International Journal of Future Generation Communication and Networking
Vol.7, No.4 (2014), pp.25-34
http://dx.doi.org/10.14257/ijfgcn.2014.7.4.03

A Literature Review of Security Threats to Wireless Networks

Umesh Kumar [1] and Sapna Gambhir [2]

YMCA University of Science and Technology, India
umesh554@gmail.com,sapnagambhir@gmail.com

Abstract

In the recent years we have huge development of wireless technology. We are presently getting more subject to wireless technology. As we know wireless networks have broadcast nature so there are different security issues in the wireless communication. The security conventions intended for the wired systems can't be extrapolated to wireless systems. Hackers and intruders can make utilization of the loopholes of the wireless communication. In this paper we will mull over the different remote security dangers to wireless systems and conventions at present accessible like Wired Equivalent Privacy (WEP), Wi-Fi Protected Access (WPA) and Wi-Fi Protected Access 2 (WPA2). WPA2 is more hearty security convention as compared with WPA on the grounds that it utilizes the Advanced Encryption Standard (AES) encryption. There are few issues in WPA2 like it is helpless against brute force attack and MIC bits could be utilized by programmer to compare it with the decoded content. So in this paper we will concentrate on different sorts of wireless security dangers.

Keywords: *Wired Equivalent Privacy, Wi-Fi Protected Access, Wi-Fi Protected Access2, Temporal Key Integrity Protocol, and Advance Encryption Standard*

1. Introduction

Wireless communication is the exchange of data between two or more points that are not joined by an electrical transmitter. The most well-known wireless technologies use electromagnetic wireless telecommunications, for example, radio. With radio waves distances could be short, for example, a couple of meters for TV remote control, or the extent that thousands or even a huge number of kilometers for profound space radio communications. It includes different sorts of fixed, mobile and portable applications, including two-way radios, cell phones, individual PDAs, and wireless networking [1].

Figure 1 shows an example of wireless communication. The various available wireless technologies differ in local availability, coverage range and performance, and in some circumstances, users must be able to employ multiple connection types and switch between them. Supporting technologies include:

Wi-Fi is a wireless local area network that enables portable computing devices to connect easily to the Internet. Standardized as IEEE 802.11 a/b/g/n, Wi-Fi approaches speeds of some types of wired Ethernet. Wi-Fi has become normal standard for access in private homes, within offices, and at public hotspots.

Cellular Data Service offers coverage within a range of 10-15 miles from the nearest cell site. Speeds have increased as technologies have evolved, from earlier technologies such as GSM, CDMA and GPRS, to 3G networks such as W-CDMA, EDGE or CDMA2000.

ISSN: 2233-7857 IJFGCN

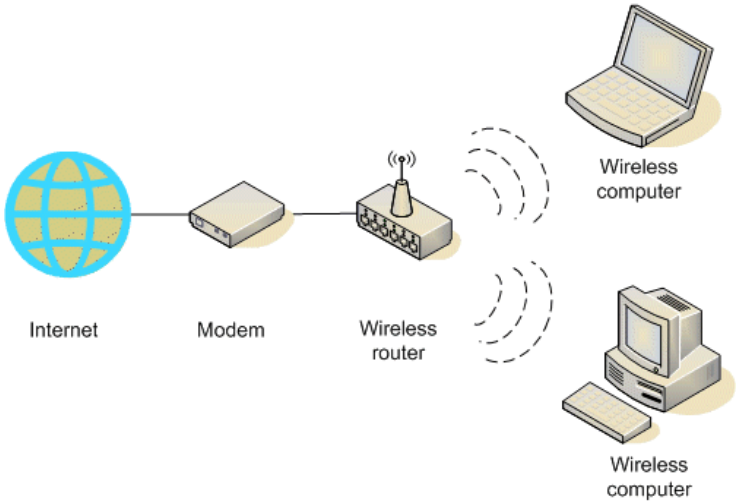

Figure 1. Wireless Communication

Mobile Satellite Communications may be used where other wireless connections are unavailable, such as in largely rural areas or remote locations. Satellite communications are especially important for transportation, aviation, maritime and military use.

Wireless Technology permits services, such as long range communications, that are impossible or impractical to implement with the use of wires. The term is commonly used in **Telecommunications Industry** to refer to telecommunications systems (*e.g.*, radio transmitters and receivers, remote controls, computer networks, network terminals, *etc.*,) which use some form of energy (*e.g.*, radio frequency (RF), infrared light, laser light, visible light, acoustic energy, *etc.*,) to transfer information without the use of wires. Information is transferred in this manner over both short and long distances [2, 3].
The following situations justify the use of wireless technology:

- To span a distance beyond the capabilities of typical cabling,
- To provide a backup communications link in case of normal network failure,
- To link portable or temporary workstations,
- To overcome situations where normal cabling is difficult or financially impractical, or
- To remotely connect mobile users or networks.

Wireless technology is becoming more and more popular due to so many advantages.

2. Need of Wireless Security

Security is one of important challenge which is to be handled in the era of wireless technology these days. Current security standards have shown that security is not keeping up with the growing use of wireless technology. Every now and then a new vulnerability comes in existence to the existing wireless standards. Wireless security is the prevention of unauthorized access or damage to computers using wireless networks. Wireless networks are very common, both for organizations and individuals. Many laptop computers have wireless cards pre-installed. The ability to enter a network while mobile has great benefits. However, wireless networking has many security issues. Hackers have found wireless networks relatively easy to break into, and even use

wireless technology to crack into wired networks. As a result, it's very important that enterprises define effective wireless security policies that guard against unauthorized access to important resources. Wireless Intrusion Prevention Systems are commonly used to enforce wireless security policies.

The risks to users of wireless technology have increased as the service has become more popular. However, there are many security risks associated with the current wireless protocols and encryption methods, and in the carelessness and ignorance that exists at the user and corporate IT level. Cracking methods have become much more sophisticated and innovative with wireless. Cracking has also become much easier and more accessible with easy-to-use Windows or Linux-based tools being made available on the web at no charge.

3. Security Requirements

While any organization wants to protect its sensitive data, to detect tampering of data and to limit access to authorized individuals, various industries must also comply with an array of regulatory and industry requirements and guidelines [4]. One common requirement is that sensitive data that is stored or communicated over public networks must be encrypted using certified algorithms. Another common requirement is for users to authenticate themselves using two-authentication, generally achieved by a combination of something the user possesses such as a security token (*e.g.*, USB dongle or security smart card), and something the user knows (*e.g.*, password). Biometric approaches can also be used as one of the authentication factors. Regulations are becoming more stringent, both at the state and federal level. Organizations designing new mobile-access solutions need to plan accordingly to ensure they comply with both current and future requirements.

The WEP was designed to provide the security of a wired LAN by encryption through use of the RC4 algorithm with two side of a data communication. The working of the WEP can be understood with the help of sender side encryption and receiver side decryption.

4. Security Threats to Wireless Networks

Protection of wireless networks means protection from attacks on confidentiality, integrity and availability. Possible threats come from vulnerabilities in the security protocols. This section explains various types of security attack techniques. These techniques can be applied to violate both confidentiality and integrity or only confidentiality and only integrity [5]. Different types of security attacks are shown in the Figure 2.

Traffic analysis: This technique enables the attacker to have the access to three types of information. The first type of information is related to identification of activities on the network. The second type of information important to the attacker is identification and physical location of access point in its surroundings. The third type of information an attacker can get by traffic analysis is information about the communication protocol. An attacker needs to gather the information about the size and number of the package over a certain period of time.

Eavesdropping: In case of eavesdropping attacker secretly listens to the private conversation of others without their permission. Eavesdropping attacks include *passive eavesdropping, active eavesdropping with partially known plaintext* and *active eavesdropping with known plaintext.*

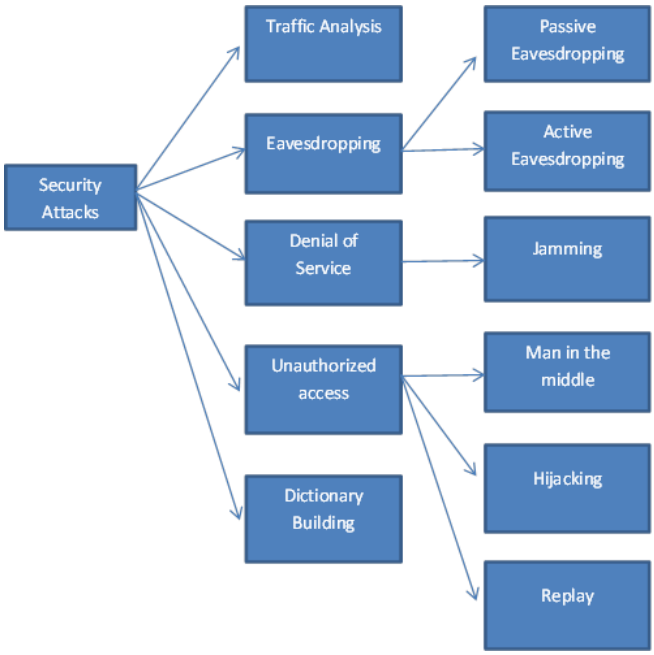

Figure 2. Different Types of Security Attacks

Passive eavesdropping is used to watch over an unlimited wireless session. The only condition to be fulfilled is that the attacker has the access to the area of emission. With a decrypted session the attacker is able to read the data during its transmission and gather data indirectly by surveying the packages. This kind of attack is not based on violation of privacy but information gathered in this way can be used for more dangerous kinds of attacks.

In *Active eavesdropping with partially known plaintext type* of attack, the attacker watches over a wireless session and actively injects own messages in order to reveal the content of the messages in the session. Precondition for this type of attack is an access to communication area and some knowledge on the part of the message, such as IP address. The attacker is able to modify the content of the package so that the integrity of the message remains preserved. Usually the attacker changes final IP or TCP address.

In *active eavesdropping with known plaintext type of attack*, the attacker injects messages known only to him into the traffic in order to create conditions for decryption of the packages that should be received by other wireless users. These conditions are created by creation of **I**nitialization **V**ector (**IV**) sequence and message for each single message that is sent. After some time, when a package with the same IV as in database appears, the attacker is able to decrypt the message. The only way to prevent this kind of attacks is to change key often.

Unauthorized access: Once the attacker gets the access to the network, he is able to initiate some other types of attacks or use network without being noticed. Some can be of an opinion that unauthorized use of the network is not a significant threat to the network since the access rights allocated to resources will disable the attackers. However, usually the unauthorized access is the key to initialization of **ARP** (**A**ddress **R**esolution **P**rotocol) attack. **V**irtual **P**rivate **N**etwork (**VPN**) and **IPsec** solution can protect users from the attacks that directly influence the confidentiality of application

data but cannot prevent attacks that indirectly ruin confidentiality. *Man in the middle, high-jacking and replay attacks* are the best examples of these kinds of attacks.

Man in the middle attack enables data reading from the session or modifications of the packages with violate integrity of the session. There are several ways to implement this type of attack. One way is when attacker disrupts the session and does not allow for the station to establish communications again with the **A**ccess **P**oint (**AP**). Station tries to establish session with the wireless network through AP, but can do that only through the workstation of the attacker pretending to be AP. At the same time, the attacker establishes connection and authentication with the AP. Now there are two encrypted tunnels instead of one: one is established between the attacker and AP, while the second one is established between the attacker and the station. This enables attacker to have the access to the data exchanged between the working station and the rest of the network. ARP attack is a sub-type of the man in the middle attack since these attacks are directed towards one component of wired network and not towards wireless clients. The attacker escapes authentication or provides false accreditations by this kind of attack. The attacker becomes valid user and gets the access to the network as authenticated user by getting the false accreditations.

In *High-jacking* type of attack, the attacker deprives the real owner of the authorized and authenticated session. The owner knows that he has no access to the session any more but is not aware that the attacker has taken over his session and believes that he lost the session due to ordinary lacks in network functioning. Once the attacker takes over a valid session he can use it for various purposes over a certain period of time. This attack happens in a real time.

Replay attack is used to access the network through authorization. The session that is under an attack does not change nor disrupt in any way. The attack does not happen in a real time. The attacker gets the access to the network after the original session expires. The attacker comes to the authentication of one or more sessions, and then replies to the session after a certain period of time or uses couple of sessions to compose the authentication and reply to it.

Denial of Service (DoS): An attacker tampers with the data before it is communicated to the sensor node. It causes denial of service attack due to wrong or misleading information. *Jamming* is one of DoS attack on network availability. It is performed by malicious attackers who use other wireless devices to disable the communications of users in a legitimate wireless network.

Dictionary-Building Attacks: In these types of attacks an attacker goes through a list of candidate passwords one by one; the list may be explicitly enumerated or implicitly defined, can incorporate knowledge about the victim, and can be linguistically derived. Dictionary building attacks are possible after analyzing enough traffic on a busy network.

To avoid these threats and to improve the security of the wireless networks various companies collaborated to make the Wi-Fi alliance to make the robust security protocol. Initially they came with the new security protocol for wireless networks known as **W**i-Fi **P**rotected **A**ccess (**WPA**). The WPA protocol implements the majority of the IEEE 802.11i standard, and was intended as an intermediate measure to take the place of WEP. WPA uses the **T**emporal **K**ey **I**ntegration **P**rotocol (**TKIP**) algorithm for encryption. TKIP is a security protocol used in the IEEE 802.11 wireless networking standard. TKIP was designed by the IEEE 802.11i task group and the Wi-Fi Alliance as a solution to replace WEP without requiring the replacement of legacy hardware. This

was necessary because the breaking of WEP had left WiFi networks without viable link-layer security, and a solution was required for already deployed hardware [6].

WPA has following advantages:

- A cryptographic **M**essage **I**ntegrity **C**ode (**MIC)**, called Michael, to defeat forgeries. Message Integrity Code (MIC) is computed to detect errors in the data contents, either due to transfer errors or due to purposeful alterations. This prevents man in the middle attack, denial of service attack.
- A new **I**nitialization **V**ector (**IV**) sequencing discipline, to remove replay attacks from the attacker's arsenal.
- A rekeying mechanism, to provide fresh encryption and integrity keys, undoing the threat of attacks stemming from key reuse. Thus provides security against eavesdropping attacks.

Although the WPA protocol has increased wireless security to a great extent but it also has some problems.

- **Weakness in Passphrase Choice in WPA Interface:** This weakness was based on the **P**air **W**ise **M**aster key (**PMK**) that is derived from the concatenation of the passphrase, **S**ervice **S**et **I**dentifier(**SSID**), length of the SSID and nonces (a number or bit string used only once in each session).
- **Possibility of the Brute Force Attack:** Brute Force is considered to be a passive attack in which the intruder will generate every possible permutation in the key and try to decrypt the encrypted message with each generated permutation, and validate the output by means of cross comparison with words, file header and any other data.
- **Placement of MIC:** It is considered a problem because it can be used by any hacker in validating the contents of the decrypted message combined with the brute force attack.

After WPA protocol **W**i-Fi **P**rotected **A**ccess2 (**WPA2**) protocol came. The WPA2 uses the more robust encryption algorithm known as **A**dvance **E**ncryption **S**tandard (**AES**). Advanced Encryption Standard is a symmetric-key encryption standard adopted by the U.S. government. AES was announced by **N**ational **I**nstitute of **S**tandards and **T**echnology (**NIST**) [4] after a 5-year standardization process in which fifteen competing designs were presented and evaluated before Rijndael was selected as the most suitable. The Rijndael cipher was developed by two Belgian cryptographers, Joan Daemen and Vincent Rijmen, and submitted by them to the AES selection process. There are various advantages of WPA2.

Advantages of WPA2 include:

- WPA2 supports IEEE **802.1X/EAP** (**E**xtensible **A**uthentication **P**rotocol) authentication or **P**re **S**hared **K**ey (**PSK**) technology. A pre-shared key or **PSK** is a shared secret which was previously shared between the two parties using some secure channel before it needs to be used. Such systems almost always use symmetric key cryptographic algorithms. Thus removing the passphrase choice problem of WPA.
- It also includes a new advanced encryption mechanism using the **C**ounter Mode with **C**ipher Block **C**haining **M**essage Authentication Code **P**rotocol (**CCMP**) called the **A**dvanced **E**ncryption **S**tandard (**AES**). Thus providing security against most of the attacks encountered due to weak encryption key.

Although WPA2 uses more robust security algorithm *i.e.*, AES but it also has some problems like:

- **Brute Force Attack:** Brute Force is considered to be a passive attack in which the intruder will generate every possible permutation in the key and try to decrypt the encrypted message with each generated permutation, and validate the output by means of cross comparison with words, file header and any other data.
- **Placement of Message Integrity Check (MIC) bits:** It is considered a problem because it can be used by any hacker in validating the contents of the decrypted message combined with the brute force attack.

Time Factor: It is a very important factor in which we measure how long will it take to brute force a protocol, currently this is done by calculating how many permutations are there in the encryption/ decryption key. As the processing power of the computers is ever increasing WPA2 protocol requires small time to brute force [7].

5. Literature Review

The KirtiRaj Bhatele, *et al.*, [7] presented hybrid security protocol for better security using a combination of both symmetric and asymmetric cryptographic algorithms. In this hash value of the decrypted message using AES algorithm is calculated using MD5 algorithm. This hash value has been encrypted with dual RSA and the encrypted message of this hash value also sent to destination. Now at the receiving end, hash value of decrypted plaintext is calculated with MD5 and then it is compared with the hash value of original plaintext which is calculated at the sending end for its integrity. By this we are able to know whether the original text being altered or not during transmission in the communication medium.

Arash Habibi Lashkari, *et al.*, [8] presented a survey on wireless security protocols (WEP, WPA and WPA2/802.11i). Here WEP protocol types, weaknesses and enhancements, WPA protocol types, WPA improvements such as cryptographic message integrity code or MIC, new IV sequencing discipline, per packet key mixing function and rekeying mechanism. They also explained major problems on WPA that happened on PSK part of algorithm. Finally paper explained third generation of wireless security protocol as WPA2/802.11i.

Gamal Selim, *et al.*, [9] explained various types of security attacks modification, fabrication, interception, brute force, maintainability and static placement of MIC. They surveyed currently available security protocols i.e. WEP, WEP2, WPA and WPA2. They also proposed a new mechanism called multiple slot system (MSS). MSS makes use of the key selector, slot selector and MIC shuffle selector. MSS uses one of four encryption algorithm RC4, RSA, Blowfish and AES.

Hyung-Woo Lee, *et al.*, [10] explained various issues and challenges in wireless sensor network. Paper explained two types of wireless security attacks – one is the attack against the security mechanisms and another is against the basic mechanisms like routing mechanism. Major attacks explained are denial of service attack, attacks on information in transit, sybil attack, hello flood attack, wormhole attack, blackhole/sinkhole attack. Paper also explained the various security schemes for wireless sensor networks like wormhole based, statistical en-route filtering, random key and tinysec. Holistic view of security in wireless sensor networks is also described.

Lifeng Sang, *et al.*, [11] proposed shared secret free security infrastructure for wireless networks based on two physical primitives: cooperative jamming and spatial signal enforcement. Cooperative jamming is for confidential wireless communication and spatial signal enforcement is for message authenticity. Proposed infrastructure

provides confidentiality, identity authentication, message authentication, integrity, sender non-repudiation, receiver non repudiation and anonymity.

Andrew Gin, *et al.*, [12] compared the performance analysis of evolving wireless 802.11 security architecture. Paper explained wireless network security methods. Paper explained security layers like WEP shared key authentication and 40 bit encryption, WEP shared key authentication and 104 bit encryption, WPA with PSK authentication and RC4 encryption, WPA with EAP-TLS authentication and RC4 encryption, WPA2 with PSK authentication and AES encryption and WPA2 with EAP-TLS authentication and AES encryption. Effects on throughput are also discussed.

Eric Sabbah, *et al.*, [13] explained attacker motivation, vulnerabilities and opportunities currently available to hackers. Wireless sensor networks are exposed to numerous security threats that can endanger the success of the application. Paper explains that security supports in wireless network is challenging due to the limited energy, communication bandwidth and computational power. Security issues and currently available solutions, various types of attacks like - attacks on routing and DoS attack, injecting false packets, attacks on real time requirements, attacks on the network using topological information, attacks on localization.

Floriano De Rango *et. al.*, [14] proposed static and dynamic 4 - way handshake solutions to avoid denial of service attack in WPA and IEEE 802.11i. Paper also explained DoS and DoS flooding attacks against IEEE 802.11i 4-way handshake. Paper also compared static versus dynamic resource oriented solutions for the 4 way handshake.

Stephen Michell, *et al.*, [15] proposed state based key hope protocol (SBKH) that provides a lightweight encryption scheme for battery operated devices such as the sensors in a wireless sensor network as well as small office, home office (SOHO) users. State based key hope protocol implements encryption in a novel state based way so as to provide cheap and robust security without additional overheads of encryption. Implementation of SBKH on real hardware is a challenge.

6. Conclusion

In the research work it is observed that many organizations are currently deploying wireless networks typically to use IEEE 802.11b protocols, but technology used is not secure and still highly susceptible to active attacks and passive intrusions. Currently available security protocols like WEP, WPA and WPA2 have some advantages and disadvantages and also there are some vulnerability exists in these security protocols. Various types of security attacks are possible as explained in the previous sections.

References

[1] http://securityuncorked.com/2008/08/history-of-wireless-security/.
[2] http://csrc.nist.gov/wireless.
[3] http://www.isaac.cs.berkeley.edu/isaac/wep-faq.html.
[4] Stamatios and V. Kartalopoulos, Editors, “Differentiating Data security and Network Security”, IEEE International Conference on Communications, **(2008)** May 19-23, Beijing.
[5] S. D. Kanawat and P. S. Parihar, Editors, “Attacks in Wireless Networks”, International Journal of Smart Sensors and Adhoc Networks, **(2011)** May 18-23.
[6] Y. X. Lim and T. Schmoyer, Editors, “Wireless Intrusion detection and response”, IEEE Information Assurance Workshop, **(2003)** June 18-20, Westpoint, Newyork.
[7] K. Bhatele, A. Sinhal and M. Pathak, Editors, “A Novel Approach to the Design of New Hybrid Security Protocol Architecture”, IEEE International Conference on Advanced Communication Control and Computing Technologies (ICACCCT), **(2012)** August 23-25, Ramanathapuram.

[8] A. H. Lashkari and M. M. S. Danesh, Editors, "A Survey on Wireless Security Protocols WEP, WPA and WPA2/802.11i", IEEE International Conference on Computer Science and Information Technology, **(2009)** August 8-11, Beijing.
[9] G. Selim, H. M. E. Badawy and M. A. Salam, Editors, "New Protocol design for Wireless Networks security", IEEE International Conference on Computer Science and Information Technology (ICACT), **(2006)** Feb 20-22.
[10] H.-W. Lee, A.-S. K. Pathan and C. S. Hong, Editors, "Security in Wireless Sensor Networks: issues and challenges", International Conference on Advanced Communication Technology (ICACT), **(2006)** February 20-22, Phoenix Park.
[11] L. Sang and A. Arora, Editors, "A Shared Secret Free Security Infrastructure for Wireless Networks", ACM Transactions on Autonomous and Adaptive Systems (TAAS), **(2012)** July.
[12] A. Gin and R. Hunt, Editors, "Performance Analysis of Evolving Wireless IEEE 802.11 Security Architectures", ACM International Conference on Mobile Technology Applications and Systems, **(2008)**.
[13] E. Sabbah, A. Majeed, K. Y.-D. Kang, K. Liu and N. Abu-Ghazaleh, Editors, "An application-driven perspective on wireless sensor network security", ACM international workshop on Quality of service & security for wireless and mobile networks, **(2006)**.
[14] F. De Rango, D. C. Lentini and S. Marano, Editors, "Static and Dynamic 4-Way Handshake Solutions to Avoid Denial of Service Attack in Wi-Fi Protected Access and IEEE 802.11i", EURASIP Journal on Wireless Communications and Networking, **(2006)** June.
[15] S. Michell and K. Srinivasan, Editors, "State Based Key Hop Protocol: A Lightweight Security Protocol for Wireless Networks", ACM international workshop on performance evaluation of wireless adhoc, sensor, and ubiquitous networks, **(2004)**.

Authors

Umesh Kumar, he is working as an Assistant Professor in Computer Engineering department of YMCA University of Science and Technology, Faridabad (YMCAUST), India since April 2012. He has completed his M.Tech degree in Computer Engineering in 2010 from YMCAUST. He has around two year experience in Android application development. He is currently pursuing Ph.D from the same university.

Dr. Sapna Gambhir, is working as an Associate Professor in Computer Engineering department of YMCA University of Science and Technology, Faridabad (YMCAUST), India. She has completed her doctorate in Computer Engineering in 2010 from Jamia Milia Islamia, Delhi, India. She has teaching experience of 12 years during which published many papers in various national/ international conferences and journals. Her current areas of interest are Network Security, Mobile Adhoc Networks, Wireless Sensor Networks and Online Social Networks.

