
1. The Initialization Vector (IV) – an incrementing number – is extended to 48 bits, and the sequencing rules are enhanced. The IV is reset to zero (0) each time a new base key is generated, which occurs at the beginning of each new session (or every 10 Kbytes of data).
2. Generation of per-packet keys, including a mixing function.
3. The "Michael" algorithm generates a Message Integrity Code (MIC) to accompany each packet (MIC is like a "keyed CRC"), and MIC is employed on the message data to generate the Integrity Check Value (ICV), which also accompanies each packet.
4. Every new session (every 10 Kbytes of transmitted data) includes a nonce to guarantee liveliness.

System Reset

The WPA reset feature is best described using a scenario. Assume an attacker sends two packets of unauthorized data, or "failed forgeries" within one second. Attacked in this manner, WPA initiates a session shut-down, and then connectivity is renewed with a new session using different keys.

The scenario begs a question, however: Did the attacker effectively achieve the intended result? The answer depends upon the attacker's purpose and tenacity. The truth is, WPA is vulnerable to all commonly known Denial of Service (DoS) attacks, plus one more – that one described above ("failed forgeries").

Figure 3: Wired Equivalent Privacy (WEP) – Good bye in RSN!



DoS attacks cause disruptions. Although one successful attack may be insignificant, a series of them could amount to a significant delay . . . it could even shut down the network. During the attack, the WPA design secures data from being stolen, but the reset delay could represent a significant reduction in productivity or to delivery of customer service or to some other time-dependant interaction, and of course, the more tenacious attacker, imposing greater duration and frequency of attack, would cause greater impact.

Still, despite its woes, WPA is better than WEP, and its status as a bridge into RSN provides sufficient hope that someday, WiFi might qualify as more than just a fun experiment. It may even become a useful component in "high security" environments.

Robust Security Network (RSN)

RSN is the full, long-term solution developed by the IEEE 802.11 Task Group. RSN is really an enhanced version of WPA. The most important difference is its use of AES (Advanced Encryption Standard), which will be used both for encrypting data traffic and for robust integrity checking. However, because block cipher AES is being used to fix the problems with WEP, and because the implementation changes are dramatic – the silicon-based designs will change – new hardware will almost certainly be required in network interface cards (NICs) for the PC and for access points (AP).

Our **February 2002** issue of *Wireless Security Perspectives* provides a summary of AES, while full details are available within the AES specification, **FIPS197**.

A future issue of *Wireless Security Perspectives* will cover RSN in detail.

Conclusion

WPA will be simply a software fix, but RSN will include both software and hardware upgrades to WiFi-Certified products in use today. WPA upgrades are expected to become available early in 2003, and RSN upgrades could occur as early as 4th quarter, 2003. No downward compatibility to WEP will be possible after an upgrade. Formal WPA certification will be voluntary at first, but mandatory certification will follow. The Wi-Fi Alliance hopes this will force rapid acceptance of WPA, and ultimately RSN, leaving WEP to flounder among the reclusive dinosaurs until it finally rests itself

calmly
on the pages
of history books (RIP).

Sources:

[1]. *Wi-Fi Protected Access*. Media Briefing. Wave Communications for the Wi-Fi Alliance.

[2]. Grimm, C. Brian. *Wi-Fi Alliance Announces Standards-Based Security Solution to Replace WEP,* and related articles under "Background Information." Wi-Fi Press Release. October 31, 2002.
www.wi-fi.com/OpenSection/ReleaseDisplay.asp?TID=4&ItemID=118&StrYear=2002&strmonth=10

Upcoming Wireless Security and Fraud Conferences & Events

The following are upcoming wireless and wireless security conferences and events that may be of interest to our wireless security and network security practitioners.

ACM Multimedia 2002
1st - 6th December 2002
Hotel Ambassadeur
Juan Les Pins, France
mm02.eurecom.fr/technicalprogram.html

Interconnect, Payments and Settlements
2nd - 5th December 2002
Hotel Sants
Barcelona, Spain
www.iir-conferences.com

1st Workshop on Security in Ad Hoc Networks
2nd December 2002
Ruhr University
Bochum, Germany
www.crypto.ruhr-uni-bochum.de/adhocsec

SANS Maryland
2nd- 7th December 2002
Sheraton Columbia Hotel
Columbia, MD
www.sans.org/Maryland

802.11 Planet Conference & Exposition Fall 2002
3rd- 5th December 2002
Santa Clara Convention Center
Santa Clara, CA
www.jupiterevents.com/80211/fall02/index.html

2.5G & 3G Wireless Seminar
9th- 10th December 2002
Phoenix, AZ
www.alexanderresources.com/3G/index.html

Annual Computer Security Applications Conference
9th- 13th December 2002
Alexis Park Resort & Spa
Las Vegas, NV
www.acsac.org

Combating Fraud for Banks and Financial Institutions
11th- 12th December 2002
The Pan Pacific, Singapore
Singapore
www.iqpc.com

2nd Annual Biometrics for Business: Developing Deployment Measures
12th- 13th December 2002
Metropolitan Hotel
New York, NY
www.srinstitute.com/part_iter_site_page.cfm?iteration_id=463

The Conference on Mobile & Wireless Security
11th- 13th February 2003
Marriott Mountain Shadows Resort
Scottsdale, AZ
www.misti.com

[3] Batista, Elisa. *WiFi Encryption Fix Not Perfect*. Wired News. November 15, 2002.

www.wired.com/news/business/0,1367,56350,00.html

[4]. Wildstrom, Stephen H. *Road to Wi-Fi: No more whining about WEP.* ZDNet Tech Update, Security. November 15, 2002.

techupdate.zdnet.com/techupdate/stories/main/0,14179,2897654,00.html

Computer Security: Special Publication 800 Series

Special Publications in the 800 series present documents of general interest to the computer security community. The series was established in 1990 to provide a separate identity for information technology security publications. Reports include generally accepted best practices, guides, comparisons, and outreach efforts in computer security, which are the result of collaborative activities between industry, government, and academic organizations.

Publication 800-48, which is now a finalized document, is an example. It includes technology overviews of 802.11 WLAN, Bluetooth ad hoc networks, and hand-held devices (PDA, for instance). In great detail, it examines the security features – both benefits and risks – of these wireless networks, and it provides practical guidelines and recommendations, in tutorial format, for mitigating these risks.

Fraud and Security Patent News

The US Patent and Trademark Office (USPTO) recently granted the following fraud and security patents. These will be of interest to some of our wireless security practitioners. Each patent includes the patent number, the invention title – linked to the corresponding USPTO webpage – a brief description, the inventor(s), and the assignee (owner). These patents were granted in October and November of 2002.

With the listing below, one can see *who* is doing *what* in the world of inventions. Moreover, it is often instructive to read issued patents, since they include patent claims, specifications, illustrations, detailed descriptions and cited references. Patents often include other references, and these are sometimes useful to broaden one's perspective of wireless communications and security.

If the wording in these is difficult to understand, recognize that the patent abstracts are generally provided in their raw legal-jargon form, straight from an attorney's word-processor. Sometimes we edit the abstracts for readability when the legalese is too impenetrable.

US Patent: 6,480,957

Method and system for secure light-weight transactions in wireless data networks

The present invention is a method and system for establishing an authenticated and secure communication session for transactions between a server and a client in a wireless data network that generally comprises an airnet, a landline network and a link server between them. The client, having limited computing resources, is remotely located with respect to the server and communicates to the server through the wireless data network. To authenticate each other, the client and the server conduct two rounds of authentication – the client authentication and the server authentication – independently and respectively. Each of the authentication processes is based on a shared secret encrypt key and a challenge/response mechanism. To reach for a mutually accepted cipher in the subsequent transactions, the server looks up for a commonly used cipher, and it forwards the cipher along with a session key to the client. The subsequent transactions between the client and the server can then proceed in the authenticated and secure communication session, and further, each transaction secured by the session key is labeled by a transaction ID that is examined before a transaction thereof takes place.

Issued: November 12, 2002

Inventor: Hanqing Liao, *et al*

Assignee: Openwave Systems Inc. (Redwood City, CA)

Interesting Reference:

[1] Needham, *et al*. *Using Encryption for Authentication in Large Networks of Computers.* Communications of the ACM, vol. 21, No. 12, Dec. 1978.

US Patent: 6,480,935

Smart card memory management system and method

A system and method for memory management in a smart card. The memory manager, preferably part of a true operating system, is the single device by which memory in the smart card is allocated and deallocated. Memory allocation for new data objects and memory deallocation as the result of data object deletion are made by reference to a memory management record, preferably a bitmap, which is stored in RAM and formed upon smart card initialization.

Issued: November 12, 2002

Inventor: Carper, *et al*

Assignee: Same**.**

Interesting References:

[1] Rankl, *et al*. *Smart Card Handbook*. (John Wiley & Sons, 1998) pp. 14,91,103,107-110, 127-128.

[2] Guthery, *et al*. *Smart Card Developer's Kit.* (Indianapolis: Macmillian Technical Publishing, 1998) pp. 175-176, 219-220.

US Patent: 6,480,724

Modular mobile communication system

A modular system for personal data acquisition and communication is expanded advantageously to a cellular telephone system, the functions of which can be increased by means of various expansion cards. A host device in the system according to the invention, such as a mobile communication device, need not be equipped with all possible functions in the manufacturing stage, but some of the functions can be realized on expansion cards, and the user can add a desired function to the host device according to need. The expansion cards are small, and they are installed substantially inside the host device, such as a mobile communication device, so that the entity formed by the host device and the expansion card seems to the user as a single compact device. Advantageously, the expansion cards include, in addition to the hardware needed, also the software required for controlling the operation of the modules.

Issued: November 12, 2002

Inventor: Marko Erkkila

Assignee: Nokia Mobile Phones Ltd. (Espoo)

US Patent: 6,480,710

System and method for managing prepaid wireless service

A method facilitates provisioning of pre-paid wireless services. Credit refresh operations involving a pre-paid wireless communication device involve SMS messages transmitted to the device over-the-air. The device uses tariff tables to keep track of a calls impact on available credit. The tariff tables are updatable at the service provider's discretion using SMS messages.

Issued: November 12, 2002

Inventor: Bernard Laybourn

Assignee: Telemac Corporation (Los Angeles, CA)

Interesting Reference:

[1] Lee, William. Mobile Cellular Telecommunications Systems, 1989 pp. 68-70.

US Patent: 6,480,497

Method and apparatus for maximizing data throughput in a packet radio mesh network

In a mesh network communication system, net throughput is optimized on the link between the communicating nodes by dynamically modifying signal characteristics of the signals transmitted between nodes in response to performance metrics which have been determined from analysis at the receivers for the corresponding links. The signal characteristics can be the data rate, modulation type, on-air bandwidth, etc. The performance metrics are calculated based on data-link on-air characteristics of received signals.

Issued: November 12, 2002

Inventor: George Flammer III, *et al*

Assignee: Ricochet Networks, Inc. (Denver, CO)

Interesting Reference:

[1] Ue, *et al*. *Symbol Rate and Modulation Level Controlled Adaptive Modulation/TDMA/TDD for Personal Communications Systems.* IEEE VTE, pp. 306-310, July, 1995 (0-7803-3742-X/95).

US Patent: 6,480,477

Method and apparatus for a data transmission rate of multiples of 100mbps in a terminal for a wireless metropolitan area network

A method and apparatus for a data transmission rate of multiples of 100 mega-bits per second (Mbps) in a terminal for a wireless metropolitan area network. A terminal includes a first media access control unit (MAC unit) for receiving Fast Ethernet data packets at a rate of 100 Mbps for communication over a wireless link, *n*-1 additional MAC units for receiving Fast Ethernet data packets at a rate of 100 Mbps for communication over the wireless link, a multiplexer having *n* inputs, wherein each input is coupled to receive the data packets from a corresponding one of the MAC units and wherein the output of the multiplexer provides time-division multiplexed data, a packet formatting apparatus coupled to the output of the multiplexer for formatting the time division multiplexed data according to radio frames, and a wireless transceiver coupled to the packet formatting apparatus for communicating the radio frames over a wireless link, wherein the wireless link has a maximum bandwidth capacity of at least *n* times 100 Mbps. Each MAC unit can include a rate control unit and a rate buffer for temporarily storing data packets received by the corresponding MAC unit prior to providing them to a corresponding one of the inputs of the multiplexer. Each MAC unit can include a corresponding layer-two or layer-three switch, having a 100 Mbps port. The maximum transmission rate is limited only by the bandwidth of the wireless link.

Issued: November 12, 2002

Inventor: Kirk Treadaway, *et al*

Assignee: Innowave ECI Wireless Systems Ltd. (Petach-Tikva, IL)

Interesting References:

[1] McMillen, G., B. Mazur and T. Abdel-Nabi. *Design of A Selective FEC Subsystem to Counteract Rain Fading in Ku-Band TDMA Systems.* International Journal of Satellite Communications, vol. 4, pp. 75-82, 1986.

[2] Barton, S. and S. Dinwiddy. *A Technique for Estimating the Throughput of Adaptive TDMA Fade Countermeasure Systems.* International Journal of Satellite Communications, vol. 6, pp. 331-341, 1988.

US Patent: 6,480,108

Method and apparatus for tracking and locating a moveable article

Tracking of an article through geographic areas using electromagnetic signals, specifically radio frequency (RF) signals. The article contains a tag operating as a transmitter and receiver. Tag-readers in the defined geographic areas transmit RF signals, and in response, the tag transmits RF signals received by the tag-reader. By knowing the areas in which the tag-readers are located, a system tracks the article by monitoring the tag-readers communicating with the tag.

Issued: November 12, 2002

Inventor: Glenn McDonald

Assignee: The United States of America, as represented by the United States Postal Service (Washington, DC)

US Patent: 6,470,447

Enabling conformance to legislative requirements for mobile devices

Provided are a method and a mechanism for dynamically controlling the performance of communication-related operations of a mobile device in accordance with legislative requirements of the particular location of the mobile device and the location of the computing device with which it is to communicate, and also in accordance with communication requirements of application programs at either end of the communication link. A first use of the invention is for ensuring conformance of a mobile device's communications to the cryptographic requirements of different countries, even when the device crosses a country boundary during communication.

Issued: October 22, 2002

Inventor: Howard Lambert, *et al*

Assignee: International Business Machines Corporation (Armonk, NY)

Further Patent Information

.To obtain a complete copy of these patents, contact the US Patent and Trademark Office at the address or telephone numbers below:

General Information Services Division
U.S. Patent and Trademark Office
Crystal Plaza 3, Room 2C02
Washington, DC 20231

800-786-9199 or 703-308-4357

US Patent: 6,470,329

One-way hash functions for distributed data synchronization

A method for synchronizing two data sets which includes computing a signature for a first data set in a first address space and a signature for a second data set in a second address space using a one-way hash function and comparing the signatures for the first and second data sets to determine whether they are identical. If the signatures are not identical, the method further includes identifying an area of difference between the first data set and the second data set and transferring data corresponding to the area of difference between the first data set and the second data set from the first data set to the second data set.

Issued: October 22, 2002

Inventor: Victoria Livschitz

Assignee: Sun Microsystems, Inc. (Palo Alto, CA)

US Patent: 6,467,685

Countable electronic monetary system and method

An electronic value transfer system using stored value in the form of serialized electronic coins and electronic bills, which provides efficient security monitoring without the need for full centralized accounting of each transaction. Central monitoring of the system-level security includes statistical sampling techniques coupled with efficient tracing of the transaction path of an electronic coin back to its source. Only small amounts of data storage and transmission are utilized, eliminating the need for large centralized databases of transaction records. Consumer privacy, as well as flexibility in making card-to-card monetary transfers, are thereby enhanced, while allowing verification of system-wide security as well as rapid detection and tracing of security breaches. Multiple editions of electronic coins permit transparent and periodic renewal of the system and re-establishment of a security baseline, and they also provide for the regular reclamation of stored value lost or abandoned by consumers.

Issued: October 22, 2002

Inventor: Mordechai Teicher

Assignee: Cardis Enterprise International N.V. (Curacao, NL)