5th INTERNATIONAL CONFERENCE
TRANSPORT SYSTEMS TELEMATICS TST'05

ZESZYTY NAUKOWE
POLITECHNIKI ŚLĄSKIEJ 2005
TRANSPORT z.59, nr kol. 1691

WLAN, IEEE802.11, computer networks, urban transport systems, telematics, TCP/IP, reliability, data transmission, network security, data mining,

Rafał CICHOCKI[1]

WLAN NETWORKS IN URBAN TRANSPORT SYSTEMS

Wide use of the wireless networks WLAN IEEE 802.11 determined turning point in data transmission in urban transport systems. Author describes basic properties of wireless networks and place emphasis on reliability and security of transmitted data and system itself. Those aspects play of great importance in transportation systems telematics.

SIECI WLAN W SYSTEMACH TRANSPORTU MIEJSKIEGO

Powszechne użycie sieci bezprzewodowych WLAN standardu IEEE 802.11 wyznaczyło punkt zwrotny w transmisji danych w systemach transportu miejskiego. Autor opisuje podstawowe właściwości sieci bezprzewodowych oraz kładzie szczególny nacisk na niezawodność i bezpieczeństwo zarówno transmitowanych danych jak i samego systemu. Aspekty te odgrywają ogromną rolę w telematyce systemów transportowych.

1. INTRODUCTION

Wide use of the wireless networks WLAN IEEE 802.11 determined turning point in data transmission in urban transport systems. Relatively low cost of infrastructure and data transmission and speed, which stretches up to 100MB/s create platform for building inexpensive and highly efficient communication systems. These features designate WLAN network to be communication base for upgrading Intelligent Transport Systems. Many telecommunications services providers offer such solutions. The example of taking advantage of 802.11 networks can be: usage of ATHEROS technology at 11th World ITS Congress in Nagoya in 2004, or public transport information systems in Gothenburg. Author describes basic properties of wireless networks and place emphasis on reliability and security of transmitted data and system itself. Those aspects play of great importance in transportation systems telematics. Wireless networking imposes known security along with obvious benefits. To take full advantage of wireless connectivity one need to consider issues such ass user authentication and protection of data crucial to transport safety and security as well as configuration, reliability and future expansion of the network.

[1] Faculty of Informatics Foundations and Computer Networks, Maritime University in Gdynia, Morska 83, 81-225 Gdynia, Poland, r.cichocki@am.gdynia.pl,

1.1. IEEE 802.11 WLAN NETWORKS

An 802.11 LAN is based on cellular architecture where the system is subdivided into cells, where each cell (called Basic Service Set, or **BSS** for short) is controlled by Base Station (called Access Point, **AP** in the 802.11 nomenclature). In many cases wireless LAN is formed by a single cell controlled by AP (it can also work without AP in ad-hoc mode), however most installations will be formed by multiple cells, where Access Points are connected through some kind of backbone (called Distribution System or **DS**), typically Ethernet. Whole wireless system (cells, AP and backbone) is seen to the upper layers of the ISO/OSI model as a single 802 network (called Extended Service Set, **ESS**). Ad hoc network is composed solely of stations within mutual communication range of each other via the wireless medium (WM). An ad hoc network is typically created in a spontaneous manner. The principal distinguishing characteristic of an ad hoc network is its limited temporal and spatial extent. These limitations allow the act of creating and dissolving the ad hoc network to be sufficiently straightforward and convenient so as to be achievable by nontechnical users of the network facilities; i.e., no specialized "technical skills" are required and little or no investment of time or additional resources is required beyond the stations that are to participate in the ad hoc network. The term ad hoc is often used as slang to refer to an independent basic service set (IBSS).

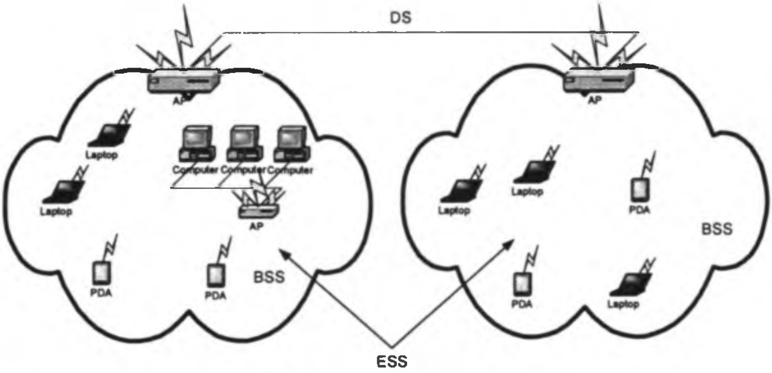

Fig.1. Typical 802.11 LAN with all components

1.1.1. IEEE 802.11 LAYERS DESCRIPTION

As any 802.x protocol, the 802.11 protocol covers the MAC and Physical Layer. The standard currently defines one MAC which interact with three physical layers:

- Frequency Hopping Spread Spectrum in the 2.4GHz Band
- Direct Sequence Spread Spectrum in the 2.4GHz Band
- InfraRed

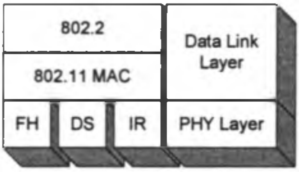

Fig.2. 802.11 Layers

Beyond standard functionality usually performed by MAC Layers, the 801.11 MAC performs other functions such as: fragmentation, packet retransmission, and acknowledgments. MAC layer also defines two different access methods: Distributed Coordination Function and the Point Coordination Function.

1.1.2. MEDIUM ACCESS METHOD

The basic access mechanism, called Distributed Coordination Function, is basically Carrier Sense Multiple Access with Collision Avoidance (CSMA/CA) mechanism. A station desiring to transmit senses the medium, if the medium is busy (some other station is transmitting) then the station will defer its transmission to a later time, if medium is sensed free then the station is allowed to transmit. The problem occurs when two station start to transmit in this same time. Collision detect mechanism known from Ethernet cannot be used in WLAN because of two main reasons: it would require Full Duplex radio what significantly increase costs, and second on the WLAN environment we can’t assume, that all stations hear each other (which is basic assumption of the collision detect algorithm). In order to overcome these problems, the 802.11 uses Collision Avoidance mechanism together with a Passive Acknowledgments scheme. In short if medium is free for a specified time (called Distributed Inter Frame Space) then station is allowed to transmit. Receiving station will check CRC and send Acknowledgment packet (ACK). If the sender do not receive ACK, then will be retransmit packet until it get acknowledgments or thrown away after a given number of retransmissions. In order to reduce probability of two station colliding because cannot hear each other, the standard defines a Virtual Carrier Sense mechanism. A station willing to transmit will transmit short control packet called RTS (Request To Send), which will include source, destination and the duration of following transaction (packet and respective ACK). Destination station will respond (if medium is free) with response packet CTS (Clear To Send) which will include this same duration information. All stations receiving either RTS and/or CTS will set their Virtual Carrier Sense indicator (NAV – Network Allocation Vector), for the given duration).

1.1.3. JOING AN EXISTING CELL (BSS)

When a station want to access and existing BSS it needs to get synchronization information from Access Point (or other station in ad hoc mode). Station can get this information by one of two means: passive from Beacon Frame from AP (beacon is periodic frame sent by the AP with synchronization information) or active by transmitting Probe Request Frame and wait for Probe Response from AP.

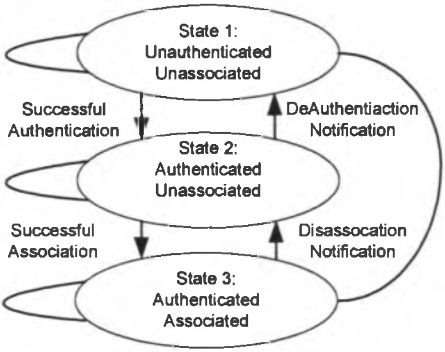

Fig.3. Transition between station state diagram

Once station has found AP it will go through Authentication Process which is interchange information between station and AP where each side proves the knowledge of a given password. When station is authenticated then it will start the Association Process, which is exchange of information about the station and BSS capabilities and which will allows DSS (the sets of APs) to know about stations current position. Only after the association process is completed, a station is capable of transmitting and receiving data frames. Its important to notice, that whole process is running without any cryptography protection. Relationship between stations state and service are given in the figure 3.

2. SECURITY ANALYSIS

It is important to understand the main threats in network, particularly in a WLAN environment. This threats should be kept in mind when implementing a network design.

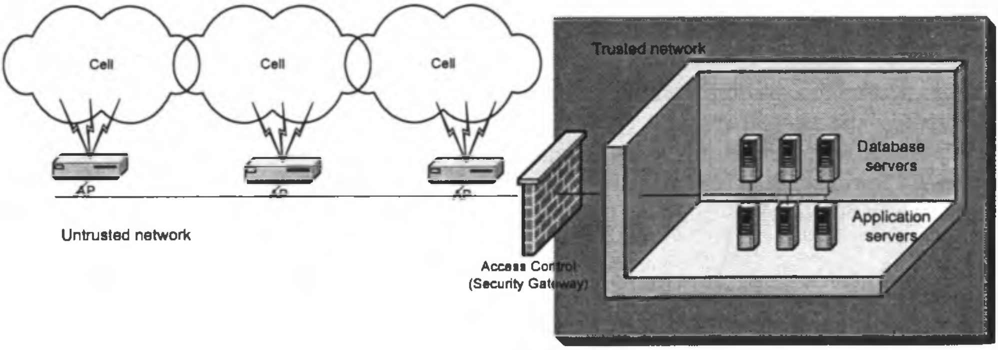

Fig.4. Typical enterprise WLAN network

A wireless LAN is insecure because it is accessible by the anyone in the vicinity. The server network must be secured from outsider by security gateway which will be authenticate users. Data or packet entry and exit to and from servers must be controlled by security gateway, as well.

2.1. EAVESDROPPING ON DATA

It is obvious that unencrypted data transmitted via WLAN network can be stolen by the hacker in the vicinity, but it's not common knowledge, that not every of encryption standard used in WLAN are sufficient to secure data. Most popular Wired Equivalent Privacy (WEP) can be broken within minutes if large amounts of encrypted data is transmitted through the wireless network. However WPA-PSK method provide both station-specific and dynamic keys it doesn't satisfy expectations due to fact, that preshared key have to be distributed across all wireless station. Only 802.1x-based Extensible Authentication Protocol (AEP) along with Transport Layer Security (TLS) or Protected EAP (PEAP) provides dynamic keys and mutual authentication with user-specific credentials. EAP-TLS works with user-specific certificates and PEAP works with password authentication. This solutions are sufficient to provide appropriate security level. Another approach utilize technology such as IPsec or Virtual Private Network which are independent of WLAN standard.

2.2. DENIAL OF SERVICE

Denial-of-service (DoS) attack use several ways to destabilize a host, device or network. In this kind of attacks primary goal is to deny the victim access to particular resource. DoS is characterized by an explicit attempt by attackers to prevent legitimate users of service from using that service. For example attackers can: to attempt to "flood" network and disabling legitimate traffic, to disrupt communications between two machines or between machine and network, to prevent a particular person from accessing network or service, to disable service(s) or host(s).

Exists numerous techniques of DoS attacks. Some of them are based on "flooding" method which consist in consume network bandwidth or consuming kernel data structures involved in establishing network connection (SYN-flood). Other are based on consuming other resources such as disk space or system memory. It can be done by for example flooding with e-mail messages or events which generates system logs or alerts. In this case system logs files can overfull badly designed system. Many techniques based on specific devices or operating systems vulnerabilities do exist. Such techniques are very easy to perform. Defence and protection against DoS attack depends on used attack techniques and in some cases only solution is to detect and identify and makes powerless, but of course it isn't simple. As one can conclude exists some kind of distributed attacks such as Trenoo, Tribe or stacheldraht and similar, which are extremely hard to protect from. Such techniques and tools uses specialized and distributed networks, cryptographic method and other sophisticated approach to stealth their presents and attack victim. In some cases there is a need to upgrade devices firmware to protect it from some attacks. Other approach can use traffic control mechanism and bandwidth reservation for critical stations to prevent packet flooding attacks.

In 802.11 WLAN it's even much worse situation. As it was mentioned above every station needs to be authorized and associated to the Access Point before it can send any packet over wireless network. This process is performed with so called management frames. This frames are send in “clear text”, even if Access Point use cryptography for data transmission. What does it mean? According to Lach [7] research any intruder in the vicinity can spoof an Access Point or wireless station and sends management frames, which will cause return to the “Unauthenticated, Unassociated” state. In this state station cannot send information through network and need to authorize itself, establish link again and return to “Authenticated, Associated” state. Because this process last for some time, depends on radio signal quality, Lach proof that attacker need to send only 1 frame per second to completely prevent any network communication.

2.3. USER AUTHENTICATION AND IDENTITY TRICKS

There are several vulnerabilities associated with identities of user. Attacker can “spoof” as a legitimate user to access and change critical resources. Obviously data encryption can prevent password sniffing, but it is strongly recommended to use robust authentication credentials such as X.509 public key certificates.

In normal circumstances user provides its authentications credentials to proof its identity and rights. This scheme is vulnerable to attack very simple to carry out. Attackers can deploy its own Access Points with strong radio signal to make wireless station associate with them. Then they would present fake authentication page to get user credential. Because of this it is needed to authentication gateway to proof its identity before user give its own credentials. Wireless stations should provide its own credentials only after verifying the peer identity. Mutual authentication and validation of identity of peer is required. In this case it is important that stations authenticate with security gateway and not with intermediate access points.

2.4. OTHER THREATS

Many other threats, which will not be fully described because of extensiveness of this topic, do exist. Rough AP mentioned above can be deployed both by the legitimate user (to “improve” access to corporate wire LAN) and the attackers. All the AP should be places outside the secure network and security gateway should allow only traffic from trusted (authenticated) Access Points. Trusted AP should be capable to detect other APs in the neighbourhood and report these to the security gateway. “Replay of data” attack can be performed by simply recording packet exchange and then replaying them without any modification. It will impact on logging system which will log false events. To prevent such attack strong encryption with per packet authentication have to be use. Another threat is bring by laptops and other PDAs which are used outside corporate network. They are exposed to virus and worms and after return to corporate can be source of infection and jeopardize all stations and servers in network.

3. WLAN AS A TELEMATIC SYSTEM OF CONTROL STRUCTURE

As Wawrzyński [9] pointed safety of transportation systems in particular control systems are main issues to be considered and deeply analyzed. Safety of transportation control system is its ability to maintain safe state of controlled object. In case of emergency controlling have to be preserved. Return to safe state must be possible. This feature results from quality of implemented software and hardware solutions used for controlling tasks of the system [9]. Following features influence transportation systems safety:

- highly functional reliable solutions in system structure
- ability of detection threat to controlling tasks realization
- transportation process participants life and health saving procedures

Controlling process is supported by telematic real time system, which meet structural safety requirements. Such systems have to contain features, which is supposed to prevent failure possibly leading to critical malfunction – e.g. life threatening or causing considerably material losses. One of the most important transportation system requirement is its ability to work under real-time constraints. It means that maximum delay in system reaction, deadline must be observed. Telematic system in transportation control process have to be up to very rigorous reliability assumptions.

Three main issues require special attention:

- fault tolerance
- structural redundancy (contributing to above mentioned tolerance)
- informational redundancy

Increasing of system reliability can be accomplished in two ways: fault prevention and fault tolerance. Fault prevention is based on increase reliability of individual elements of the system. Such overall reliability was characterized a priori as minimal acceptable fault probabilities. Fault tolerance is accomplished by structural redundancy. Essential system component are duplicated and when one of them fails then duplicate take over its functions and transportation process runs without disrupting.

Characteristic of WLAN 802.11 wireless networks was presented as possible part of system security. Review of the primary threats were done. Special emphasis was placed on denial of service attacks method, which directly influence to reliability of WLAN network. Fact, that little afford is needed to perform effective attack. The attack can totally disable network and it is hard to avoid it. All this aspects were presented as well. Luckily it is possible to protect network both against sniffing and data integrity attack, and many identity control method can be applied. The IEEE 802.11 network control mechanisms (3 station states, control frames) on the lowest level are its Achilles heel. It was shown that station association mechanism (process of establishing connection to the Access Point) is based on management frames. Unfortunately management frames are transmitted in "clear text" and in simple manner attacker can use them to unplug station from access point, in effect attacker can destabilize network.

4. QUESTIONS AND FUTURE WORKS

In present form standard 802.11 does not consider any improvement which can secure management process. In connection with this facts it is reasonable to ask a few questions:

- Can the standard, WLAN 802.11 wireless network, be used as reliable telematic system in view of requirements for control process in transportation systems?
- How can fault prevention and tolerance be improved in WLAN during communication system development?
- How and if at all, using structural redundancy, WLAN can be secured against denial of service attacks?
- Do profits resulting from using wireless networks overweight threats inherently related to WLAN equipment?

Positive answers to some questions do exist, other need to be found out. Author intends to design appropriate laboratory station and will undertake research to answer all this questions.

BIBLIOGRAPHY

[1] BRENNER P., A technical Tutorial on the IEEE 802.11 Protocol, http://www.sss-mag.com/pdf/802_11tut.pdf

[2] CERT, Denial of Service Attacks, http://www.cert.org/tech_tips/denial_of_service.html.

[3] CICHOCKI R., Techniki Uczenia Maszynowego w Systemach Wykrywania Intruzów, Współczesne problemy sieci komputerowych. Zastosowanie i bezpieczeństwo., Praca zbiorowa pod redakcją A. Grzywaka, WNT 2004.

[4] CICHOCKI R., Bezpieczeństwo danych w systemach rozproszonych – systemy wykrywania intruzów, Studia Informatica, Gliwice 2003.

[5] CICHOCKI R., Wybrane problemy bezpieczeństwa sieci komputerowych, XX Międzynarodowe Sympozjum Naukowe Studentów i Młodych Pracowników Nauki, Zielona Góra 1999.

[6] IEEE Computer Society, PART11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications, http://standards.ieee.org/getieee802/802.11.html, 1999

[7] LACH J. Ataki DOS w WLAN, Wysokowydajne sieci komputerowe, zastosowanie i bezpieczeństwo, WKŁ, Warszawa 2005.

[8] UNIVERSITY OF WASHINGTON, Distributed Denial of Service (DDoS) Attacks/tools, http://staff.washington.edu/dittrich/misc/ddos/.

[9] WAWRZYŃSKI W., Bezpieczeństwo systemów sterowania w transporcie, Wydawnictwo Instytutu Eksploatacji, Warszawa-Radom 2004.

Reviewer: Ph. D. Stanisław Krawiec