MINISTRY OF EDUCATION AND SCIENCE OF UKRAINE
NATIONAL AVIATION UNIVERSITY
FACULTY OF AERONAVIGATIONS, ELECTRONICS AND TELECOMMUNICATIONS
DEPARTMENT OF TELECOMMUNICATION AND RADIO ENGINEERING SYSTEMS

ADMIT TO DEFENCE

Head of the Department

Victor HNATIUK

“_____” _____2023 y.

QUALIFICATION WORK

(EXPLANATORY NOTE)

MASTER'S DEGREE GRADUATE

Topic: «Security system of mobile ad-hoc networks»

Performer: Mykola KOLCHYN

(signature)

Supervisor: Maryna MALOIED

(signature)

Consultants from individual sections of the explanatory:

Consultant in the «Occupational Safety» section: Batyr KHALMURADOV

(signature)

Consultant of the «Environmental Protection» section: Andrian IAVNIUK

(signature)

N-controller: Denys BAKHTIIAROV

(signature)

Kyiv 2023

NATIONAL AVIATION UNIVERSITY

Faculty of aeronavigation, electronics and telecommunications
Department of telecommunications and radioelectronic systems
Specialty 172 «Telecommunications and radioengineering»
Educational and professional program «Telecommunication systems and networks»

APPROVE

Head of the Department

_____ Victor HNATIUK

"_____"_____2023 y.

TASK

for the performance of qualification work

Mykola KOLCHYN

(full name of the graduate)

1. Topic of qualification work: « Security system of mobile ad-hoc networks »

approved by the rector's order from «28» september 2023 y. №1965/ст.

2. The term of the work: from 02.10.2023 y. to 31.12.2023 y.

3. Initial data for work: Ad-Hoc wireless networks is being investigated; security of mobile information technologies; issues in Ad-Hoc wireless networks; advantages and disadvantages of typical technological protections against network attacks; security of the public key infrastructure.

4. The content of the explanatory note: Ad-Hoc wireless networks – a new level of mobile information technology development; issues in Ad-Hoc wireless networks; technological protection against network attacks; Ad-Hoc network security using a self-organized public key infrastructure; occupational health; environmental protection.

5. List of mandatory graphics (illustrative) material: cellular and ad hoc wireless networks; differences between cellular networks and ad hoc wireless networks (table); wireless mesh network covering a highway; classifications of attacks; defense against attacks.

6. Calendar plan-schedule

№	Task	Term of implementation	Performance note
1	Develop a detailed content of the sections of the thesis	02.10.2023-04.10.2023	Done
2	Introduction	05.10.2023-08.10.2023	Done
3	Ad-Hoc wireless networks – a new level of mobile information technology development	09.10.2023-22.10.2023	Done
4	Issues in Ad-Hoc wireless networks	23.10.2023-05.11.2023	Done
5	Technological protection against network attacks	06.11.2023-20.11.2023	Done
6	Ad-Hoc network security using a self-organized public key infrastructure	21.11.2023-30.11.2023	Done
7	Occupational Health	01.12.2023-06.12.2023	Done
8	Environmental protection	07.12.2023-17.12.2023	Done
9	Elimination of shortcomings and defense of the thesis	18.12.2023-31.12.2023	Done

7. Consultants from separate sections

Chapter	Consultant (position, Full Name)	Date, signature	
		Issued the task	Task accepted
Occupational Safety	Ph.D. in Med., Professor Batyr KHALMURADOV		
Environmental Protection	Ph.D. in Biol., Associate Professor Andrian IAVNIUK		

8. Release date of the task: September “29", 2023

Supervisor of Qualification Work _____ Maryna MALOIED

(signature of the supervisor) (full name)

The task has been taken on for execution _____ Mykola KOLCHYN

(graduate signature) (full name)

ABSTRACT

Graduate work on the topic «Security system of mobile ad-hoc networks». It contains 127 p., 3 tables., 21 figures., 18 references.

KEYWORDS: AD-HOC WIRELESS NETWORKS, TRAFFIC SECURITY TECHNOLOGIES,

The purpose and objectives of the study is analysis of technological means of providing security system of mobile ad-hoc networks, substantiation as well as provision of recommendations for the use of modern methods of cryptography and traffic protection in ad-hoc networks.

The object of study is ad-hoc networks.

The subject of research is methods s of security system of mobile ad-hoc networks.

Research methods are comparative analysis of scientific literature, optimization of information technologies, methods of information protection, methods of scientific research.

CONTENTS

LIST OF ABBREVIATIONS

AK – asymmetric key

BS – base station

GPS – global positioning system

iCAR – integrated cellular ad-hoc relay

IN – intermediate node

IS – information security

KEK – key encrypting key

MAC – medium access control

MANET – mobile ad-hoc networks

MCNs – multi-hop cellular networks

PRNET – Packet Radio Network

ITU – Telecommunications Union Radiocommunication

SK – symmetric key

QoS – Quality of service

WN – wireless networks

ARPA – Advanced Research Projects Agency

PIN – personal identification number

PANs – personal area networks

INTRODUCTION

Actuality of theme. Wireless networks (WN) are a technology for transmitting/receiving information (including voice, data, multimedia) using radio communication (modulated electromagnetic waves propagating in open space). Many modern BMs (let's tentatively call them "traditional") are now widely used, for example: mobile cellular communication, Wi-Fi, Wi-Max, etc. networks.

Recently, another class of technologies based on the principle of communication organization (it is known as Ad-Hoc networks) with dynamic self-organization and multihop routing, which is intended for decentralized, dynamic, distributed applications, has been actively developing.

The specifics of such modern information communication applications and future scenarios, potential technical limitations on the part of end devices - all this raises the general problem of a theoretical and conceptual plan regarding the architecture of mechanisms, principles and organization of secure information exchange in BM; and imposed engineering and technical requirements, primarily for information security (IS).

Most of the ad-hoc network traffic security technologies considered in the thesis are aimed at preventing security breaches based on cryptographic mechanisms. However, these mechanisms alone cannot always effectively cover the specific vulnerabilities of Ad-Hoc networks and do not protect against all possible threats. However, those parts related to the actual architecture and mechanisms of reactive security technologies of Ad-Hoc networks, especially the mechanisms and measures for responding to incidents of attacks in the data forwarding plane of multi-hop routing, remain insufficiently resolved today, or these solutions are not suitable for practical application. . A promising direction is also the creation of a second line of defense aimed at detection, response and processing of intrusions.

The purpose and objectives of the study is analysis of technological means of providing security system of mobile ad-hoc networks, substantiation as well as provision of

recommendations for the use of modern methods of cryptography and traffic protection in ad-hoc networks.

The object of study is ad-hoc networks.

The subject of research is methods s of ecurity system of mobile ad-hoc networks**.**

Research methods are comparative analysis of scientific literature, optimization of information technologies, methods of information protection, methods of scientific research.

The practical significance of obtained results. Materials of the diploma work are recommended for use in research and practical activities on the planning ad-hoc wireless networks**.**

Approbation of the obtained results. The results of the thesis can be used in the educational process when studying the disciplines related to radio communication networks.

CHAPTER 1
AD-HOC WIRELESS NETWORKS – A NEW LEVEL OF MOBILE INFORMATION TECHNOLOGY DEVELOPMENT

1.1. Basics of radio wireless communication technology

1.1.1. Features of the electromagnetic waves use for communication

Consider main characteristics of radio propagation, such as multiple access techniques, some signal modulation mechanisms as well as error control mechanisms. A familiarity with all these basic principles of wireless transmission is vitally important for understanding the questions participate the design of wireless networks.

It's common knowledge that all wireless communication directly depends on the principle of broadcast as well as electromagnetic waves reception. These waves can be described by either their wavelength (λ) or their frequency (f). Frequency is determined as the wave oscillations number per one second. It is measured, of course, in Hertz. In turn, wavelength is the distance between 2 consecutive maxima or minima in this wave. Also known the fact, the speed (c) of these waves propagation changes from medium to medium. There is exception their propagation in a vacuum where any electromagnetic waves move at the same speed (it is light speed). The well-known relation between the above parameters can be given as

$$c = \lambda \times f \tag{1.1}$$

where c is well-known light speed (3×10^8 *m/s*), f is the wave frequency, and λ is its wavelength [1].

The low-frequency bands are made up of the microwave, radio-, infrared, as well as visible light portions of the spectrum. They can be applied for information transmission with the help of modulating such wave's parameters as amplitude, frequency, or phase. Actually high-frequency waves including X-rays and Gamma rays, though theoretically considerably

better for information propagation. The lasts are not used because of practical considerations including the some complication to modulate or generate such waves, and the considerable harm they could cause to many living things.

Given that the electromagnetic spectrum is common resource and it is open for access by any person, numerous national and international agreements were concluded concerning utilization of the different frequency bands within certain spectrum. The individual national governments allocate certain spectrum for applications including TV broadcasting, AM/FM radio broadcasting, mobile telephony, different military communication, as well as government utilization. Global, an agency of the International Telecommunications Union Radiocommunication (ITU-R) Bureau called World Administrative Radio Conference (WARC) tries to coordinate present spectrum allocation with the help of the different national governments, as a means toall communication devices that can work in several countries can be manufactured [1, 3]. Despite that, the recommendations of ITU-R are not binding on any government. Concerning present national spectrum allocation, even in case the government sets aside any portion of such spectrum for a particular application/use (such as cellular telephony), another problem turns up – the problem of which company is to use which range of existing frequencies. Many different techniques have been tested for this frequency allocation among several competing carriers.

It’s common knowledge that radio waves generally experience some propagation mechanisms, such as scattering, diffraction and also reflection:

– Scattering: Well-know, that if waves move through a medium, which contains many different objects with dimensions small in comparison with its wavelength, scattering occurs. It is well known that wave gets scattered into numerous weaker outgoing signals. In practice, some objects including lamp posts, different street signs, and also foliage cause scattering.

– Diffraction: Such propagation effect is undergone by any wave when it hits some impenetrable object. Then wave bends at edges of this object, so that propagating in different directions. This phenomenon is also known as diffraction.

Note that the dimensions of the diffracting object can be compared to the diffracted wavelength. The bending causes the wave to reach places behind the object which cannot

normally be reached with the help of the line-of- sight transmission. Remember that amount of diffraction is always frequency-dependent and lower frequency waves diffracting more.

– Reflection: When the propagating radio wave hits an object which is huge in comparison with its wavelength (including tall buildings and surface of the Earth), the wave gets reflected by that object. Then reflection causes a phase shift (equal to 180°) between incident and the reflected rays [2].

Fig. 1.1 represents the different propagation mechanisms which radio wave encounters.

In the case transmitted wave is received at receiver, and received signal power is usually lower than the power with which it was transmitted. The total loss in the signal strength (attenuation) is because of numerous previously mentioned factors.

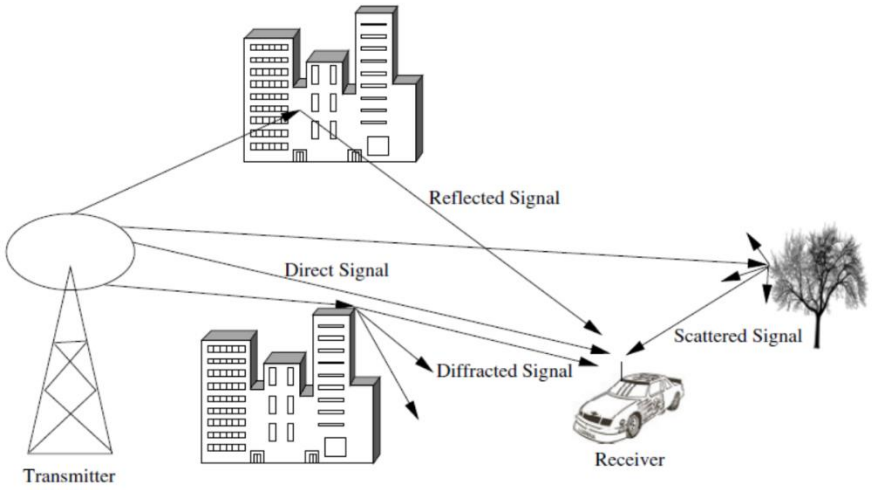


Fig. 1.1. Propagation mechanisms

1.1.2. General characteristics of the wireless channel

The wireless channel (namely transmission medium) is susceptible to many transmission impediments including path loss, interference, and signal blockage. All these factors considerably forbid data rate, real range, as well as the wireless transmission reliability. The degree of influence of these factors on transmission relies on really environmental conditions and the mobility of any receiver and transmitter. Generally, the transmitted signals have a direct-path component between pair transmitter and receiver.

Other components of the transmitted signal well known as multipath components are reflected, diffracted, along with scattered in the surrounding medium, and arrive at the receiver already shifted in amplitude, frequency, as well as phase relative to the direct-path component. In the next, we consider different characteristics of existing wireless channel including fading, path loss, interference, as well as Doppler shift. Actually 2 key limitations, Nyquist's along with Shannon's theorems are presented. They govern the ability to transmit some information at different data rates.

Any path loss may be expressed as the ratio of the real transmitted signal power to the power of the same signal received with the help of the receiver, on given path. This is a propagation distance function. Evaluation of path loss is extremely important for designing along with deploying wireless communication networks. It is well known that path loss is dependent on a number of factors including the radio frequency used plus the nature of the terrain. Given that numerous of these factors (namely the terrain) cannot be the same everywhere, and also single model may not be enough. So they cannot be used for describing main characteristics of every transmission. For this reason, in designing up-to-date network, numerous models are required to describe all variety of possible transmission environments.

Let's note that *free space* propagation model is the most simpl path loss model with existing direct-path signal between pair receiver and transmitter. Here there is no atmospheric attenuation as well as multipath components. In such model known relation between given transmitted power *Pt* and the received power *Pr* is given by: [1]

$$P_r = P_t G_t Gr \left(\frac{\lambda}{4\pi d}\right)^2 \tag{1.2}$$

where G_t along with G_r are respectively transmitter and receiver antenna gains, in the direction from one transmitter to one receiver, d is known distance between pair transmitter and receiver, and λ is actually signal wavelength. But realistic path loss models which take into account all propagation effects in specific environments can be obtained with the help of solving Maxwell's equations [3]. Given that obtaining solutions for this model includes complex algorithms and many computation intensive operations. Note that several simpler models have been proposed to represent existing loss.

Interference. Existing wireless transmissions have to withstand interference from quite wide variety of sources.

There are 2 main forms of interference: co-channel interference plus adjacent channel interference. In the last case, signals in nearby frequencies have some components outside their allocated ranges. Thus, all these components may interfere with current transmissions on adjacent frequencies. Note, that it can be avoided with the help of carefully inserting guard bands between all allocated frequency ranges. In the case of co-channel interference (sometimes also concerning as narrow-band interference) we have nearby systems (namely AM/FM broadcast) using the same transmission frequency [2].

Note, that narrow-band interference because of frequency reuse in present cellular systems can be significantly minimized using 3 directional antennas, special multiuser detection mechanisms, and also dynamic channel allocation techniques. Another interference type is inter-symbol interference. Here distortion in the received signal is effected by temporal spreading or consequent superimposition of individual pulses in the signal. If this temporal spreading of individual pulses (it is delay spread) exceeds a certain limit (it is symbol detection time), then receiver becomes unable to accurately distinguish any changes of state in the signal. So, the bit pattern interpreted with the help of a receiver is not the same as that sent with the help of a sender. Let's note that adaptive equalization is a generally used technique for existing combating inter-symbol interference. Today adaptive equalization includes several mechanisms for gathering all dispersed symbol energy into its original time interval. Existing complex digital processing algorithms are also applied in the equalization process. The most important principle behind adaptive equalization is the evaluation of channel pulse response to the periodically transmitted known bit patterns. And it is so called training sequences.

Fading speaks about some fluctuations in signal strength when it received at the receiver. Now fading can be classified into. They are fast fading/small-scale fading, and slow fading/big-scale fading.

Fast fading speaks about the rapid fluctuations in the amplitude, phase, or multipath delays of the received signal, because of the interference between several versions (or copies) of one and same transmitted signal arriving at any receiver at slightly different times.

Let's note that time between real reception of the first signal version and the last echoed signal is called the *delay spread*. The multipath propagation of the transmitted signal, causing quite rapid fading, is because of 3 previously mentioned propagation mechanisms. In fact, a signal that has multiple signal paths can sometimes combine constructively or sometimes destructively at this receiver, causing some change in the received signal power leve. It is well known that received signal envelope of rapidly fading signal is said to follow a Rayleigh distribution. But in the case there is no line-of-sight path between the transmitter and the receiver (usually applicable in outdoor environments), along with a Ricean distribution if one such path is available (usually characterizes, as a rule, indoor settings) [2].

The main goal of most wireless networks (WN) in present today is to support all voice communication. If only data signal consisting of binary digits is to be transmitted, then bits to be transmitted can be used directly to modulate necessary carrier signal to be used for further transmission. Commonly such process is not so direct in respect of analog voice signals. Here voice coding process converts necessary analog information into its equivalent digital form. The analog speech signal to be transmitted is first converted into proper digital pulses sequence. Then signal must be transmitted without any perceivable distortion. Well-known, that devices performing such analog to digital conversion (namely at the sender) along with the reverse digital to analog signal conversion (namely at the receiver) are known as *codecs* (coder plus decoder). Actually the central point of a codec is to convert necessary voice signal into digital bit stream with lowest possible bit rate. At the same time, we need to maintain acceptable quality level for signal. Also, it should be possible to properly reproduce the original analog speech information at the receiver without any noticeable distortion or disturbances. Pulse position modulation (PPM) is one of existing techniques which can be used for converting back analog signal into its digital form. In PPM, the amplitude along with pulse width remains constant. PPM requires constant transmitter power. Considering this all pulses will have the same constant amplitude and duration. PPM is applied generally in the infrared physical layer specification of the document IEEE 802.11. The central disadvantage of PPM is that perfect synchronization is required between

the pair transmitter and receiver. Pulse code modulation is another technique which is generally used for conversion of an analog signal into its corresponding digital form.

Note, that on any transmission channel, and particularly on the wireless channel, it is never guaranteed that all transmitted data will be delivered without any noticeable errors at the end point. So we always have non-zero probability that the bit stream gets altered during transmission. Let's note that bit error rates (BERs is bits fraction that are received in error) for the wired channel and the wireless one can be respectively 10^{-9} and 10^{-4}. The unreliable nature of all wireless channels makes error control even more critical in the WNs context.

Actually now numerous coding techniques are available. They try to provide necessary resistance against errors by adding redundant bits to some transmitted bits. So these redundant bits help the receiver detecting errors or request a retransmission (namely error detection). Also it helps to identify and next correct the faulty bits (namely error correction). We have various coding schemes for error detection as well as for error correction. Generally process of adding the redundant bits to existing bit stream is known as channel coding.

1.2. Network technologies of data exchange

1.2.1. Computer networks

Basics of wireless communication technology, now let’s appropriate to know how WNs operate. But before we delve into the WNs specifics, it would be good to understand the main principles of general computer network. All computer networks interconnect autonomous computers/nodes. Well-known, that computer networks are almost indispensable in today’s world. And they have become vitally important for our day-to-day life and also are used for very wide range of applications.

Generally all computer networks can be classified under 2 basic categories: peer-to-peer and client/server networks. Let's note that last type of network includes client and server processes, which usually located on various machines. The client processes always request and receive services from the server processes. Note, that such client/server model is very widely used for sharing different resources including files, printers, and so on. For example,

a Web server may be a server process receiving requests for any Web pages from Web browsers (namely client processes) running on various machines, and sending them back the required Web pages. Other popular applications including electronic mail clients and file transfer session clients (namely FTP clients) follow the client/server model too. A peer-to-peer network, as an alternative, doesn't need any dedicated server. So every computer on such network type can share its resources (such as files or printers) with any other computer on this network. Note that this is only if computers have been granted sufficient access privileges. In essence, every computer connected to the network is a client as well as a server.

Built on the transmission technology used, existing networks can be classified under 2 broad categories, in particular, point-to-point and broadcast networks. The last one now uses a single shared communication channel. Any message transmitted with the help of a node can be quite heard by all other nodes in this network. The other nodes simply ignore this message. Actually broadcast network is mainly used to connect machines within a small geographic area. Data transmitted with the help of the source node can be received only using intended next hop receiver node. For this reason, the transmitted data might have to traverse through several hops as a means toreach the final destination. Such point-to-point links are used to connect machines that are physically separated with the help of large geographic distances. Built on the geographic span of the network, all networks can be classified as LANs, MANs, as well as WANs.

1.2.2. Bluetooth technology

Generally WLAN technology enables device connectivity to infrastructure-based services via any wireless carrier provider. Despite that, the need for personal devices to communicate wirelessly with each other, without an established infrastructure has led to the emergence of the personal area networks (PANs). And first attempt to determine a standard for existing PANs dates back to Ericsson’s Bluetooth project 2 (1994) to enable communication between mobile phones by low-power along with low-cost radio interfaces. In 1998, numerous companies including such company Nokia, IBM, Intel, and Toshiba joined Ericsson to form so called Bluetooth Special Interest Group (SIG). They goal was to

develop a *de facto* standard for PANs. Now, IEEE has approved a Bluetoothbased standard (document IEEE 802.15.1) for present wireless personal area networks (WPANs). The current standard covers only the MAC along with the physical layers while the Bluetooth specification details the all protocol stack. Pay your attention that Bluetooth uses radio frequency (RF) technology for communication. It uses frequency modulation method to generate radio waves in the ISM band [1-3].

Let's note that very low power consumption of Bluetooth technology and an offered range of up to 10 meters have paved the way for numerous utilization models. One can have an interactive conference by setting up up-to-date laptops ad-hoc network. Cordless computer, instant postcard [they send digital photographs instantly (usually camera is cordlessly connected to a mobile phone)]. Also it may be three-in-one phone are other indicative utilization models. Three-in-one phone has similar phone functions as cordless phone (usually at home, a fixed-line charge), intercom (usually at the office with no telephone charge), and mobile phone.

Bluetooth security. In all present Bluetooth communications or devices may be authenticated and next links may be encrypted. The authentication of devices is performed with the help of a challenge-response mechanism. It directly depends on a commonly shared secret link key created through special user-provided personal identification number (PIN). Actually authentication begins with the transmission of an LMP challenge packet along with ends with the verification of result returned by the claimant. At choice, any link between them can be encrypted too.

Generally Bluetooth is the first known wireless technology. It has actually tried to make all existing household consumer electronics devices follow one specific particular communication paradigm. This has been partially successful, but it does have specific limitations.

Let's note that bluetooth communication now does not provide any support for routing. Pay your attention that some research is being done to address this in the Bluetooth specification. Once the routing is provided, inter-piconet communication could be really enhanced. The question of handoffs has not yet been dealt with till nowadays. Nevertheless master–slave architecture has aided cheap, the master becomes so called bottleneck for all

existing piconet in terms of fault tolerance, performance, as well as bandwidth utilization. Note that, Bluetooth communication using same frequency band as that of WLAN and therefore robust coexistence solutions must be developed to avoid existing interference (but it is still under development). Now, there are nearly 1,800 adopter companies that are contributing to development of such technology.

1.3. Comparative analysis of wireless networks technologies - ad-Hoc and cellular

1.3.1. Features of wireless ad-Hoc networks

The idea of developing the creation of a-Hoc wireless technology arose from the principle of Packet Radio Network (PRNET).

PRNET was a set of early, only experimental mobile ad-hoc networks. Their technologies developed with time. It was funded with the help of Advanced Research Projects Agency (ARPA). Primary participants in this project involved Hazeltine Corporation, BBN Technologies, as well as SRI International.

Generally successful demonstrations of PRNET technology proved the feasibility and effectiveness of infrastructureless networks as well as their applications for different military or civilian purposes. Next DARPA extended the work on multi-hop WNs via the survivable radio networks (SURAN). This project intended for providing up-to-date ad-hoc networking with low both cost and power devices which have efficient protocols and also significantly improved scalability or survivability (usually it is ability of network to survive in the event of failure of network links and nodes).

During the 1980s, significant amount of research into military applications was heavily funded across the globe. Realizing the necessity to have open standards in this emerging field of computer communication, a working group within the Internet Engineering Task Force (IETF), was called the mobile ad-hoc networks (MANET) working group [1]. It was formed for standardizing different protocols and functional specifications of ad-hoc WNs.

Also at 1994, the Swedish communication equipment manufacturer Ericsson have proposed to develop short-range, low-power and low-complexity as well as budget radio interface and also associated communication protocols concerning as *Bluetooth* for all ubiquitous connectivity between existing heterogeneous devices. This effort was later taken over with the help of a Special Interest Group (SIG) formed by numerous primary computer and telecommunication vendors including 3Com, IBM, Ericsson, Intel, Motorola, Microsoft, Nokia, and so on. Actually Bluetooth SIG aims at providing one universal solution for connecting heterogeneous devices. This is one of the first existing commercial realizations of up-to-date ad-hoc WNing. Also bluetooth standardizes point-to-point single-hop wireless link to help in exchanging data and voice. Also it helps to form opiconets which are formed by nodes group in a smaller geographical region (in case when every node can reach every other node in this group within one single-hop).

Even though ad-hoc WNs are expected to operate in the absence of any fixed infrastructure, latest advances in WN architectures reveal quite interesting solutions. They allow any mobile ad-hoc nodes to operate in the presence of infrastructure. Generally multi-hop cellular networks (MCNs) and self-organizing packet up-to-date radio ad-hoc WNs with overlay (SOPRANO) may be examples of such networks types. Such hybrid architectures (usually it combines the all benefits of cellular and ad-hoc WNs) significantly improve the capacity of the system significantly.

1.3.2. Up-to-date cellular and ad-hoc wireless networks

Fig. 1.2 illustrates a representation of various WNs. The current cellular WNs (Fig. 1.2) are usually classified as the infrastructure dependent networks. The path setup for a call between 2 nodes, for example, node *C* to node *E*, is completed through the base station (BS) as showed in Fig. 1.3.

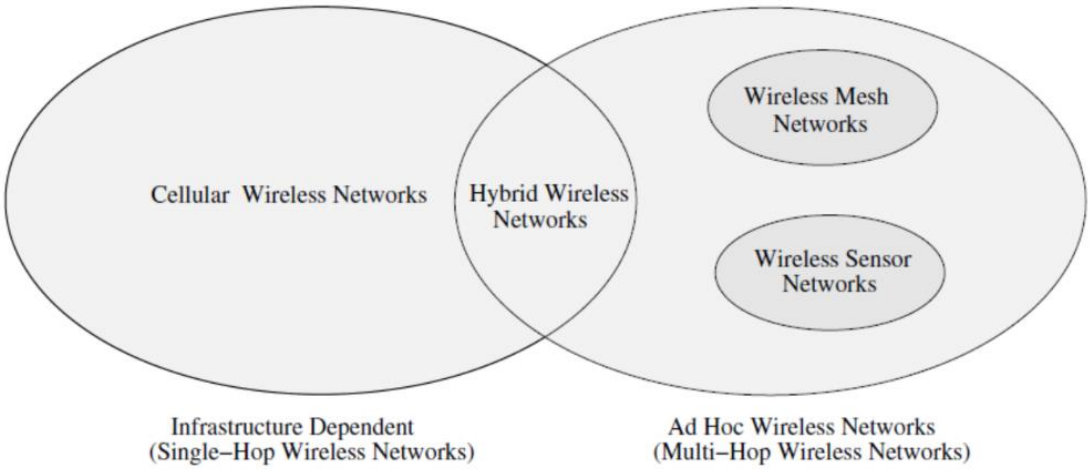


Fig. 1.2. Cellular and ad-hoc wireless networks

Let's note that ad-hoc WNs are determined as the category of WNs that utilize multi-hop radio relaying are able to work without any support of fixed infrastructure (therefore they are sometimes called infrastructureless networks). The absence of any BS or central coordinator makes the routing quite complex one in comparison with cellular networks.

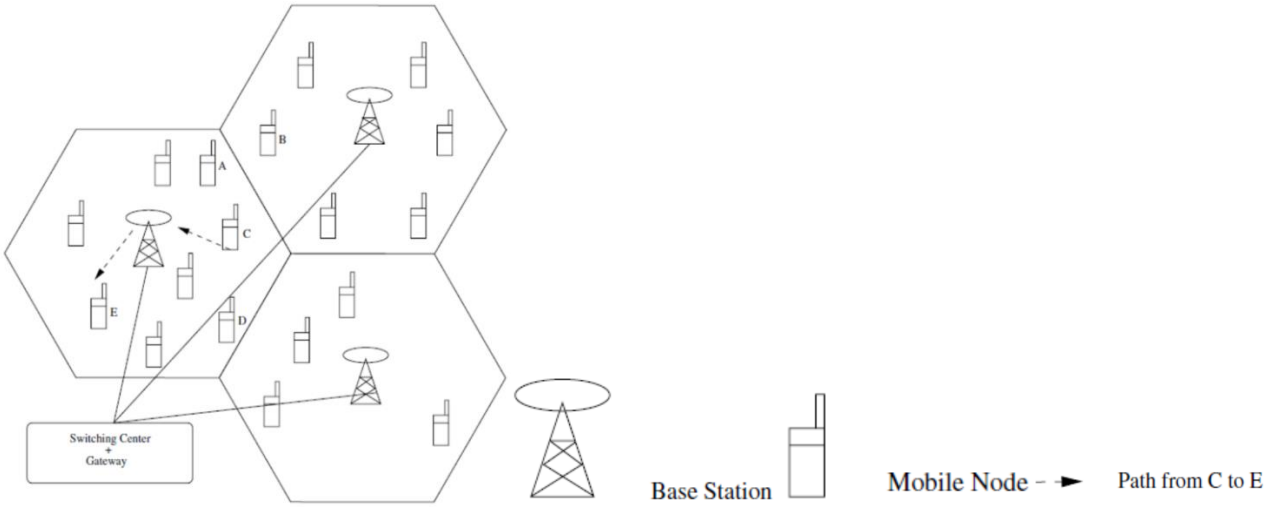


Fig. 1.3. A cellular network

Ad-hoc WN topology for modern cellular network is shown in Fig. 1.3 as well as in Fig. 1.4. Pay attention to that in Fig. 1.4 the cell boundaries are shown only for comparison with cellular network in Fig. 1.3. So it does not carry any special significance. In this case path setup for a call between 2 nodes, (here is node *C* to node *E*), is completed via the intermediate mobile node *F*, as showed in Fig. 1.4. Actually wireless mesh networks and

also wireless sensor networks are specific examples of up-to-date ad-hoc WNs. The primary differences between cellular networks and ad-hoc WNs are summarized in Table 1.1. Generally presence of base stations significantly simplifies routing and resource management in any cellular network since routing decisions are made in a centralized manner with additional information about some destination node. But in up-to-date ad-hoc WN, the resource management and routing are done in a distributed way in which all nodes coordinate to ensure communication between them. This requires that each node to be more intelligent as a means to it can operate both as a network host for receiving and transmitting data as well as network router for routing certain packets from other nodes. Therefore the mobile nodes in ad-hoc WNs are significantly more complex than their counterparts in other mobile networks.

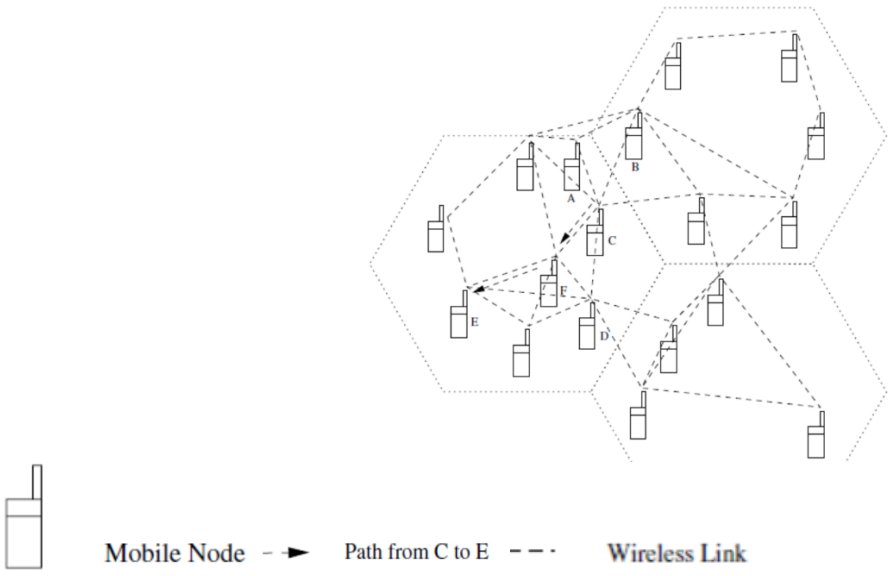


Fig. 1.4. An ad-hoc wireless network

1.3.3. Applications of ad-hoc wireless networks

Let's note that ad-hoc WNs, because of their quick and cost-effectively less deployment, find applications in numerous areas. Some of these involve, for example different military applications, distributed or collaborative computing, certain emergency operations, wireless mesh and sensor networks, as well as hybrid WN architectures.

Table 1.1.

Differences between cellular networks and ad-hoc wireless networks

Cellular Networks	Ad Hoc Wireless Networks
Fixed infrastructure-based	Infrastructure-less
Single-hop wireless links	Multi-hop wireless links
Guaranteed bandwidth (designed for voice traffic)	Shared radio channel (more suitable for best-effort data traffic)
Centralized routing	Distributed routing
Circuit-switched (evolving toward packet switching)	Packet-switched (evolving toward emulation of circuit switching)
Seamless connectivity (low call drops during handoffs)	Frequent path breaks due to mobility
High cost and time of deployment	Quick and cost-effective deployment
Reuse of frequency spectrum through geographical channel reuse	Dynamic frequency reuse based on carrier sense mechanism
Easier to achieve time synchronization	Time synchronization is difficult and consumes bandwidth
Easier to employ bandwidth reservation	Bandwidth reservation requires complex medium access control protocols
Application domains include mainly civilian and commercial sectors	Application domains include battlefields, emergency search and rescue operations, and collaborative computing
High cost of network maintenance (backup power source, staffing, etc.)	Self-organization and maintenance properties are built into the network
Mobile hosts are of relatively low complexity	Mobile hosts require more intelligence (should have a transceiver as well as routing/switching capability)
Major goals of routing and call admission are to maximize the call acceptance ratio and minimize the call drop ratio	Main aim of routing is to find paths with minimum overhead and also quick reconfiguration of broken paths
Widely deployed and currently in the third generation of evolution	Several issues are to be addressed for successful commercial deployment even though widespread use exists in defense

Military applications. Now ad-hoc WNs can be extremely useful in setting up communication for a group of soldiers during tactical operations. Establishing any fixed infrastructure for communication between some soldiers group in enemy territories may not be possible. So in such environments, ad-hoc WNs provide the required communication mechanism quickly enough. Another application is its coordination of different military objects moving at high speeds including warships and airplanes. Actually such applications require quick along with reliable communication.

Generally secure communication is very important because eavesdropping or other existing security threats can compromise the communication objective or the safety of personnel participates in these operations. They also need the support for reliable and secure multimedia multicasting. For instance, the leader may want to give some order to all soldiers or to only set of chosen personnel participate in such operation. For this reason, the routing protocol should be able to provide secure, fast enough, as well as reliable multicast communication with real-time traffic support. This is especially relevant now in Ukraine.

Since military applications require extremely secure communication at any cost, the vehicle-mounted nodes can be considered extremely powerful and complex. They can have several high-power transceivers, each have ability to hop between various frequencies for security reasons. It can be assumed that such communication systems are equipped with long-life batteries which may not be economically advantageous for normal exploitation. They can even apply other services including location tracking or other satellite-based services for effective communication along with coordination. Let's note that resource limitations including battery life and transmitting power may not exist in certain types of applications of up-to-date ad-hoc WNs. For instance, the ad-hoc WN formed with the help of a military tanks may not suffer from the power source limitations present in the ad-hoc network. They are formed by a set of different wearable devices applied by the foot soldiers.

Collaborative and Distributed Computing. Another domain where ad-hoc WNs now can find applications is collaborative computing. All requirements of any temporary communication infrastructure for fast communication with minimal configuration between a group of individuals during a conference and meeting require the formation of an ad hoc.

For instance, consider some group of researchers who want to share their presentation materials at a conference, or a lecturer distributing special notes to the class on the fly. In this case, the formation of an ad-hoc WN with the necessary support for reliable multicast routing can serve such purpose. Other applications including streaming of multimedia objects between participating nodes in an ad-hoc WN may require support for so called soft real-time communication. Actually all users of such applications prefer cost-effective and also portable devices, as a rule powered by battery sources. For this reason, a mobile node can drain its battery and may have different transmission power. This can result in

unidirectional connections to neighbors. Let's note that all devices applied for such typical applications could as a rule be laptops with add-on wireless interface cards, any mobile devices with high processing power and so on. In the presence of such heterogeneity, interoperability is very important task.

Emergency Operations. Ad-hoc WNs are extremely useful in emergency operations including search and rescue, commando operations, and so on. The primary factors that favor ad-hoc WNs for such tasks are self-configuration of any system with minimal cost, regardless of centralized or fixed infrastructure, mobility flexibility, the terrain nature of such applications, along with conventional communication infrastructure unavailability. Note, that in environments where any conventional infrastructure-based communication facilities have been destroyed because of a war or because of natural calamities including earthquakes, immediate deployment of up-to-date ad-hoc WNs would be very good solution for coordinating all rescue activities.

Given that the ad-hoc WNs require minimum initial network configuration for their functioning, extremely little or no delay is participates making the network fully operational. All above-mentioned scenarios are unexpected, in most cases unavoidable, and also could affect a large number of individuals. Actually ad-hoc WNs used in such circumstances must be distributed as well as scalable to a large number of nodes. They must also be able to special provide fault-tolerant communication paths.

Wireless mesh networks are ad-hoc WNs that are designed to provide alternate communication infrastructure for fixed or mobile nodes or users, without any spectrum reuse restrictions along with the network planning requirements of present cellular networks. The mesh topology for wireless mesh networks provides multiple alternate paths for data transfer session between a destination and a source. It is resulting in reasonably fast path reconfiguration when the existing path fails because of node failures. Up-to-date wireless mesh networks provide the most cost-effective data transfer option combined with the freedom of mobility [3]. Given that the infrastructure built is in the form of quite small radio relaying devices fixed on the buildings rooftops in a residential zone as shown in Fig. 1.4, or similar devices fitted on the lamp posts as represented in Fig. 1.5. Note, that necessary investment for wireless mesh networks is considerably less than what is necessary for

cellular network counterparts. These networks are formed with the help of placing wireless relaying equipment spread over the territory to be covered by the network.

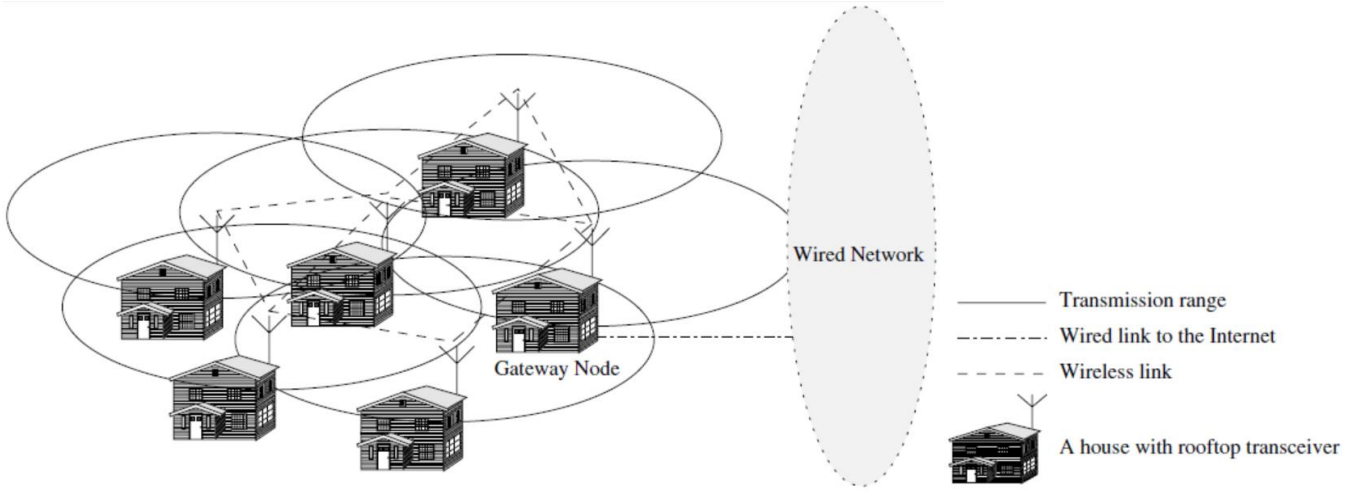


Fig. 1.5. Wireless mesh network operating in a residential zone

Let's note that possible deployment scenarios for wireless mesh networks involve: 1 - highways (facility of communication for all moving automobiles is needed), 2 - residential zones (connectivity of broadband Internet is needed), 3 - business zones (alternate communication system to cellular networks is needed), 4 - important civilian regions (very high degree of service availability is needed), along with university campuses (budget campus-wide network coverage can be provided). Actually wireless mesh networks must be capable maintenance and also self-organization. The ability of existing network to overcome failures of one or more node due to disasters makes it convenient for providing the communication infrastructure for all strategic applications.

The primary advantages of any wireless mesh networks are support for quite high data rate, quick and budget deployment, enhanced services, easy extendability, high availability and scalability, cheap per bit and so on [1]. Up-to-date wireless mesh networks as a rule operate at the license-free ISM bands around 2.4 GHz or 5 GHz. Depending on the technology which applied for the physical and MAC layers communication, data rates from 2 Mb/s upto 60 Mb/s can be supported. For instance, if document IEEE 802.11a is applied, a maximum data rate of 54 Mb/s can be supported. The deployment time that required for

such network is considerably less than that provided by other infrastructure-based networks. Partial batch and ncremental deployment also can be performed.

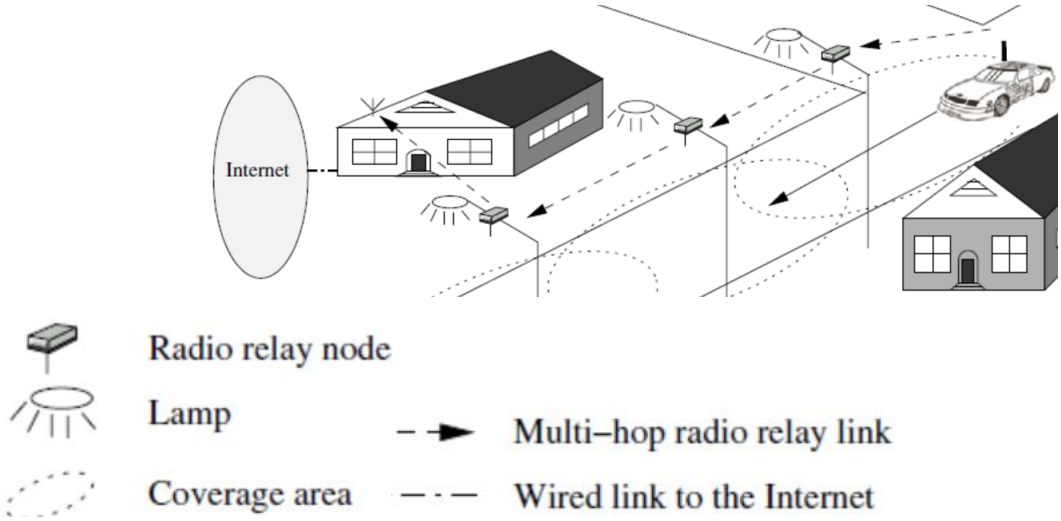


Fig. 1.6. Wireless mesh network covering a highway.

Existing wireless mesh networks provide very cost-effective communication infrastructure in terms of data transfer costs plus its deployment. Services including smart environments that can update information about the environment or locations to the visiting nodes are now possible in such an environment. Let's note that truck driver can use advanced location discovery services, and therefore spotting his location on an updated digital map is possible. Actually mesh networks scale well to provide support for large number of nodes. Even at extremely high density of mobile nodes, using power control at the relay and mobile nodes, support for a large number of users as well as better system throughput can be achieved. But in respect of cellular networks, all improving scalability requires only additional infrastructural nodes. They in turn include very high cost. As indicated previously, mesh networks provide possibility of expanding service in more cost-effective manner. Note that partial roll out and network commissioning as well as extending the service in a seamless way without any impacting the existing installation are the advantages from the viewpoint of many service providers. Generally wireless mesh networks provide huge availability in comparison with the existing cellular architecture, where the presence of a fixed BS that covers considerably larger area includes the risk of failure single point.

1.3.4. Wireless Sensor ma Hybrid Networks

Note, that sensor networks are a special category of up-to-date ad-hoc WNs that are applied to provide some wireless communication infrastructure between the sensors deployed in a specific application area. Latest achievements in WNs technology and recent research in ad-hoc WNs have made smart sensing a reality. Generally sensor nodes are tiny devices that have the capability of measuring some physical parameters, processing the collected data, and communicating via networks to the monitoring station. Actually sensor network represents as collection of quite large number of sensor nodes which are deployed in certain region. Probing activity can be irregular or periodic.

One example for the periodic type is this sensing of some environmental factors for parameters measurement including humidity, temperature, as well as nuclear radiation.

The question that make sensor networks a separate category of ad-hoc WNs are:

• **Size of the network:** Note that nodes number in typical sensor network can be considerably larger than that in any ad-hoc WN now.

• **Data/information fusion:** Existing limitation for power and bandwidth require aggregation of information and bits at the intermediate relay nodes which are responsible for relaying. Data fusion speaks about the aggregation of several packets into one before relaying it. It is mostly intended for reducing the bandwidth consumed with the help of redundant headers of the packets and also reducing the media access delay participates transmitting several packets. Such fusion is required to process the sensed data at the intermediate nodes (IN) and also relaying the outcome to special monitor node.

• **Mobility of nodes:** It is not a mandatory requirement in modern sensor networks. Despite that, the sensor nodes which are placed on the bodies of patients in a post-surgery hospital ward may be designed to support their limited mobility. Mostly, sensor networks do not necessarily in all cases be designed to support mobility of sensor nodes.

• **Density of deployment:** In a sensor network nodes density changes with the application scope. For instance, all military applications require higher network availability, thus making redundancy the highest priority.

• **Power limitations:** Now power limitations in typical sensor networks are considerably more stringent than those in any ad-hoc WNs. This is primarily because the all

sensor nodes are expected for operation in harsh geographical or environmental conditions, with no human or minimum maintenance plus supervision [1, 6]. The operation of the network (has nodes powered by battery source with quite limited energy) requires extremely effective protocols at network, physical layer, and also data link. Let's note that power sources applied in sensor networks now can be divided into such 3 categories:

– *Regenerative power source***:** In this case power sources have the ability to regenerate power from measured physical parameter. For instance, the sensor used to measure temperature at a power plant can apply power sources that can generate electricity using appropriate transducers.

– *Replenishable power source***:** In some sensor networks applications, usual power source may be replaced when the existing source is completely drained (such as wearable sensors that are applied to measure some body parameters).

– *Non-replenishable power source***:** In certain specific sensor networks applications, the power supply cannot be replenished after the network is deployed. The replacement of such sensor node is the only one possible solution (such as deploying sensor nodes in a remote, hazardous area).

• **Traffic distribution:** The communication traffic structure changes depending on application area of sensor networks. This type of traffic requires quite low bandwidth [1, 6]. Actually sensor network used to detect border intrusions in a military program generates traffic when certain events are detected; as a rule these events might have time limits for delivery.

Hybrid WNs. One of the main application areas of typical ad-hoc WNs is in hybrid wireless architectures including multi-hop cellular networks (MCNs) and also integrated cellular ad-hoc relay (iCAR) networks [1, 6]. The huge growth in the subscriber base of present cellular networks has reduced the cell size upto the pico-cell level.

Let's note that basic concept of cellular networks is geographical channel reuse. Different techniques including cell resizing or sectoring, and also multi-tier cells have been proposed to increase cellular networks capacity. Most of these schemes usually increase the cost of equipment. Generally real capacity of a cellular network can be significantly

increased if the network includes the multi-hop relaying capabilities along with the support of available fixed infrastructure [1, 6].

The MCN architecture is represented in Fig. 1.7. When 2 nodes in same cell want to communicate with each other, in this case connection is routed through several wireless hops via the INs.

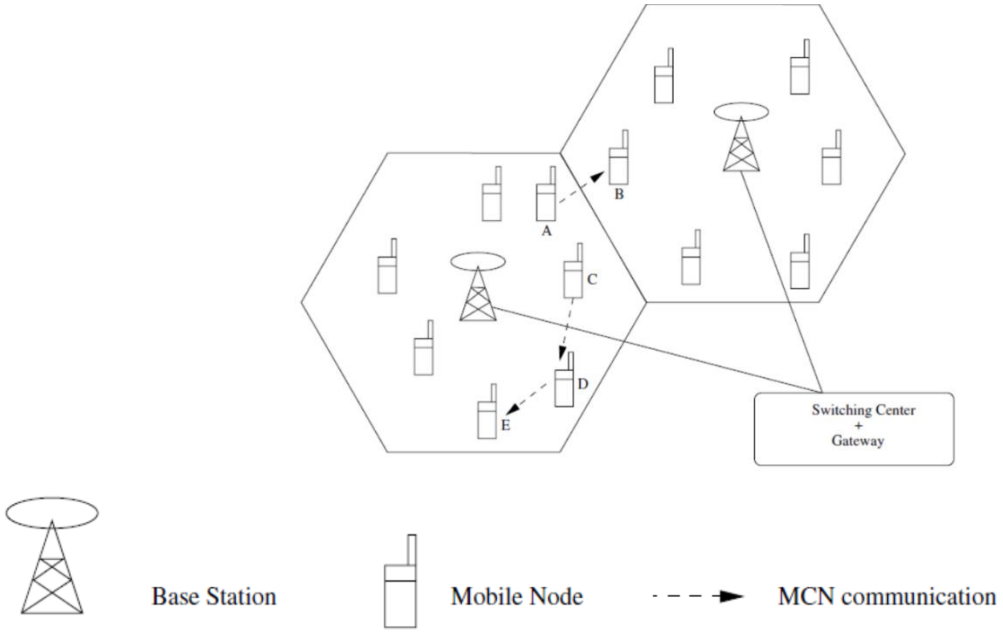


Fig. 1.7. MCN architecture.

Note, that BS maintains some information about the network topology for effective routing. Actually BS may or may not be participates this multi-hop path. Consider an example when node A wants to communicate with node B. In the case when all nodes are capable of operating in MCN mode, then node A can reach node B directly but if the node B is found within node A's transmission range. In the case when node C wants to communicate with node E and both are found in the same cell, node C can reach node E via node D. It acts as an intermediate relay node. Generally such hybrid WNs can provide quite high capacity resulting in lower cost of communication than provided by cellular networks.

The primary benefits of hybrid WNs are:

– It has increased reliability and flexibility in routing process. In this cace flexibility is the best suitable nodes for routing process. It is done via several mobile nodes or via base stations, or may be by combination of both.

– It has higher capacity compared with cellular networks obtained because of the better channel reuse provided with the help of transmission power reduction, since mobile nodes use a power range that is only fraction of the cell radius.

– It has much better coverage and connectivity in general (since areas that are not covered because of transmission difficulties including antenna coverage or the direction of antenna) of a cell can be provided with the help of several hops through INs in the cell.

1.4. AD-HOC wireless internet

Generally typical ad-hoc wireless Internet extends the Internet services to the end users via ad-hoc WN. Ad-hoc WN schematic diagram of is presented in Fig. 1.8.

Note that for successful ad-hoc wireless Internet the main questions to be considered are the following:

• **Address mobility:** Typical ad-hoc wireless Internet can also faces the problem of address mobility. And here it worse, since all nodes operate through several wireless hops. Solutions including Mobile IP can also provide temporary alternatives to this.

• **Gateways:** Its nodes in typical ad-hoc WN are the entry points to the wired Internet. The primary part of the service provision lies on all gateway nodes. Typically service provider-owned and managed gateways perform such tasks as bandwidth management, end-user tracking, and so on.

• **Routing:** Routing is a primary challenge in the ad-hoc WN, because of the gateways presence, the dynamic topological changes, multi-hop relaying, as well as the hybrid character of such network. One possible solution for this case is the usage of some separate routing protocol, for the wireless part of typical ad-hoc WN. Routing protocols are more suitable because they take advantage of the presence of gateway nodes.

• **Load balancing:** It’s likely that the ad-hoc WN gateways experience heavy traffic. Therefore the gateways can be saturated considerably much earlier than other nodes in this network. Load balancing methods are vitally important for load distribution to avoid the situation where the gateway nodes become so called bottleneck.

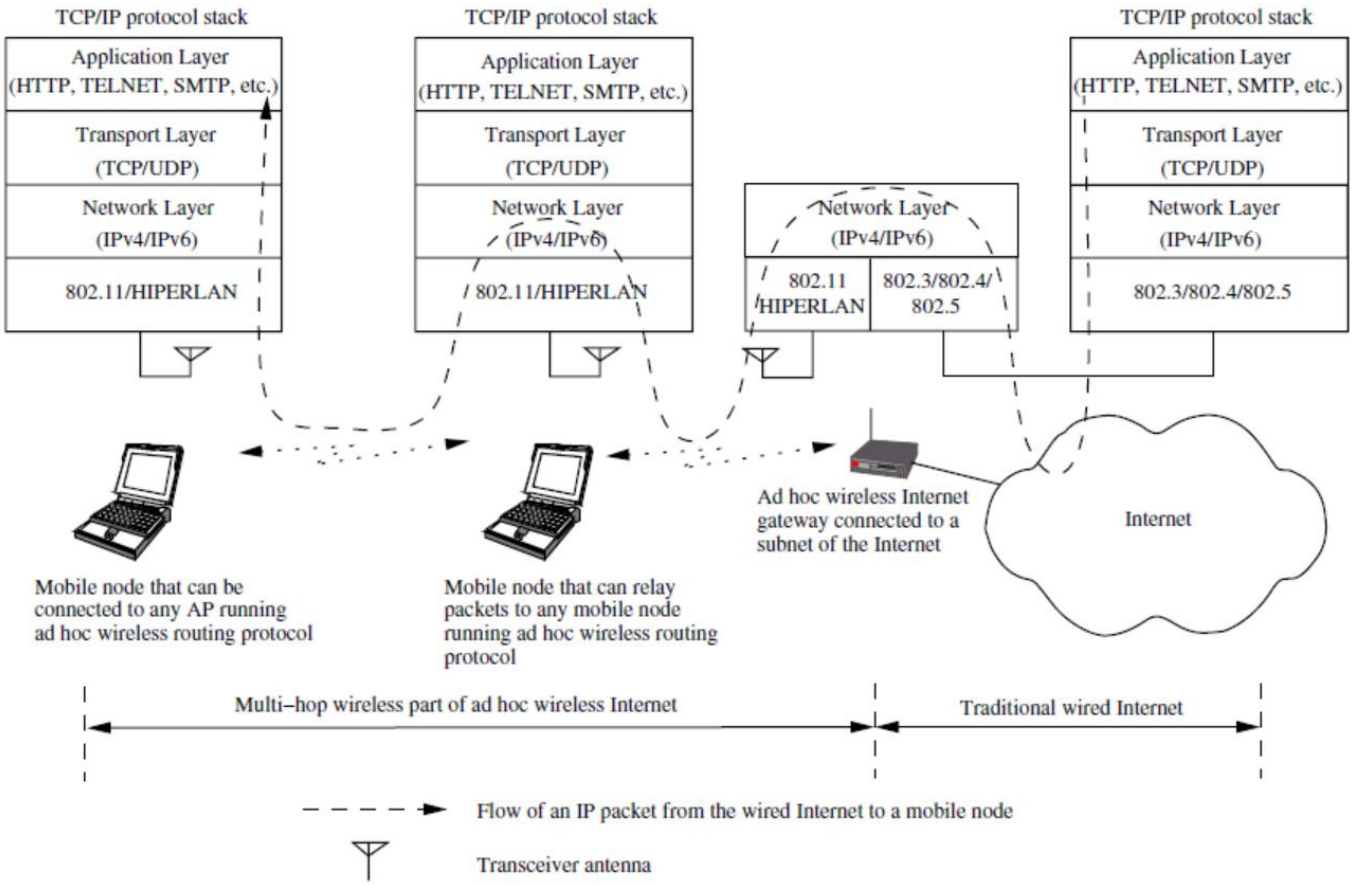


Fig. 1.8. A schematic diagram of the ad-hoc wireless Internet

• **Transport layer protocol:** Although there are numerous solutions for transport layer protocols for ad-hoc WNs, unlike other layers, possible choice lies in favor of TCP extensions proposed now for all ad-hoc WNs.

Split approaches that apply standard wired TCP for the wired part and also specialized transport layer protocol for typical ad-hoc WN part can be considered when the gateways act as the INs on which possible connections are split.

• **Provisioning of security:** Generally inherent broadcast nature of all wireless medium attracts not only the mobility seekers but also latent hackers. Therefore security is a key concern in the ad-hoc WN. Given that the end users can use the ad-hoc WN infrastructure to conduct e-commerce transactions, it is very important to involve security mechanisms in typical ad-hoc WN.

• **QoS support:** Note that with the widespread deployment of voice over IP (VoIP) and significant growing multimedia applications over the Internet, ensuring QoS support in

any ad-hoc WN becomes a very important task. As you know, this is a complex problem both in the wired part and in the wireless part.

• **Service, location and address discovery:** Service discovery in present networks speak about the activity to identify the party that provides a particular resource or service. The location discovery speaks about various activities including detecting the location of particular mobile node in the network. Address discovery speaks about the services including those provided with the help of address resolution protocol (ARP) or typical domain name service (DNS) operating within the wireless area.

Fig. 1.9 illustrates a wireless mesh network that connects numerous houses to the Internet via gateway node.

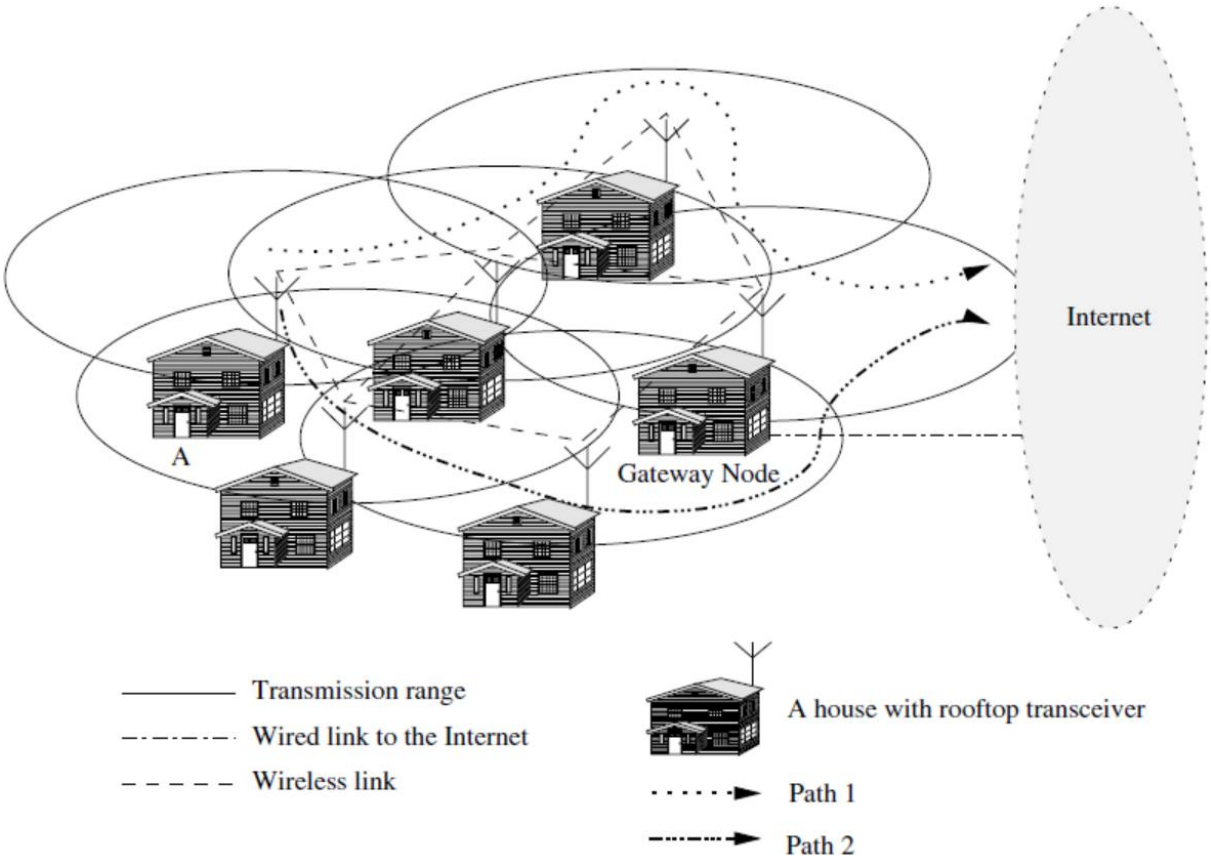


Fig. 1.9. An illustration of the ad-hoc Internet implemented by a wireless mesh network

Let's note that such networks can provide quite reliable broadband WNs for the urban and also for rural population in a cost-effective way with fast deployment and reconfiguration. Actually this wireless mesh network is a special case of typical ad-hoc WN

where mobility of some nodes is not a primary concern because most relay stations and end users appy fixed transceivers.

CONCLUSION TO CHAPTER 1

In this chapter, the primary questions as well as using ad-hoc WNs were described.

Different applications of ad-hoc WN have been analyzed. Also we studied different applications, such as military distributed or collaborative computing, emergency operations, wireless mesh and sensor network and so on.

Comparative analysis of wireless networks technologies (ad-hoc and cellular) have been carried out. The design question for every layer of protocol stack and deployment scenarios were discussed. Actually applications of ad-hoc WNs involve collaborative or distributed computing, various military applications, emergency operations, as well as different hybrid wireless architectures. The most important deployment question for ad-hoc WNs are scenario of deployment, required longevity of network, necessary coverage area, necessary service availability, operational integration with other infrastructure, as well as choice of necessary protocols.

CHAPTER 2
ISSUES IN AD-HOC WIRELESS NETWORKS

2.1. Basic technological question in AD-HOC wireless networks

Here we consider the some challenges and question that must be taken into account when designing ad-hoc wireless system. Moreover deployment considerations for installation, futher operation as well as maintenance of ad-hoc WNs are presented too. Consider the main question that influence on ad-hoc wireless system design, deployment, and also performance. They are [8]:

- System scalability;
- Addressing as well as service discovery;
- Routing;
- Transport layer protocol;
- Self-organization;
- Necessary medium access scheme;
- Multicasting and pricing scheme;
- Quality of service for networks and its security;
- Energy management and deployment considerations.

Medium access scheme. The essential responsibility of any medium access control (MAC) protocol in existing now ad-hoc WNs is, as you know, the distributed arbitration for the shared channel of a packets transmission. Today performance of any WN depends on the MAC protocol, especially for existing ad-hoc WNs. Consider main question in designing a MAC protocol for ad-hoc WNs. They are:

• **Access delay:** Such delay with regard to the network average delay that any packet experiences to get transmitted. The MAC protocol must try to minimize this delay.

• **Exposed terminals:** For instance, the nodes those are within the sender transmission range of current session. They are prevented from making necessary transmission. As a means to significantly improve the effectiveness of the MAC protocol, so exposed nodes

must be allowed to transmit in a controlled manner without causing any collision to the on-going data transfer.

• **Network synchronization:** Generally MAC protocol design should bear in mind the current requirement of time synchronization. As a rule, synchronization is required for all TDMA-based systems for management of transmission and reception slots. Synchronization includes utilisationof scarce resources including bandwidth and battery power. The control packets appid for synchronization may significantly magnify collisions in such network.

• **Distributed operation:** Typical ad-hoc WNs need to operate in medium where no centralized coordination is possible. Actually MAC protocol design must be fully distributed with minimum control cost. Dealing with the subject of polling-based MAC protocols, note that partial coordination is required.

• **Hidden terminals:** They are nodes that are hidden (or currently not reachable) from the sender of any data transmission session. But they are available to the session receiver. In such situation, the hidden terminal may result in collisions at any receiver node. Note that presence of hidden terminals can significantly decrease the capacity of a MAC protocol used in all ad-hoc WNs. Hence the MAC protocol should be able to alleviate the effects of hidden terminals.

• **Capacity:** The MAC protocol used in all ad-hoc WNs should attempt to maximize the capacity of the system. The important considerations for capacity enhancement are minimizing the appearance of collisions, maximizing channel usage, and minimizing control cost.

• **Fairness:** It applies to the ability of the MAC protocol to provide weighted or equal share for present bandwidth to all competing nodes. As a rule, former tries to provide an equal share of bandwidth for competing nodes, while the latter provides an equal share only for competing data transfer sessions. In typical ad-hoc WNs, fairness is important because of the multi-hop relaying done with the help of the nodes. An unfair relaying load for a node leads to draining the resources of that node considerably faster than that of other nodes.

• **Real-time traffic support:** Generally in a contention-based channel access medium, without any central coordination, with quite limited bandwidth, and also with location-

dependent contention, with support of time-sensitive traffic including video, voice, and real-time data need explicit support from the MAC protocol.

• **Ability to measure resource availability:** As a means to withstand the resources including bandwidth effectively and also perform call admission control built on their availability, the MAC protocol must be able to provide an evaluation of resource availability on each node. It can also be applied for making congestion-control decisions.

• **Resource reservation:** QoS provisioning determined by necessary parameters just for delay, bandwidth, and also jitter requires reservation of resources including bandwidth, necessary buffer space, and processing power. Here MAC protocol must be able to provide mechanisms to support necessary resource reservation and QoS provisioning.

• **Capability for power control:** Generally transmission power control can decrease the energy consumption at the nodes. It causes sufficiently reduce in interference at neighboring nodes, and also magnifys frequency reuse. Actually support for power control at the MAC layer is extremely important in the ad-hoc wireless medium.

• **Adaptive rate control:** This speaks about change in the data bit rate achieved by the channel. A MAC protocol with adaptive rate control can apply sufficiently high data rate when the receiver and sender are close to each other and they adaptively decrease the data rate if they move away from each other [4].

Routing protocol responsibilities as a rule involve exchanging the route information; finding a possible path to a destination built on criteria including minimum power required, hop length, and also of wireless link lifetime. It is collection of information about the path breaks; as well as utilizing minimum bandwidth. The main issues that any routing protocol faces are:

– **Bandwidth constraint:** Given that the channel is shared by all present nodes in the broadcast region. The bandwidth available for all wireless links depend on the number of nodes and available traffic they handle. Therefore just a fraction of existing total bandwidth is available for each node.

– **Mobility:** One of the main attributes of all up-to-day ad-hoc WNs is the mobility associated with the nodes. Node mobility leads to frequent path breaks, trite routing

information, possible transient loops, and some complication in resource reservation. As a general rule, good routing protocol should effectively solve all the above questions.

– **Error-prone and shared channel:** The bit error rate (BER) in any wireless channel is extremely high (from 10^{-5} upto 10^{-3}) as opposed to that in its wired counterparts (from 10^{-12} upto 10^{-9}). Present routing protocols designed for ad-hoc WNs should take this data into account. Actually consideration of the wireless link state, real signal-to-noise ratio, and path loss for routing in ad-hoc WNs can significantly improve the effectiveness of the routing protocol.

– **Route acquisition delay** for any node that does not have a route to a particular destination node should be minimized. Such delay may vary depending on network size and the network load.

– **Quick route reconfiguration:** All unpredictable changes in the present network topology as a rule require that the routing protocol be able to rapidly perform route reconfiguration as a means to withstand path breaks and also subsequent packet losses.

– **Loop-free routing:** It is basic requirement for all routing protocol to avoid unnecessary wastage of network bandwidth. In ad-hoc WNs, because of the random nodes movement, present transient loops may form route established in this way. Known, that routing protocol must detect all transient routing loops and take necessary corrective actions.

– **Distributed routing approach:** Generally ad-hoc WN is a fully distributed WN and apply centralized routing approaches in such network may consume quite large amount of bandwidth.

– **Scalability:** It is the ability of any routing protocol to scale well (or perform effectively) in a network with quite large number of nodes. This requires real minimization of control costs and quick adaptation of the routing protocol to real network size.

– **Provisioning of QoS:** All routing protocols must be able to provide a certain level of QoS according to the requirements of the nodes or the category of calls.

– **Support for time-sensitive traffic:** Generally all communications and similar applications require special support for time-sensitive traffic. As a rule, the routing protocol must be able to support hard as well as soft real-time traffic.

– **Security and privacy:** Let's note that routing protocol in ad-hoc WNs must be resilient to threats and some vulnerabilities. It should have built-in capability to avoid resource consumption, impersonation, denial-of-service, and also similar attacks possible against any ad-hoc WN.

Generally arbitrary movement of nodes changes existing topology dynamically in an unpredictable ways. Actually mobility of nodes, with the limitations of power source and bandwidth, makes multicast routing extremely challenging. As you know traditional wired network multicast protocols including different core based trees (CBT), protocol independent multicast (PIM), as well as distance vector multicast routing protocol (DVMRP) do not work well in ad-hoc WNs because existing tree-based multicast structure is unstable enough and requires frequent reconfiguration to involve broken links. Usage of any global routing structure including the link-state table leads to high control cost. The usage of single-link connectivity between the nodes in a multicast group leads to a tree-shaped multicast routing topology. Existing tree-shaped topology provides high multicast effectiveness, with low packet delivery ratio because of the frequent tree breaks. Provisioning of several links between the nodes in typical ad-hoc WN leads to mesh-shaped structure. The mesh-based multicast routing structure may work quite well in high-mobility medium. The main questions in designing multicast routing protocols are [1-3]:

• **Effectiveness:** A multicast protocol must perform a minimum number of transmissions to deliver a data packet to all members of the group.

• **Robustness:** It is known that multicast routing protocol must be able to quickly recover and reconfigure itself from potential communication failures caused by mobility, making it suitable for usage in highly dynamic mediums.

• **Efficient group management:** Such type of management applies to the process of accepting multicast session members and also maintaining existing connectivity between them until the session expires. This group management process must be carried out with minimal exchange of all control messages.

• **Control cost:** Insufficient bandwidth availability in real ad-hoc WNs requires minimal control cost for the multicast session.

• **Scalability:** Generally multicast routing protocol must be able to scale for a network with quite large number of nodes.

• **QoS** support is vitally important in multicast routing because, as a rule, the data transferred in a multicast session is quite time-sensitive.

• **Security:** Session member's authentication and also prevention of non-members from receiving unauthorized information play a main role in many military communications.

The basic objectives of the transport layer protocols involve setting up and maintaining end-to-end connections, necessary flow control, reliable end-to-end delivery of data packets, and congestion control. For instance, in real ad-hoc WN that uses a contention-based MAC protocol, all nodes in a high contention region experience certain backoff conditions which lead to magnified number of collisions and a high latency. Actually connectionless transport layer protocols, without realizing this situation, magnify the load in this network, degrading network performance. The main performance degradation faced by quite reliable connection-oriented transport layer protocol including transmission control protocol (TCP) in ad-hoc WN arises because of frequent path breaks, high link error rate, presence of trite routing information, as well as frequent network partitions.

The following discussion of each of listed above properties and their impact on the performance of the transport layer protocol assumes that TCP is the transport layer protocol. Because of the mobility of nodes and some limited transmission range, an existing path to a destination node is often interrupted. Each such path break leads to route reconfiguration which relies on the routing protocol used. Present congestion control algorithm reduces the size of the congestion window, resulting in low capacity. In medium where path breaks are frequent, the running congestion control algorithms on every path break influences the capacity drastically.

Generally delay associated with the reconfiguration of a broken path and applies route caches result in trite route information at the nodes. Wherefore the packets will be forwarded through several paths to a destination, causing magnify in the number of out-of-order packets. Besides, multipath routing protocols including temporally-ordered routing algorithm (TORA) [6] and also split multipath routing (SMR) protocols [8, 9] use several paths between a source-destination pair. Note that arrivals of out-of-order packet force the

receiver of the TCP connection to produce full duplicate acknowledgments (ACKs). When duplicate ACKs are received, the sender initiates the congestion control algorithm.

Let's note that wireless channels are inherently unreliable because of the high probability of errors caused by interference. In addition to the error because of the channel noise, hidden terminals presence contributes to the magnifyd loss of present TCP data packets or ACKs. If TCP ACK is delayed longer than the round-trip timeout, the congestion control algorithm is triggered. Because of the mobility of the nodes, typical ad-hoc WNs often experience isolation of the nodes from the rest of such network or appearance of so called partitions in the network. When a TCP connection spans across several partitions, meaning the pair receiver and sender of the connection are in 2 different partitions, all packets are dropped. Actually such tends to be more serious when the partitions exist for a fairly long duration, resulting in several retransmissions of the TCP packets and subsequent magnify in the retransmission timers. Of course such behavior causes fairly long periods of inactivity even in case the transient partition in network doesn't last long. Adaptation of the existing transport layer protocols must attempt to withstand the above questions for performing effectively in ad-hoc WNs.

All ad-hoc WNs' functioning relies on the presence of relaying nodes and also their willingness to relay other nodes' traffic. In the case node density is sufficiently enough to provide fully connected network [4, 7]. And then relaying neighbor node may not be interested in relaying any call and may only decide to power down. Suppose that optimal route from node *A* to node *B* passes through node *C*, and node *C* is not turned on. Then node *A* will have to set up more expensive and suboptimal route to *B*. Here non-optimal path consumes more resources and influences the capacity of the system. As the INs in a path that relay the present data packets expend their resources including battery charge as well as computing power, they should be correctly compensated. Wherefore pricing schemes that include compensation of service or service reimbursement are required. Let's note that ad-hoc WNs used for special tasks including many military missions, different rescue operations not require such pricing schemes, although the successful commercial deployment of ad-hoc WNs requires proper billing and pricing. Now obvious solution to guarantee participation is to provide incentives to forwarding nodes [4-6].

QoS is the level of performance services offered by a network or any service provider to all users. Rendering QoS in ad-hoc WNs can be on per-link, per-flow, or per-node basis. In some ad-hoc WNs, the boundary between the service provider (or network) and the user (or host) is blurred, so it is vitally important to have better coordination between the hosts to achieve QoS. Actually limited resources and also lack of central coordination make the problem worse.

• **QoS parameters:** Because various applications in turn have different requirements, then their QoS level and all associated QoS parameters also vary quite a bit from application to application. For instance, for existing multimedia applications, the delay and bandwidth are always key parameters, although military applications have the additional requirements in the field of reliability and security. For all applications including emergency rescue and search operations, availability is key QoS parameter. Multiple link disjoint paths may be the main requirement for such applications. Necessary applications for hybrid WNs can have maximum available delay, total link life, channel usage, and bandwidth as the key parameters for QoS. And finally, applications including communication between the nodes in any sensor network require that transmission between them leads to minimum energy consumption. Wherefore, all battery life or energy conservation can be the prime QoS parameters here.

• **QoS-aware routing:** Known that first step to QoS-aware routing protocol is usage of QoS parameters for path discovery. Such parameters which consider when making routing decisions include packet delivery ratio, network capacity, reliability, delay, total delay, packet loss rate, jitter, bit error rate as well as path loss. Decisions about the level of QoS and the related parameters for such services in real ad-hoc WNs are application specific and must be respected by the core network. This also requires the ability to reserve the necessary amount of bandwidth for such particular connection.

• **QoS framework:** is a complete system that must provide the promised services to each user or application. Let's note that its key component is a QoS service model which determines how user requirements are satisfied. Generally key design problem is whether to serve the user on a per-class basis as well as a per-session basis. Actually each class represents an aggregation of users built on certain criteria. The other main components of

real framework are necessary QoS medium access control, QoS signaling for resource reservation required by all users and application, QoS routing to find some or all feasible paths in existing network that can satisfy most user requirements, necessary connection admission control, as well as scheduling schemes pertaining to this service model.

One extremely important property is that all ad-hoc WNs must demonstrate independ organization and maintenance of the network. The main activities that ad-hoc WN must perform for self-organization are neighbor discovery, properly topology organization, and topology reorganization if it necessary. It may also require periodic transmission of special short packets named *beacons*, or promiscuous channel tracking for necessary detecting activities of neighbors. Some MAC protocols allow transmission power to be varied to significantly improve spectrum reuse. During the topology reorganization phase, ad-hoc WNs require updating current topology information with the help of incorporating the topological changes that have occurred in the network because of nodes failure, the nodes mobility, and the complete depletion of node power supplies. The reorganization consists of 2 main activities. The first type of activity is the aperiodic or periodic exchange of necessary topological information.

Another activity is adaptability (recovery from main topological changes in the network).

In the same way, network splitting and merging of 2 existing partitions require main topological reorganization. Let's note that ad-hoc WNs must be able to perform necessary self-organization effectively and also quickly in a way transparent to the application and all users.

The communication security in real ad-hoc WNs is extremely important, particularly now in many military applications. Actually lack of any central coordination along with shared wireless medium makes them more vulnerable to attacks compared to wired networks. All attacks against ad-hoc WNs are generally categorized into 2 types: active and passive attacks. The last one as a rule made attempts with the help of malicious nodes to understand the nature of activities and also obtain information that transacted in the network without disrupting its operation. Let's note that active attacks disrupt the operation of the network. Statistics show that those active attacks that are carried out by

nodes outside the network are usually called external attacks, and those that are carried out by nodes belonging to the same network are respectively called internal attacks. The main security threats that exist in typical ad-hoc WNs are as follows:

• **Resource consumption:** The lack of resources in ad-hoc WN makes it an easy target for internal attacks, especially aimed at consuming resources available in the network. We highlight the main types of resource-consumption attacks. They are:

– **Energy depletion:** Given that the nodes in ad-hoc WNs are highly limited by the energy source, this type of attack is mainly aimed to deplete the battery power of present critical nodes by routing unnecessary traffic through them.

– **Buffer overflow:** Such attack is performed either by filling special routing table with unnecessary routing entries or by using up the data packet buffer space with unnecessary data. Such attacks may cause a large number of present data packets being dropped, resulting in loss of critical information. Also routing table attacks may cause variety of problems, including preventing nodes from updating route information only for important destinations as well as filling the necessary routing table with routes for non-existent destinations.

• **Host impersonation:** Note that compromised internal node can act as another node and respond accordingly with appropriate control packets creating wrong route entries. It can also terminate the traffic meant for some intended destination node.

• **Denial of service:** The attack in which necessary network resource becomes unavailable for service to other nodes, either by using up the bandwidth or by overloading the system, is well-known as denial of service (DoS). The simplest scenario where a DoS attack disrupts the operation of ad-hoc WNs is that the target node remains busy forcing it to process unnecessary packets.

• **Information disclosure:** Here compromised node can act as an informer with the help of deliberate disclosing confidential information to unauthorized nodes. Information including the volume and the periodicity of traffic between a chosen pair of pattern and nodes of traffic changes can be extremely valuable for many military applications. The usage of filler traffic may not be appropriate in resource-constrained ad-hoc WNs.

• **Interference:** A common attack in some defense applications is to jam the wireless communication by generating a wide-spectrum noise. This can be done by using special single wide-band jammer, covering the entire spectrum. The MAC along with the physical layer technologies must be able to withstand such external threats.

Service discovery and addressing. This becomes important in ad-hoc WNs because of the absence of any centralized coordinator. Actually address which is globally unique in the connected part of the ad-hoc WN is required for a node as a means of participating in communication. Auto-configuration of addresses is necessary to allocate non-duplicate addresses to the nodes. In present networks with highly dynamic topology, frequent splitting and merging of necessary network components require special uplicate address-detection mechanisms as a means to maintain unique addressing across all connected parts of the network. So nodes in the network must be able to locate services that other nodes provide. Wherefore, it requires using effective service advertisement mechanisms. Any topological changes force any change in the location of the service provider as well, therefore fixed positioning of any server providing a particular service is eliminated. Rather, identifying the current location of necessary service provider gathers importance. On the other hand, provisioning of certain kinds of services requires authentication, billing, and confidentiality which in turn require separation of service discovery protocols from the network layer protocols.

Energy management is, as a rule, determined as the process of managing the sources energy and energy consumers in a network (or node) in general to increase the network lifetime. The energy management can be categorized into the following 4 types:

– Battery energy management**:** It is intended for extending node's battery life by using its chemical properties benefit, discharge patterns, and also selecting battery from available set of batteries using for redundancy. Last studies showed that battery pulsed discharge gives significantly longer life than continuous discharge. Let's note that controlling battery charging/discharging rate is important for avoiding early charging to maximum charge value or full discharge below existing minimum threshold. This can be achieved with the help of necessary embedded charge controllers in the battery pack. Besides, the protocols at the network and data link layers can be designed for usage of the

discharge models. Monitoring of the battery for remaining capacity, voltage levels, as well as temperature for necessary proactive actions (for instance, gradual powering off of certain devices, or turning off the mobile node when the voltage crosses a threshold) may be necessary.

– Transmission power management**:** Here power consumed with the help of the radio frequency (RF) module of a mobile node is mainly determined by certain factors including the operation state, the transmission power, as well as the technology applied for the RF circuitry. The operation state as a rule applies to the process of transmition, receiving, as well as sleep operation modes. Real transmission power is determined with the help of the reachability requirement of the network, the MAC and routing protocols used.

The RF hardware design must minimise the power consumption for all available operation states. Consider sleep mode when there is no reception or transmission, it is possible with the help of additional equipment that can waking up when receiving control signal. Actually power conservation responsibility lies across the data link, network, transport, and application layers. With the help of designing a data link layer protocol that decreases unnecessary retransmissions, by switching to standby or sleep modes when possible, by preventing collisions, and also by reducing the receive or transmit switching, power management can be carried out at the data link layer.

The usage of a variable power MAC protocol may cause certain benefits that involve energy-saving at the nodes, magnify in bandwidth reuse, and also reduction in interference. Besides, MAC protocols for directional antennas are at their infancy. Special network layer routing protocols can take into account battery life and real relaying load of the INs choosing a path as a means of the load alancing across entire network, as well as reducing the size and frequency of control packets plus optimizing. At the transport layer, protocols can include reduction in the number of retransmissions, as well as local recognition and elimination of causes of packet loss. At the application layer, the power consumption changes across applications. Note that in a mobile computer, the image or video processing/playback software as well as 3D gaming software consumes more power than other applications. Therefore application software developed for existing mobile computers must bear in mind all energy consumption aspect.

– Processor power management**:** Generally clock speed and the number of instructions executed per unit of time are among the processor parameters that influence power consumption. Also CPU can be set to various power-saving modes when processing load is low. CPU power can actually be interrupt that can be applied to turn on the CPU when user interaction or other events are detected.

– Devices power management**:** Now intelligent device management can significantly decrease power consumption of a mobile node. This can be done through the operating system (OS) using selectively powering down interface devices which are not applied or through putting devices into various power-saving modes, depending on their utilization. Require advanced power management characteristics built into the OS and necessary application softwares to effectively manage devices.

Despite the fact that number of nodes in an ad-hoc WN is not growing in the same magnitude as today's Internet, the operation of quite large number of nodes in all ad-hoc modes is just around the corner. Generally traditional applications including military, emergency operations and crowd control may not lead to such a big ad-hoc WN.

For instance, the latency of path-finding included with on-demand routing protocol in quite large ad-hoc WN may be unacceptably high. In the same way, the periodic routing cost participates a table-driven routing protocol can consume a significant amount of bandwidth in such big networks.

Also such large ad-hoc WN cannot be expected to be formed with the help of homogeneous nodes, raising questions including widely varying resource capabilities across the nodes. Generally hierarchical topology-based system and addressing may be more suitable for big real ad-hoc WNs. Typical hybrid architectures that combine the multi-hop microwave communications with infrastructure in place can significantly improve scalability.

2.2. Deployment Considerations

The deploying ad-hoc WNs includes actions different from those of existing wired networks. It requires careful planning and evaluation of future traffic growth on any network

link. Let's note that time-consuming planning stage is followed by actual network deployment. Actually time and cost required installing fiber or copper cables make it quite difficult to reconfigure any partial deployment that has already been completed [4-6]. The deployment of any commercial ad-hoc WNs has the following benefits as opposed to any wired network:

• **Budget deployment:** The usage of multi-hop wireless relaying largely eliminates the basic requirement of laying cables and also maintenance in a commercial deployment of existing communication infrastructure. Therefore the included cost is considerably lower than that of any wired networks.

• **Incremental deployment:** In commercial wireless WANs built on present ad-hoc WNs, deployment can be done incrementally across existing geographical regions of the city. Any deployed part of the network begins to function immediately after the minimum configurations have been done. For instance, during the deployment process for covering any highway, whenever all radio relaying equipment is installed on the side of highway, it can be put into operation.

• **Short deployment time:** As opposed to wired networks, the deployment time is considerably less because of the absence of any wired links. Besides, wiring a dense urban area is extremely time-consuming and difficult in addition to the inconvenience caused.

• **Reconfigurability:** The cost participates reconfiguring a wired network covering a metropolitan area network (MAN) is extremely high as opposed to that of any ad-hoc WN covering the same service area. Besides, the incremental deployment of ad-hoc WNs may require changes in the topology of the fixed part (such as the relaying devices mounted on some rooftops or lamp posts) of the network at a later stage.

The questions and solutions for deployment of ad-hoc WNs vary with the type of applications and the medium in which the networks are to be deployed. The following are the main questions to be considered in deploying any ad-hoc WN:

• **Scenario of deployment:** This becomes important because the capability required for a mobile node changes with the medium in which it is applied. These capabilities required for the mobile nodes that form any ad-hoc WN between ships fleet are not the same as capabilities required for forming an ad-hoc WN between a set of notebook computers at

a conference. Below are some of the various scenarios in which the deployment questions vary widely.

– Military deployment: Such deployment of ad-hoc WN may be data-centric (such as a wireless sensor network) or user-centric (such as sprcial armored and soldier vehicles carrying soldiers equipped with wireless communication devices). Generally data-centric networks handle a various pattern of data traffic and may be partially made up ofstatic nodes, although the user-centric network consists of highly mobile nodes without and with support from present infrastructure (such as military satellite constellations). Actually vehicle-mounted nodes have significantly better power supplies and computational resources at their disposal, although the portable devices are limited in energy and also computational resources.

So, real resource availability requires appropriate changes in the protocols used. Besides, the military environment requires quite secure communication. Routing must include as few nodes as possible to avoid possible leakage of information. Typically, flat addressing schemes are preferred over hierarchical addressing because the latter addressing requires establishing paths through the hierarchy, and therefore the chances of unreliable nodes forwarding the packets are very high.

– Emergency operations deployment: Such kind of application scenario requires a rapid deployment of rescue personnel equipped with portable communication equipment. Basically, the network must provide support for time-sensitive traffic including voice and video. Typically, short data messaging can be applied in case the resource limitations do not allow voice communication. Also in such scenario, a flat fixed addressing scheme with a static configuration is preferred. Generally, the network size for such applications does not exceed 100 nodes. Actually nodes are completely mobile without waiting for support from any fixed infrastructure.

– Commercial wide-area deployment: One example of such deployment scenario is all wireless mesh networks. The purpose of the deployment is to provide an alternate communication infrastructure for WN in urban areas and areas where any traditional cellular BS cannot cope with the traffic volume. This scenario is important because it provides very cheap per bit transferred as opposed to the wide-area cellular network infrastructure.

Another main benefit of this application is that it can withstand failure of a certain number of nodes.

Process of configuration, addressing, positioning of relaying nodes, nodes redundancy, and also power supplies are the main questions in deployment. QoS provisioning, billing, security, as well as mobility are main requirements that the service providers must answer.

– Homenetwork deployment: You need to consider the limited range of the devices that can connect to your network. Given the short transmission ranges of a few meters, it is vitally important to avoid network splitting. This problem can be solved by placing relay nodes at certain key points in home network. Besides, network topology must be decided in order to every node is connected via several neighbors to ensure availability.

• **Required longevity of network:** The deployment of ad-hoc WNs the required network lifetime must also be considered. If the network is needed for a short period of time (such as the connectivity between a group of researchers at a conference and the connectivity needed for coordination of a crowd control team), battery-powered mobile nodes can be applied.

• **Area of coverage:** As a rule, the coverage area of an ad-hoc WN is determined with the help of the application nature for which the network is set up. For instance, any home area network is significantly limited to the surroundings of a home. The mobile nodes' capabilities including the transmission range as well as associated software plus hardware, and of course power supply must match the required coverage area. Sometimes when some nodes can be fixed and the network topology is partially or completely fixed, the coverage can be improved with the help of directional antennas.

• **Service availability:** It is determined as the ability of ad-hoc WN to provide service even when certain nodes fail. Availability is becoming important both in a fully mobile ad-hoc WN applied for the tactical communication and in partially fixed ad-hoc WNs applied in the commercial communication infrastructure including wireless mesh networks. Dealing with the problems of wireless mesh networks it is known, that fixed nodes must to be placed in such a way that the failure of several nodes does not lead to lack of service in that area.

Sometimes, redundant inactive radio relaying devices can be placed so that if active relay node fails, the redundant relaying device can take over all its duties.

• **Choice of protocols:** at different layers of the protocol stack is to be done taking into account the deployment scenario [3, 6].

TDMA-based insecure MAC protocol may not be the best option for military application as opposed to CDMA-based MAC protocol. Generally MAC protocol must provide security at the link level. At the network layer, the routing protocol must be chosen carefully. Let's note that routing protocol which applies GPS information may not work properly in situations where such information is not available. For instance, any search-and-rescue operation teams which work underground or in extreme terrains or inside some building may not be able to apply such a routing protocol. Any ad-hoc WN with nodes that cannot replenish their power supplies should apply a routing protocol that does not use periodic *beacons* for routing. Actually in situations with high mobility periodic all routing or beacons updates, will drain the battery over time. For instance, an ad-hoc WN formed using devices connected to any military vehicles, the power consumption may not be extremely important and therefore one can use some beacon-based routing protocols for them. It is obvious that updated information about connectivity leads to significantly improved performance. Dealing with the subject of deploying wireless mesh networks, the protocols should use some fixed nodes to avoid any unstable paths because of the mobility of the relaying nodes.

• **Operational integration with other infrastructure:** In this case operational integration of ad-hoc WNs with other present infrastructures can be considered to improve the performance or collect additional information, or to provide better QoS. In the military environment, ad-hoc WNs integration with unmanned aerial vehicles (UAVs) or satellite networks significantly improves all ad-hoc WNs capability. Certain routing protocols rely on global positioning system (GPS), which is a satellite-based infrastructure that can provide geographical location information as a resource for network geographical positioning and also synchronization. Actually handover to a various network may be performed to avoid call loss when a mobile node with an active call moves to a region where service is not provided using current network.

2.3. The security basics for ad-hoc wireless networks

As indicated previously in this thesis, because of the unique features of well known ad-hoc WNs, the last ones are highly defenceless against security attacks contrasted with different wired networks or the infrastructure-based WNs. Here we discuss the several necessary conditions for security in current ad-hoc WNs, certain types of cyber attacks which may appear in such networks, as well as some solutions for guaranteeing today network security.

Now security protocols for up-to-date ad-hoc WNs need to meet all next requirements. The main ones are listed below. Of course they should be met by current security protocols for other classes of telecommunication networks.

– First is network **integrity:** All data transmitted by any source node must achieve its' destination node as it was transmitted. It's unaltered requirement. Putting it differently, it should not be able for any so called network malicious node to tamper with the data at the time of transmission process.

– Second is network **confidentiality:** The data transmitted by the sender (it is network source node) must be intelligible only to the aimed receiver (or destination node). Though intruders might get hold of the data being transmitted, they must not be able to derive users' useful information out of such data. It's known that one of the most popular techniques which can be intended for guaranteeing confidentiality is data encryption.

– Third is **non-repudiation:** It is a special mechanism to guarantee that the message sender cannot later disown having transmitted this message as well as that the recipient cannot disown having received such message. It is known that digital signatures, which function is unique identification for each network user, is very similar to written signature, are applied widely for such purpose.

– Fourth is **Availability:** Here network must remain in working condition all the time. It must also be robust enough to tolerate link failures plus it must be capable of surviving several attacks mounted on it. In addition it should be possible to give the guaranteed services at any moment when authorized network users require them.

As you know designing any security foolproof protocol for ad-hoc WN is really challenging task. This is mainly due to certain unique features of ad-hoc WNs, in particular, the insecure operating medium, shared broadcast radio channel, real lack of central authority, significant lack of the association between nodes, significant resources limited availability, as well as real physical vulnerability. Consider some complication in providing security in existing ad-hoc WNs.

First of all it's **insecure operational medium.** It meens, that operating mediums where ad-hoc WNs are utilized may not always be so secure as we think. One essential application of such type of networks is in battlefields. In such usage, nodes may move in as well as out of hostile and also enemy insecure territory, where they would be notably defenceless against security attacks.

Secondly it's **shared broadcast radio channel:** It can be stated that in contrast to in wired networks where any separate dedicated transmission line may be given between a pair of nerwork end users, the radio channel can be intended for communication in existing ad-hoc WNs as known is broadcast in the nature and is shared by all existing nodes in such network. Data which sent by any node is received by all network nodes within such direct transmission range. So any malicious node could absolutely easily get data being transmitted over this network. This problem can be significantly minimized to a certain extent by using, For instance, directional antennas.

Thirdly it's **Lack of central authority:** In wired networks as well as special infrastructure-based WNs, it would be able monitoring network traffic through certain essential central points (such as base stations, routers, and, of course, different access points) Also it would be able implement necessary security mechanisms at such points. As long as existing ad-hoc WNs don‘t have such central points, described mechanisms cannot be used in any ad-hoc WNs.

In the fourth it's **lack of association:** As long as these networks are dynamic in its nature, so any node can leave or join the network at any moment of the time. If there is no proper authentication mechanism which intended for associating nodes with a network, the intruders would be possible to join into such network quite easily and made her or his attacks.

Next is quite **limited resource availability:** It can be stated that resources including battery power, bandwidth, and also computational power (to some extent) are scarce in existing ad-hoc WNs. So, it is absolutely clear, that now implement special complex of cryptography-based security mechanisms in such type of networks really difficult.

The last is **physical vulnerability:** Some nodes in such networks are generally hand-held and compact in its nature. Please note that they could easily get damaged and they are vulnerable to theft too.

As you know attacks on ad-hoc WNs may be categorized into two broad types, in particular, *active* and *passive* attacks. Tha last one does not disrupt the current operation of the network. Attacker intercepts the data exchanged in the network without changing it. So, the confidentiality requirement can be easily violated if an attacker is also possible to interpret the data collected through snooping. The passive attacks detection is really difficult as long as it does not influence the operation of network itself.

One of the way overcome existing problems it is usage quite powerful encryption mechanisms to encrypt all data being transmitted. In this way it make impossible for eavesdroppers to get essentially useful information from the data overheard.

If we talk about active attack it tries to destroy or alter the data being exchanged in this network, thus it disrupts the normal network operating. The active attacks can also be grouped further into two categories, in particular, *internal* and *external* attacks.

Tha last ones are performed by the nodes that don’t belong to this network. Such attacks can be easily prevented by means of the standard security mechanisms for instanceencryption techniques along with different firewalls. Internal attacks are from compromised nodes that are special firewall is applied to separate any local network from the outside world. Note, that it is special software which operates closely with router program and filters necessary packets entering the network to determine whether these packets should be forwarded to their intended destinations. As is well known firewall protects the resources of any private network from the malicious intruders on foreign networks for instance the Internet.

In an existing ad-hoc WN, the firewall software can be installed on each network node. It is actually part of such network. As long as the attackers are already a part of the

network as its authorized nodes, it can be conclude that internal attacks are more severe. Also they really hard to detect contrasted with external attacks.

As you can see Fig. 2.11 illustrates a classification of several types of attacks which are possible in ad-hoc WNs. Next we describe the several attacks listed in the Fig. below.

Now we give brief descriptions of the attacks related to the network layer in modern network protocol stack. Consider the main ones.

– **Information disclosure:** Generally compromised node can transmit confidential or essential information to unauthorized nodes in the network. This information may also include information concerning network topology, necessary geographic location of nodes, or optimal routes to authorized nodes in such network.

– **Blackhole attack:** Here, a malicious node falsely advertises correct paths (such as most stable or shortest path path) to the end node during all path-finding process or in necessary route update messages. Actually intention of the malicious node may be to disrupt the path-finding process or to intercept all necessary data packets being transmitted to respective destination node.

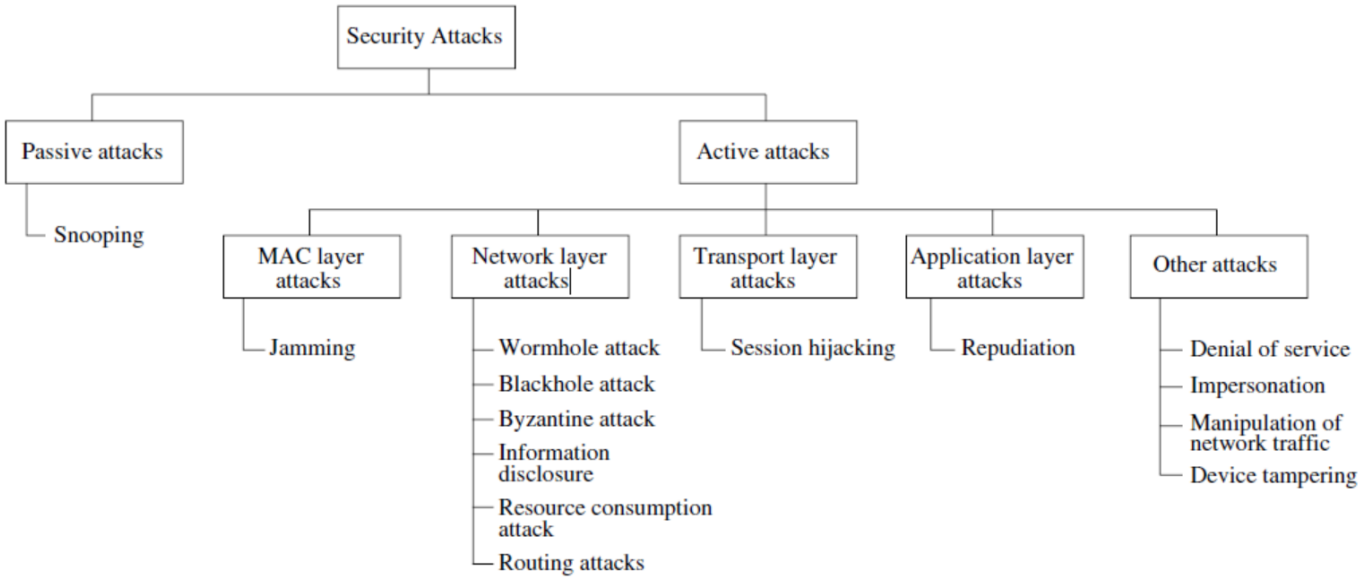


Fig. 2.1. Classifications of attacks

– **Wormhole attack:** In this case, some attacker receives packets at one location in the network and also tunnels them to another one in the network, where the necessary packets are retransmitted into the network [10]. Note that this tunnel between 2 colluding

attackers is concerning as a wormhole. It can be installed over single long-range wireless link or even over necessary wired link between 2 colluding attackers. Because of the broadcast nature of any radio channel, the attacker can create a wormhole even for packets not addressed to it. Nevertheless no considerable harm is done if the wormhole is applied correctly for effective relay packets, it puts the attacker in a strong position as opposed to other nodes in the network that any attacker can apply in ways that could compromise the network security. As is well known proper mechanisms are not used to protect the network from wormhole attacks, most of all existing routing protocols for present ad-hoc WNs may fail to find valid routes.

– **Routing attacks:** There are certain types attacks fixed on the routing protocol that are intended for disrupting the operation of the network. Further, the several attacks on the routing protocol are described briefly.

– **Byzantine attack:** In this case, a compromised IN or a set of compromised INs works in possible collusion and carries out attacks. For instance, it may be necessary routing packets on non-optimal paths, creating routing loops, along with selectively dropping packets [9].

– **Routing table poisoning:** In this case, the compromised nodes in such networks send bogus routing updates and modify genuine route update packets transmitted to other uncompromised nodes. Special routing table “poisoning” may result in sub-optimal routing, overloading parts of the network, or even causing some parts of such network inaccessible.

– **Resource consumption attack:** In such case, a malicious node tries to consume or waste away all resources of other nodes available in the network.

– Routing table overflow: Here, special adversary node advertises routes to non-existent nodes, for the authorized nodes existing in the network. Actually basic goal of such an attack is to cause routing tables to overflow, which in turn will prevent the creation of entries corresponding to new routes to authorized nodes. Generally proactive routing protocols are more defenceless against this attack contrasted with existing reactive routing protocols.

– Packet replication: Here, an adversary node replicates trite packets. This consumes additional bandwidth along with battery resources available to these nodes and in turn causes unnecessary confusion of routing process.

– Route cache poisoning: When we used on-demand routing protocols (for instance the AODV protocol [9]), every node maintains a route cache which contains information about routes that have become known to this node in the recent past. So, similar to special routing table poisoning, attacker can also poison this route cache to achieve same goals.

– Rushing attack: On-demand routing protocols that apply duplicate suppressionduring the route discovery process are defenceless against this attack [8]. As is well known adversary node that receives a so called *RouteRequest* packet from the source node quickly broadcasts packet across the network before other nodes that also receive the same *RouteRequest* packet can respond.

It is necessary to mention that nodes which receive the legitimate *RouteRequest* packets assume those packets are duplicates of the packet already received via the adversary node and therefore discard those packets. Any route discovered with the help of the source node will contain the adversary node as one of the INs. That is why this may cause some failure; becouse source node would not be possible to find secure routes, that is, routes that do not involve the adversary node. It is really hard to detect such attacks in existing ad-hoc WNs.

Here consider the attack which is specific only to transport layer in all protocol stacks of present networks.

The first of all is **session hijacking:** In such case, an adversary takes control over a session between 2 nodes. As long as most authentication processes are performed only at the session beginning, once the session between 2 nodes is established, the adversary node masquerades as one of the session end nodes as well as hijack the session.

Application Layer Attacks

Here we very briefly describe some security flaw associated with the application layer in any network protocol stacks.

Repudiation: In simple terms, repudiation applies to the denial or attempted denial using node participates a communication of having participated in all or part of the

communication. As you know, non-repudiation is one of the essential requirements for a security protocol in any communication network.

Multi-layer Attacks. They could occur generally in any layer of the network protocol stack. Impersonation and also service denial are common multi-layer attacks. Here we consider several multi-layer attacks in ad-hoc WNs.

Denial of Service: In such type of attack, adversary attempts for preventing all authorized and legitimate users of services offered using the network from accessing those services. Actually denial of service (DoS) attack can be performed in many ways. It is necessary to mention that classic way is to send packets to any centralized resource (such as access point) used in the network in order to the resource is not available anymore to nodes in this network, and as a result the network no longer operates tha way it was designed to operate. That is why this may cause some failure in the delivery of guaranteed services to the end users. Because of the unique characteristics of existing ad-hoc WNs, there exist many more ways to launch a DoS attack in such a network, which would not be able in wired networks.

Well known DoS attacks can be easily launched against any layer in the network protocol stack [9]. On the MAC as well as on physical layers, an adversary can use jamming signals that disrupt the ongoing transmissions on any wireless channel. Let's note that on the network layer, an adversary can take part in some routing process and use the routing protocol to disrupt the normal functioning of all networks.

Jamming: Here attacker initially continues to monitor all wireless medium to determine the frequency at which some receiver node is receiving signals from some sender. It then transmits signals on that frequency in order to error-free reception at the receiver is hindered. As is well known frequency hopping spread spectrum (FHSS) and also direct sequence spread spectrum (DSSS) are 2 currently widely used now techniques to overcome jamming attacks.

When receiving the SYN packets, the victim node sends reverse acknowledgment (SYN-ACK) packets to nodes whose addresses were specified in the received SYN packets. On the other hand, the victim node will not receive any ACK packet in return. Essentially, a half-open connection is created.

It’s known that victim node create a data/table structure to store information about all pending connections. As long as the maximum possible size of the table is limited, the increasing number of half-open connections leads to overflow in such table. For this reason, in the case a connection request comes from some legitimate node at a later point of time, due to the table overflow, the victim node will be forced to reject any call request [6-8].

Distributed DoS attack: A more severe form of the DoS attack is the distributed DoS (known as DDoS) attack. In such type of attack, some adversaries that are distributed throughout the network collude and prevent legitimate users from accessing the services offered by the network.

Device tampering. Unlike present nodes in all wired network, nodes in existing ad-hoc WNs as a rule, are softer, more compact, as well as hand-held in nature. That is why they could get damaged or stolen easily.

Impersonation: In such attacks, an attacker assumes the privileges and identity of an authorized node, either for usage of existing network resources that may not be available to it under normal conditions, or to disrupt the normal operation of the network by introducing false routing information into the network. An adversary node can masquerade as an authorized node using certain techniques. Let's note that it can accidentally guess the authentication or some identity details of this authorized node, or it can track information concerning authentication or identity of the target node from a previous communication session, or it can bypass or disable existing authentication mechanism on the target node. Actually *man-in-the-middle* attack is another type of impersonation attack.

CONCLUSION TO CHAPTER 2

In this chapter classifications of attacks was considered. Security fundamentals for ad-hoc wireless networks have been analyzed. In most of the networks discussed, communication is carried out using radio waves of the appropriate wavelength. In some scenarios, only infrared light was used to transmit all data. It is proposed to use new effective network protocols at the physical and also at MAC layers so that the transition from existing wired to modern wireless networks is smooth enough for higher levels of the protocol stack.

Also clearly shows that when deploying and selecting the appropriate technology for modern WLANs, there is always a combination of different factors to consider, namely QoS requirements, total cost deploymen, expected traffic load, bandwidth requirements and many others.

CHAPTER 3
TECHNOLOGICAL PROTECTION AGAINST NETWORK ATTACKS

3.1. Key management

Having seen the different kinds of methods possible on any ad-hoc WNs, so let’s consider at different techniques used to overcome the attacks. Cryptography is just one of the most reliable and common tools. The cryptography is not specific to existing ad-hoc WNs. Generally it can be applied today to any communication network. It is the research of the methods, principles, and algorithms via which necessary information is transformed into a disguised version that no unauthorized person can read. But intended recipient can reconstruct (or recover). In the cryptography “language”, the original information transmitted from one person to another is known as plaintext.

There are 2 main kinds of cryptographic algorithms: symmetric key (SK) and symmetric key (AK) algorithms. The last one uses the same key for decryption and encryption procedures. In AK algorithms are used 2 different keys for decryption and encryption procedures.

Let's note that SK algorithms are as a rule faster to execute electronically, but require a secret key to be shared between pair of receiver and sender. When communication network needs to be established between node groups, each pair receiver and sender must share a key in use.

Essentially AK algorithms are built on some mathematical lows that make it impossible to receive one key using another one; so, one of such keys can be public while the other is kept private. This is known as public key cryptography. Such systems are widely used in practice, but their safety has not been proven. They depend on the complication of solving some scientific problems, and in this case network would be open to the attacks once the underlying this problem is solved.

3.1.1. Symmetric Key Algorithms

SK algorithms depend on the presence of the shared key at pair receiver and sender, which has been replaced by certain previous arrangement. There are 2 existing kinds of SK algorithms, one with the participation of block ciphers and the other with the participation of stream ciphers. Any block cipher is special encryption scheme where the plaintext is broken into some fixed-length segments called blocks, and all blocks are encrypted one at a time. One of the simplest examples involves transposition and substitution procedures. In last one, each plaintext alphabet is substituted by another in the special ciphertext. Next this table displaying the original and then substituted alphabet is available at pair receiver and sender. Let's note that transposition cipher permutes the alphabet in the necessary plaintext to produce some ciphertext. Fig. 3.1 (a) shows the encryption using such substitution, and Fig. 3.1 (b) illustrates a transposition cipher. The block length used is five.

Original Alphabet	A B C D E F G H I J K L M N O P Q R S T U V W X Y Z
Substitution	E F G H I J K L M N O P Q R S T U V W X Y Z A B C D
Plaintext	EVERYDAY CREATES A HISTORY EVERY DAYCR EATES AHIST ORY
Ciphertext	IZIVC HECGV IEXIW ELMWX SVC

(a)

Transposition	1 2 3 4 5 ↓ 3 5 1 4 2
Plaintext	EVERYDAY CREATES A HISTORY EVERY DAYCR EATES AHIST ORY
Ciphertext	EYERV YRDCA TSEEA ITASH YOR

(b)

Fig. 3.1. Substitution and transposition

A stream cipher is, as a result, a block cipher of block length one. As an example may be Vernam cipher, than can use the same length key as any plaintext for encryption. For instance, if some plaintext is the binary string 10010100, and its key is 01011001, in this case the encrypted string is given by XOR of both key and plaintext, will be 11001101. Essentially plaintext is recovered once more with the help of XORing the ciphertext with the same key. If the key is randomly chosen, transported securely to the receiver, and used for only one communication network, this can forms the onetime pad that has proven to be the most secure of all existing cryptographic systems. As a result only “bottleneck” here can securely send any key to the receiver.

3.1.2. Asymmetric key algorithms

Let's note that AK algorithms use different keys at the sender and receiver ends for encryption and decryption, respectively. Let current encryption be represented with the help of a function *E*, and decryption with the help of *D*. Next plaintext *m* is transformed into the ciphertext *c* as function $c = E(m)$. The receiver and then decodes *c* with the help of applying *D*. For this reason, *D* is such that $m = D(c) = D(E(m))$. When this AK concept is used in public key algorithms, then key *E* is made also public, while *D* will be private, and it is known only to some intended receiver. Anyone who would like to send a message to this receiver encrypts it using *E*. As a result *c* can be overheard with the help of attackers, the function *E* is built on a computationally difficult scientific problem, including the factorization of big prime numbers. For this reason, it’s not possible for attackers to derive *D* given *E*. Just the receiver can decrypt *c* using the private key *D*.

Essentially digital signatures schemes are also built on public key encryption. In these schemes, just functions *D* and *E* are chosen and $D(E(m)) = E(D(m)) = m$ for any necessary message *m*. It’s known as reversible public key systems. Here, the person who would like to sign a document encrypts can use her/his private key *D*, which is known only to her/his. Anybody who has his/her this public key *E* can decrypt it and receive the original document, in the case when it has been signed with the help of the corresponding sender. As a rule, a trusted third party (TTP) is agreed upon in advance, who is responsible for issuing certain

digital signatures (pairs *D* and *E*) and for resolving all disputes concerning the signatures. As a rule it may be a business and governmental organization.

3.1.3. Key management approaches

The main objective of all key management is to share some necessary information between a specified set of participants. Today there are several techniques that can be used to perform this operation, all of them requiring varying amounts of initial configuration, communication, as well as different computation. The most important l approaches to key management are key procedures such as transport, predistribution, arbitration as well as agreement [10, 12].

Let's note that key predistribution, as is clear, includes distributing keys to all interested parties before the beginning of communication process. This technique includes much less proctdure of communication and necessary computation, but necessary that all participants must be known *a priori* (before network deployment). Unfortunately there is no mechanism after deployment to involve new members in this group or to change in some way this key. As an improvement over the basic pre-assignment scheme, certain sub-groups may be formed within existing group, and so some communication proctdure can be limited just to the subgroup. Despite that, the formation of such sub-groups will be also an *a priori* decision with no flexibility during its functioning.

In the all key transport systems, one of certain communicating entities generates some keys and then transports them to the other network members. The simplest case assumes that a shared key already exists between all participating members. As a result such prior shared key is applied for encryptng a new key and next transmition to all corresponding nodes. It's clear that only those nodes which have the prior shared key can decrypt it. It’s known as key encrypting key (KEK) technique. Despite that, the existence of a prior key cannot always be assumed. In the case when existing public key infrastructure (PKI) is present, then key can be encrypted using each participant’s public key and then transported to it. Essentially this assumes the existence of TTP, which may not be available for some ad-hoc WNs.

Let's note that interesting technique for key transport without availability of prior shared keys is well-known Shamir's three-pass protocol [10]. Its scheme is built on a special type of encryption known as commutative encryption schemes. The message exchanges of mentioned above protocol are illustrated in Fig. 3.2.

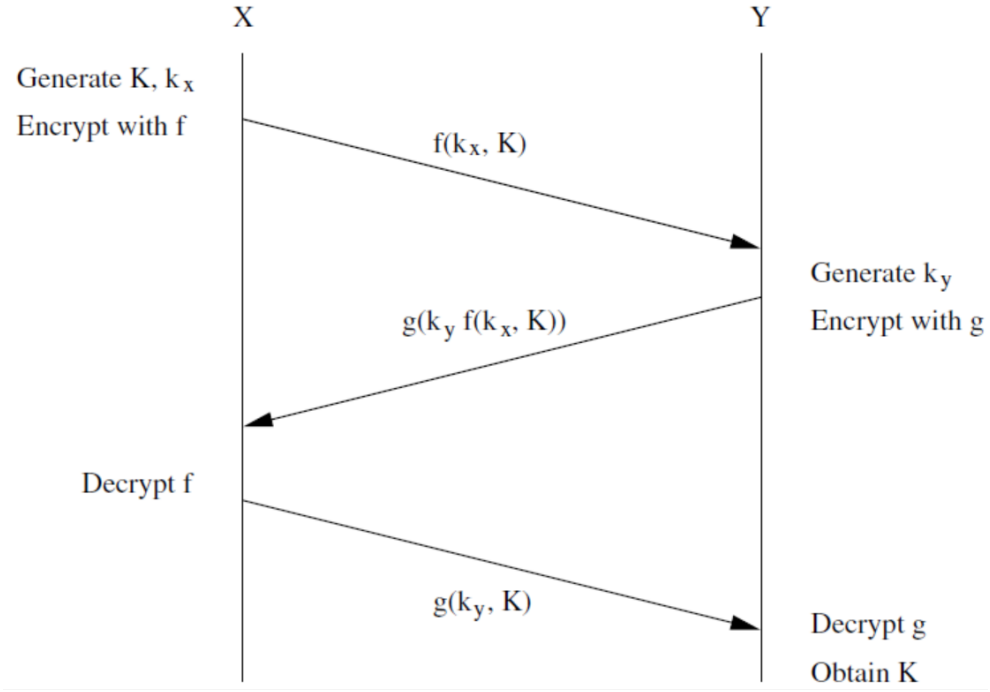


Fig. 3.2. Shamir's three-pass protocol

Such key arbitration scheme uses a central arbitrator to create and then distribute keys between all participants. For this reason, they are some class of key transport schemes. All networks which have a fixed infrastructure can apply the AP as an arbitrator, as it does not have stringent power and computation limitations. Generally in ad-hoc WNs, the problem with implementing arbitrated protocols is that any arbitrator has to be enabled at all times and to be always available to all nodes. As a result this leads to significant loss of power on that particular node. As alternative may be solution to make the keying service distributed, but such simple replication of the arbitration at differing nodes would be quite expensive for all resource-constrained devices and in this way would offer many points of vulnerability for attacks. In the case when any one of the replicated arbitrators is attacked, the security of the whole system breaks down.

Statistics show that most key agreement schemes are built on AK algorithms. They are used when 2 or more individuals want to agree upon a secret key that will then be applied for further necessary communication process. Let's note that key agreement protocols are applied to establish a secure context over where certain session can be run, beginning with many parties wanting tocommunicate and an insecure channel. Generally in all group key agreement schemes, each participant contributes some part to pecial secret key. In this case least amount of preconfiguration it requires, but such schemes have fairly high computational complexity. Today, most popular key agreement schemes apply the Diffie-Hellman exchange, it is special AK algorithm built on discrete logarithms [12].

3.1.4. Key management in ad-hoc wireless networks

Typicala ad-hoc WNs create certain specific problems in key management because of the lack of necessary infrastructure in such networks. Research has shown that there are types 3 of infrastructure, that are absent in ad-hoc WNs [9, 13]. The first type is the network infrastructure, including routers and some stable links that provide communication procedures with all nodes. The second type of missing infrastructure is services including directory, name resolution, as well as TTPs. The third type of missing infrastructure in ad-hoc WNs is the necessary administrative support of certifying authorities.

One example of such scenario implementation is a meeting room, where differing mobile devices want to begin its secure session. In this case, all participants included in the session are to be identified (identification is built on their location) in this way, all devices in the room can be part of this session. For this reason, relative location is used as some criterion for access control. In the case when a TTP knows the location of all participants, then it can implement special location-based access control.

Let's note that password-based system has been investigated where, in the simplest case, a long string is set as the password for users for only one session. Despite that, we know that people beings tend to prefer natural language phrases as passwords, over randomly generated several strings. As a result such passwords, in the case when used only directly keys during a session, are quite weak and also open to attack due to high redundancy, as well as the possibility of reuse over differing sessions. For this reason,

protocols have been proposed to derive strong key (invulnerable to attacks) from quite weak passwords given with the help of the participants. Now statistics show, that password-based system could be two-party, with individual exchange between any 2 participants. Or it may be for the whole group of the participants, with some leader being elected to preside over the session. This leader election represents a special case of setting up an order between all participants. Essentially protocol used is as follows. Each participant creates a random number, and then sends it to all others participants. When every node has received such random number of every other node, general predecided function is utilized on all the numbers to calculate special *reference value*. All nodes are applied the difference between their random number and special reference value.

Existing public key infrastructure (PKI) provides the easy keys distribution and also is a scalable technique. Each node should have pair of private/public key, and also certifying authority (CA) can bind the keys to the specific node. But the CA must be present at all times that may not be feasible in ad-hoc WNs. Pay attention to the fact that it is also not advisable to simply replicate the CA at differing nodes.

Note that to sign a certificate, each server must generate so called partial signature using its private key and then submits it to certain combiner. The last one can be any one of the servers. To ensure that all key are combined correctly, $t + 1$ combiners can be applied to account for at most t malicious servers. Applying $t + 1$ special signatures (receiveed from itself and t other servers), the combiner calculates a signature and next verifies its validity with the help of public key. In the case when the verification fails, it means that at least one of existing $t + 1$ keys is not valid, so another subset of $t + 1$ special signatures is tried. In the case when the combiner itself is malicious, it cannot get any valid key, since the special signature of itself is always invalid.

Let's note that scheme can be used to asynchronous networks, with no restrictions on message processing and delivery times. This is one of strong points of this scheme, since all requirement of synchronization makes the system quite vulnerable to DoS attacks.

Statistics show that mobile attackers can move from one server to another, attack them, and so take ove of their private keys. An attacker may have more than t private keys over a period of time. To counter this, necessary *share refreshing* has been proposed; in this

situation servers must create a new independent set of shares (the special signatures that are applied by the servers) periodically. For this reason, to break the system, an adversary must attack and take over more than *t* servers within certain period between 2 successive refreshes; otherwise, the earlier shared data will no longer be valid. This significantly improves current protection against mobile attackers.

Some authors proposed to use completely self-organized public key system for ad-hoc WNs [11]. It requires absolutely no infrastructure – such as CA, TTP, and any server – even during initial configuration. All users in the ad-hoc WN issue certificates to each other built on personal acquaintance. Essentially certificate is a binding between some node and its public key. Such certificates are also stored and next distributed with the help of the users. All certificates are issued only for a certain period of time and along with them indicate the time of expiration of their validity. Before it expires, the certificate must be updated with the help of the user who had issued the certificate.

Pay attention to the fact that initially, each user has a local repository consisting of the certificates issued with the help of him and the certificates issued with the help of other users to him. For this reason, each certificate is initially stored twice, with the help of the issuer and with the help of the person for whom it is issued. Periodically, certificates from neighbors are requested and certain repository is updated with the help of adding any new certificates.In the case when any of the certificates are conflicting (such as the certain public key to differing users, or the same user having differing public keys), it is possible that some malicious node has issued a false certificate. In this case node labels such certificates as *conflicting* and also tries to resolve this conflict. Various techniques exist to compare the confidence in one certificate with other. For example, another set of certificates receiveed from another neighbor can be applied to take a majority solution.

This can be applied to evaluate the trust in other users and detect malicious nodes.In the case when the certificates issued with the help of some node are found to be wrong, then that node may be assumed to be malicious.

Some authors determine a certificate graph as a graph whose vertices are public keys of any node and whose edges are public-key certificates issued with the help of users [10]. In the case when any user *X* wants to receive the public key of another user *Y*, she/he finds

a chain of valid public key certificates leading to *Y*. Essentially chain is such that the first hop uses an edge from *X*, so, a certificate issued with the help of *X*, the last hop leads to *Y*, and then all INs are trusted via the previous certificate in this path. Note that protocol assumes that trust is transitive that may not always be valid.

3.2. Secure routing in ad-hoc wireless networks

Unlike existing so-called traditional wired Internet, where there are dedicated routers controlled with the help of the Internet service providers (ISPs) exist, in typical ad-hoc WNs, nodes act both as regular terminals (e.g. source and destination) as well as as routers for other nodes. Generally in the absence of dedicated routers, ensuring security becomes quite difficult task in these networks. Various existing factors that make the task of ensuring secure communication process in ad-hoc WNs quite difficult involve necessary nodes mobility, limited processing power, a promiscuous operation mode, as well as limited availability of resources including battery bandwidth, power, and so on.

3.2.1. Requirements of a Secure Routing Protocol for Ad-hoc Wireless Networks

The basic requisites of secure routing protocol for any ad-hoc WNs are listed below:

• **Stability against attacks:** Here any routing protocol must be self-stable in the sense that it should be able to return to its normal operating mode within a finite amount of time after active as well as passive attacks. Essentially routing protocol must take care that these attacks do not permanently disrupt the routing process. All such protocol should also provide Byzantine robustness [10].

• **Guarantee of correct route discovery: In the case when** a route exists between some destination and some source nodes, then routing protocol should be able to find this route, and must also ensure that the chosen route is correct.

• **Detection of malicious nodes:** In this case secure routing protocol must be able to detect the presence of all malicious nodes in the network and also must avoid the participation of these nodes in the routing process. Evenin the case when such malicious

nodes participate in the route discovery process, the routing protocol must choose necessary paths that do not involve such nodes.

• **Confidentiality of network topology:** It is known that information disclosure attack may cause the discovery of the network topology with the help of the malicious nodes. Pay attention to the fact that once the network topology is known, the attacker may try to research the traffic pattern in the network.In the case when some of the nodes are found to be more active as opposed to others, the attacker may try to mount (such sa DoS) attacks on such bottleneck nodes.

3.2.2. Security-aware ad-hoc routing protocol

The security-aware ad-hoc routing (SAR) protocol as a rule uses security as one of the key metrics in path finding. It is known that framework for measuring or enforcing the attributes of some security metric enables the use of differing levels of security for differing applications that use SAR for routing [9-12].

Statistics show that in ad-hoc WNs, communication between end nodes via possibly multiple INs is built on the fact that the two end nodes trust the INs. SAR determines *level of trust* as a routing metric and also as one of the attributes for security to consider when routing. Here routing protocol built on the level of trust is explained below with the help of Fig. 3.3. Here only 2 paths exist between 2 officers $O1$ and $O2$ who want to communicate with each other. One of these paths is a shorter path that runs through private nodes whose trust levels are quite low. For this reason, the protocol chooses a longer but secure path that passes through other secure (officer) nodes.

Generally in the AODV protocol, any source node broadcasts a *RouteRequest* packet to its neighbors. IN, on receiving special *RouteRequest* packet, forwards it further in the case when it does not have a route to this destination. Besides, it initiates a *RouteReply* packet back to the source node using for this reverse path traversed with the help of the *RouteRequest* packet. In SAR, definite level of security is included into the packet-forwarding mechanism. Pay attention to the fact that, each packet is associated with a security level that is determined with the help of a number calculation technique. Each IN is also associated with a definite level of security.

Next, on receiving packet, the IN compares its level of security with that determined for the packet. In the case when the node's security level is less compared to the packet level, the *RouteRequest* is simply discarded.

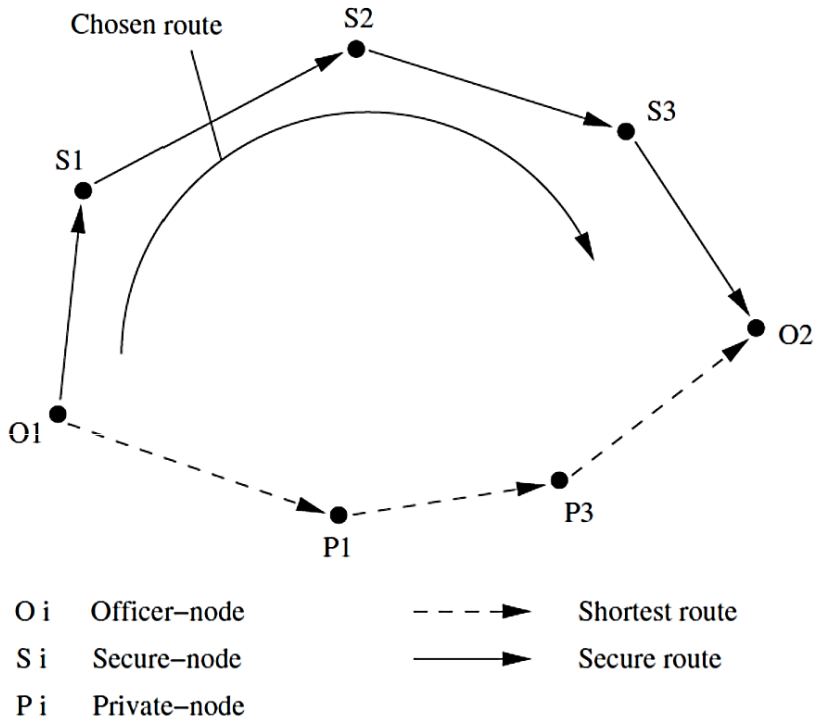


Fig. 3.3. Illustration of the level of trust metric

In the case when it is greater, the node is considered as secure node and is allowed to forward the packet in addition to the ability to view the packet. In the case when the security levels of the IN and the received packet are turned out to be equal, then the IN has no ability to view such packet; it only can forward the packet further.

Essentially equal levels nodes of of trust distribute a common key between themselves and with those nodes having higher trust levels. For this reason, certain hierarchical level of security must be maintained. This ensures that an encrypted packet can be decrypted (with the help of common key) only with the help of nodes of the same or higher levels of security as opposed to the level of security of the packet. Statistics show that differing levels of trust can be determined using a number calculated built on the level of security required. Generally it can be calculated applying many techniques. Considering that timeliness, authenticity and authorization, in-order delivery of the packets, confidentiality and integrity, as well as non-repudiation are only some of the desired characteristics for routing protocol,

a necessarynumber can be determined for the trust level for any nodes or packets built on the number of such characteristics have been taken into account.

Pay attention to the fact that SAR mechanism can be easily included into some traditional routing protocols for ad-hoc WNs. It should be included to table-driven or on-demand routing protocols. Generally SAR protocol permits the application to choose certain level of security it requires. However the protocol requires differing keys for differing levels of security. This tends to significantly increase the number of keys required in the case when the number of security levels applied increases.

Secure effective ad-hoc distance vector (SEAD) routing protocol, is a secure typical ad-hoc routing protocol built on the destination-sequenced distance vector (DSDV) routing protocol [11]. Such protocol is mainly intended to overcome security attacks including DoS as well as resource consumption attacks. All protocol applies a one-way hash function and does not include any AK cryptographic operation.

Today metric applied for routing is the distance measured in terms of some hop-count. Existing routing table is updated periodically with the help of exchanging routing information. Statistics show that alternative to this approach is triggered updates, in that each node broadcasts routing updates only in the case when its routing table gets changed. In this case DSDV protocol for typical ad-hoc WNs applies sequence number tags to prevent the formation of loops, to of solve the problem counting to infinity and for faster convergence. In the case when a new route update packet is received for an end point, next node updates the corresponding entry in necessary routing table only in the case when the sequence number on the received update is quite greater compared to recorded with the corresponding entry in such routing table [11].

Pay attention to the fact that SEAD can use authentication to distinguish between updates received from malicious and non-malicious nodes. This leads to minimization of resource consumption attacks caused by some malicious nodes. Note that SEAD applie one-way hash function for authenticating the necessary updates. Generally one-way hash function (H) creates an one-way hash chain ($h1, h2, \ldots$). Here function H maps input bit-string of any length to a fixed length bit-string. So we have, $H : (0, 1)* \rightarrow (0, 1)\rho$, where ρ is the length in output bit-string bits. To make necessary one-way hash chain, certain node

creates a random number with initial value $x \in (0, 1)\rho$. $h0$. Note that first number in this hash chain is initialized to x. Essentially remaining values in this chain are computed with the help of general formula, $hi = H(hi-1)$ for $0 \leq i \leq n$, for some n. It's clear that one-way hash function includes security into the special DSDV-SQ routing protocol. Usually SEAD protocol assumes an upper bound on the metric applied. For instance, in the case when the metric applied is distance, then the upper bound value $m - 1$ determines the maximum diameter of any ad-hoc WN. For this reason, the routing protocol ensures that no route of length greater than m hops exists between any two nodes.

Generally if the sequence of values calculated with the help of a node using only hash function H is given by ($h1, h2, \ldots, hn$), where n is divisible by m, next for certain routing table entry with sequence number i, let $k = k\ m - i$. In the case when the metric j (it is distance) applied for that routing table entry is $0 \leq j \leq m - 1$, then we have that value $hkm+j$ is applied to authenticate necessary routing update entry for such sequence number i as well as that metric j. When any route update message is sent, the node adds the value applied for authentication along with it. In the case when the authentication value applied is $hkm+j$, then the attacker trying modifying this value can do so only in the case when she/he knows value $hkm+j-1$. Considering that it is a one-way hash chain, calculating value $hkm+j-1$ becomes impossible. An IN, on receiving all authenticated update, next calculates the new hash value built on the earlier updates ($hkm+j-1$), as well as value of the metric, or sequence number. In the case when the calculated necessary value matches with the one present in this route update message, then the update carried out. Otherwise, we have that received update is only discarded. Generally SEAD avoids routing loops unless there is more than one attacker in the loop.

Pay your attention that his protocol could be implemented with minor modifications to the certain distance vector routing protocols. Such protocol is robust against multiple uncoordinated attacks. Besides SEAD protocol, despite that, couldn't overcome overcome attacks where any attacker can use the same metric and sequence number that were applied by the recent update message, and also sends a new routing update.

3.2.3. Authenticated Routing for Ad-hoc Networks

Most of the authenticated routing for all ad-hoc networks (ARAN) routing protocol [10, 12], built on cryptographic certificates, is secure routing protocol that successfully defeats all identified attacks in this network layer. Besides it takes care of authentication, certain message integrity, and also non-repudiation, but expects a small amount of prior security coordination between nodes.

Pay attention to the fact that during the route discovery process of ARAN and source node broadcasts certain *RouteRequest* packets. Any destination node, on receiving the *RouteRequest* packets, responds with the help of unicasting back a reply packet on the chosen path. The ARAN protocol can use some preliminary cryptographic certification process. It followed by an end-to-end route authentication process that ensures the creation of secure route.

Typically ARAN protocol assumes that keys are created *a priori* with the help of the server and distributed to all nodes in the network. Such protocol does not specify all specific key distribution algorithms. When joining the network, all nodes receive definite certificate from the trusted server. The certificate received with the help of a node *A* from the trusted server *T* looks like as presented below:

$$T \rightarrow A : certA = [IPA, KA+, t, e]KT- \quad (3.1)$$

In this case, *IPA*, *KA*+, *t*, *e*, and *KT* are represented the IP address respectively of node *A*, the public key for node *A*, the time of this certificate creation, expiry date of this certificate, and the private key for server, respectively.

The most important objective of this end-to-end route authentication process is to ensure that all packets sent from certain source node reach the correct intended its destination. In turn source node *S* broadcasts special *RouteRequest*/*RouteDiscovery* packet destined to the end point node *D*. Besides *RouteRequest* packet contains certain packet identifier e.g. route discovery process (RDP), the source node certificate *S* (CertS), IP address of destination (IPD), the current time (*t*), as well as nonce *NS*.

In this case, *KS*− is the private key of the source node *S*. It is presented below:

$$S \rightarrow broadcasts : = [RDP, IPD, CertS,NS, t]KS- \quad (3.2)$$

When the source sends special route discovery message, then it increases the nonce value. This “nonce” is a counter applied in conjunction with the time-stamp as a means to facilitate reuse of nonce. When a node receives any RDP packet from the source with higher value of this source’s nonce compared with the previously received the RDP packets from same source node. Next, it records neighbor from that it has received this packet, then encrypts this packet using its own certificate, and finally transmits it. Such process is denoted below:

$$A \rightarrow broadcasts : = [[RDP, IPD, CertS,NS, t]KS-]KA-, CertA \quad (3.3)$$

An IN *B*, on receiving RDP packet from a node *A*, deletes its neighbor’s certificate, then inserts its own certificate, and finally broadcasts the packet.

Statistics show that end point node, on receiving necessary RDP packet, then verifies node S’s certificate and also tuple (*NS, t*). Next, it replies with special *RouteReply* packet (REP). The end point unicasts the REP packet to the source node along with reverse path is presented here below:

$$D \rightarrow X : = [REP, IPS, CertD,NS, t]KD- \quad (3.4)$$

where node *X* is end point node *D* neighbor, note that it have originally forwarded RDP packet to the node *D*. Next, REP packet follows the same procedure on its reverse path as as route discovery packet. Any error message is createdin the case when the timestamp or nonce does not meet the requirements orin the case when necessary certificate fails. All error message looks similar to the other packets the difference is that the packet identifier is replaced with ERR message.

Table 3.1 illustrates some comparison between DSR, AODV, and ARAN protocols with reference to their security-related characteristics. As a result ARAN remains robust in the presence of any attacks including securing shortest paths, spoofed route signaling, the

unauthorized participation, the fabricated routing messages, the routing messages alteration, as well as replay attacks [8, 11].

Here we consider security solutions that address a specific security flaw in the AODV routing protocol [11]. AODV as known is on-demand routing protocol where all route discovery process is initiated with the help of sending *RouteRequest* packets only in case when data packets arrive at necessary node for transmission. Generally malicious IN could announce that it has the shortest path to the end point, thereby redirecting all the packets via itself. This is well-known as so called blackhole attack.

Table 3.1.

Comparison of vulnerabilities of ARAN with DSR and AODV protocols

Attacks	Protocols		
	AODV	DSR	ARAN
Modifications required during remote redirection	Sequence number and hop-counts	Source routes	None
Tunneling during remote redirection	Yes	Yes	Yes
Spoofing	Yes	Yes	No
Cache poisoning	No	Yes	No

The blackhole attack is represented in Fig. 3.4. Let node *M* is the malicious node that enters the network. It promises that it has the shortest path to the end point node *D* when it receives the *RouteRequest* packet sent with the help of node *S*. Essentially attacker may not be able to succeedin the case when node *A*, that also receives the *RouteRequest* packet from node *S*, replies earlier than node *M*. But a main benefit for the malicious node is that it does not have to search necessary routing table for a route to the end point. Besides, the RouteReply packets originate directly from the malicious node and not from the end point node. For this reason, the malicious node would be able to reply faster than node *A*, that would have to search its routing table for a route to the end point node. Thus, node *S* may tend to establish a route to end point *D* through the malicious node *M*, allowing node *M* to listen to all packets meant for the end point node.

One of possible solutions for existing blackhole problem is to forbid the INs from originating *RouteReply* packets. Only the end point node would be allowed to initiate *RouteReply* packets. Security is still not completely assured, since the malicious node may lie in the path chosen by the end point node. Besides, delay included in the route discovery process may increas as the size of the network increases. Another possible solution for this problem may be usage of the *RouteReply* packet to receiv from one of the INs, another *RouteRequest* packet will be sent from the source node to the neighbor node of the IN in certain path.

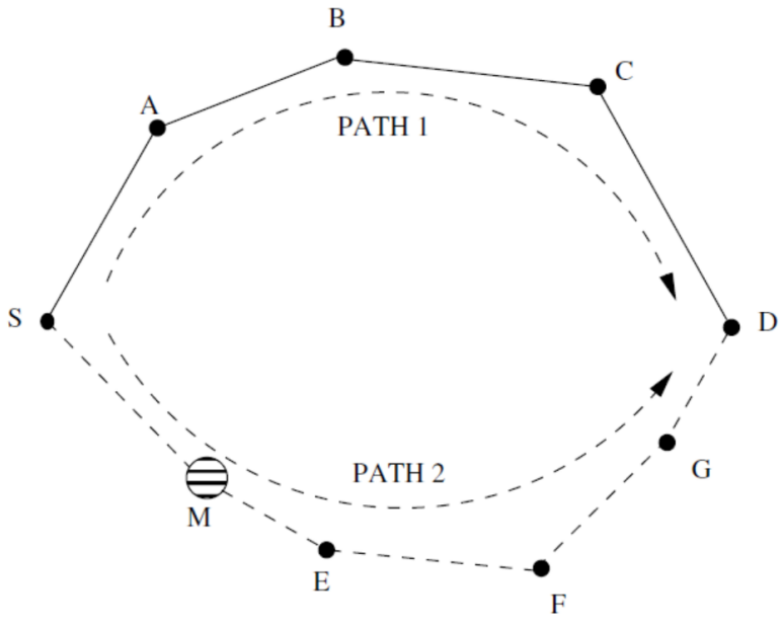


Fig. 3.4. Illustration of blackhole problem

This is to ensure that such a path exists from the IN to the end point node. For instance, let the source node send certain *RouteRequest* packets and in turn receive *RouteReply* via the intermediate malicious node *M*. This *RouteReply* packet of node *M* contains information about its next-hop neighbor nodes. Let it contain all necessary information about neighbor node *E*. In this case, as presented in Fig. 3.5, the source node *S* will send *FurtherRouteRequest* packets to neighbor node (here is node *E*).

In this example node *E* responds by sending a certain *FurtherRouteReply* packet to source node *S*. Considering that node *M* is a malicious node that should not be present in the routing list of node *E*. So, *FurtherRouteReply* packet sent with the help of node *E* will not

contain any route to malicious node *M*. But in a situation when it contains some route to the end point of node *D*, then the new route to the end point via node *E* is chosen, and the earlier chosen route via node *M* will be rejected. Such protocol completely eliminates the blackhole attack which caused by only single attacker.

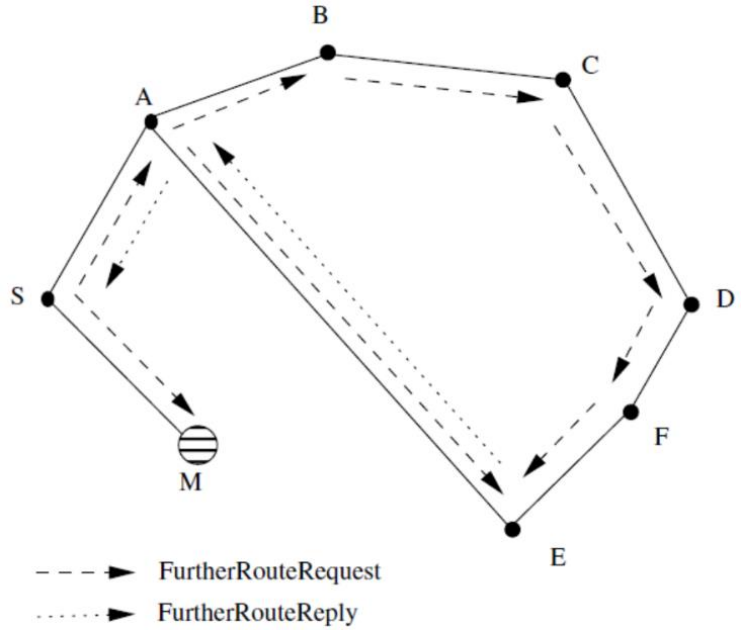


Fig. 3.5. Propagation of *FurtherRouteRequest* and *FurtherRouteReply*

Next Table 3.2 lists out the different attacks possible in present ad-hoc WNs along with the typical solutions proposed for countering those attacks.

CONCLUSION TO CHAPTER 3

This chapter discussed the main problems faces by all transport layer protocol in any ad-hoc WNs. The main goals of developing transport layer protocol have been listed here. Also classification of present transport layer solutions has been provided. Have been noted, that now TCP is the most widely used transport layer protocol. It is considered as basis or backbone of modern Internet.

Table 3.2.

Defense against attacks

Attack	Targeted Layer in the Protocol Stack	Proposed Solutions
Jamming	Physical and MAC layers	FHSS, DSSS
Wormhole attack	Network layer	Packet Leashes [16]
Blackhole attack	Network layer	[25], [29]
Byzantine attack	Network layer	[17]
Resource consumption attack	Network layer	SEAD [26]
Information disclosure	Network layer	SMT [30]
Location disclosure	Network layer	SRP [30], NDM [31]
Routing attacks	Network layer	[19], SEAD [26], ARAN [28], ARIADNE [32]
Repudiation	Application layer	ARAN [28]
Denial of Service	Multi-layer	SEAD [26], ARIADNE [32]
Impersonation	Multi-layer	ARAN [28]

Generally it provides quite reliable, end-to-end, byte-streamed, in-order delivery of all packets to nodes. Considering that TCP was designed to withstand problems present in existing traditional wired networks, many of such prolems don’t connected with dynamic topology networks including ad-hoc WNs. All of this results in reduction of throughput when using TCP in ad-hoc WNs. It’s quite important to use TCP in ad-hoc WNs because it is also important to seamlessly communicate with the Internet anytime and anywhere it is available.

The second half of thesis chapter devoted to some security aspect of communication process in modern ad-hoc WNs. Main problems and existing challenges included in provisioning security in ad-hoc WNs were identified. This was followed by a layer-by-layer classification of the different types of known attacks. Detailed discussions on efficient key management methods as well as secure routing methods for typical ad-hoc WNs were also provided here.

CHAPTER 4
AD-HOC NETWORK SECURITY USING A SELF-ORGANIZED PUBLIC KEY INFRASTRUCTURE

4.1. Problem statement for network security

It is widely known that reinforcing security mechanisms a posteriori can be extremely painful and quite expensive process. Nowadays, security in typical mobile ad-hoc networks is quite dificult to ensure, notably since the sporadic nature of connectivity, the limited physical protection of each existing nodes, the links vulnerability, the some dynamically changing topology, the absence of a certification authority, as well as the lack of a centralized monitoring or some control point.

Clearly, that many security requirements significantly depend on the kind of mission for that the mobile ad-hoc network has been designed, and aslo a medium where it has to operate. For instance, a military mobile ad-hoc network obviously will have extremely stringent requirements in terms of resistance and also privacy to “denial-of-service” attacks. Generally mechanisms to encourage cooperation between several nodes can be highly desirable in the civilian context, although they make little sense in their military context. Besides, anonymity as a rule will be desirable in both civilian and military contexts, but with diferent avors: in respect of the battleeld. Actually it is quite important to hide the location of the headquarters, although in some commercial scenario, consumer may wish to protect his privacy with reference to a given service vendor or provider.

The analysis shows that essentially attacks on the basic mechanisms of the ad-hoc network, including routing. In order to prevent these attacks requires special security mechanisms that are often built on cryptographic algorithms.

Despite that, due to peculiarities of ad-hoc net operations, and its solution requires specific attention.

Unlike nodes of traditional (e.g. wireline) networks, nodes of typical ad-hoc networks cannot be assumed to be secured in special locked cabinets. For this reason, they risk being

captured and then compromised. Some terminals of cellular networks, for instance, have been often stolen or hacked by rogue users, causing losses for operators in the order of millions hundreds of dollars. Because all communications are carried out wirelessly, ad-hoc networks are vulnerable to attacks ranging from eavesdropping to different active interference.

Consider another problem. It related to the previous one is such algorithms are assumed to be cooperative. For instance, in MAC layer, nodes are expected to cooperate. In a contention-based mechanism, nodes must follow the predetermined rules to avoid any collisions or recover from them. Generally in a contention-free mechanism (that is much better suited to typical ad-hoc networks), each node should receive some agreement from all others for an exclusive apply of necessary channel resource. In both of these cases, when a node doesn't follow the rules, the channel allocation will be unfair and thus network performance may be seriously affected.

Actually routing mechanisms are more vulnerable in any ad-hoc networks compared to traditional networks since in ad-hoc networks each device acts only as a relay. For instance, that attacker who takes over ad-hoc node could paralyze the entire network with the help of spreading false routing information. Generally less dramatic but more subtle malicious behavior is node selfishness, e.g. some nodes may be tempted to not relay some packets (such as as a means to save their own battery) [11].

Besides, weaknesses in the protocols can be exploited to detect malicious neighbor. For example, researchers have recently presented how this type of attack can be carried out against current Bluetooth device [12].

In almost any network, the basic security mechanisms require that the users to use appropriate cryptographic keys. Note that main goal of a good cryptographic design is to decrease complex problems to the proper management and also safe-keeping of a small number of cryptographic keys. This goal is quite dificult to achieve in an ad-hoc network (where the some nodes move around and where connectivity as a rule is not guaranteed).

Simple examples of attacks against any security mechanisms are the following situations, such as some keys can be compromised; all public keys can be maliciously

replaced; in the case there is a (only distributed) trusted server or it can fall under the control of an attacker.

All these threats are not specific to typical ad-hoc networks, but such solutions must take into account the features of ad-hoc networks.

4.2. Protection basic mechanisms

A radio interface protection will not be considered in this work (such as jamming or prevention of eavesdropping) since this problem is not really specific to present mobile ad-hoc networks.

4.2.1. Network tamper resistance

Since some device can be captured and hijacked, it must be protected in some way. Generally traditional solution is to protect the device (mayby just part of it) with the help of implementing it in tamper-resistant hardware. A first option would be to embed the cryptographic information (such as secret key) in special smart card that at will could be plugged into and deleted from the node. All SIM of GSM solutions work on this principle.

An additional need is to protect the network mechanisms built into the node (such as routing). The solution here is to store all related software in a smart card. In the case when the smart card is insufficient; a possibility is use security processors which include some memory, processor, as well as appropriate tamper detection circuitry [9, 12]. This can provide more security than the smart card. But there is still quite a problem. Despite that a software package including routing needs to be upgraded from time to time. For this reason, there must be a mechanism by which the operating system can verify the legitimacy of a new software version.

Actually related task is system imprinting: upon initialization, a system needs to communicate in some way to whom and how it has to obey (e.g. who are its users, what is the identity of other devices it is entitled to communicate with and so on).

4.2.2. Routing-based mechanisms for ad-hoc networks

In typical mobile ad-hoc networks, a lot of research has been devoted to routing algorithms. Despite that, in most cases, the nodes are considered to be cooperative. The researchers propose to consider the case where some malicious nodes agree to forward packets but fail to do so [11]. As a means to cope with this problem, they propose 2 different mechanisms. The first is a so-called watchdog, responsible for identifying the misbehaving nodes, and the second is a mechanism, responsible for defining the best route circumventing these nodes.

As an alternative, certain characteristics of ad-hoc networks can be used to achieve secure routing. Generally routing protocols of typical ad-hoc networks have to cope with outdated routing information to match the dynamically changing topology. False routing information created with the help of compromised nodes can be considered as outdated information to some extent. Since the number of correct nodes remains large enough, the routing protocol should be able to find routes that bypass the compromised nodes. Because each routing protocols can discover several routes, all nodes can switch to an alternative route when the primary route fails.

Actually attacker can also try to change existing content of the routing table. The simplest way to prevent such an attack is to avoid these routing tables, and to base all packet forwarding on geographic information [11]. Despite that, this requires that each of the nodes to know its geographic position as well as it is able to share it with others. Therefore other types of vulnerabilities may be created.

4.2.3. Neighborhood and service enforcement

Attacks can be built on the protocols between neighbors, including the hello protocol. With the help of this technique, an attacker can force a victim node to unveil private data, including its identity. Actually, even in the considerably simpler case of cellular networks, where users can depend ontheir home network operator to protect their privacy, many solutions have been proposed, but unfortunately this problem is not yet really solved [6, 10].

Recent research in the framework of Bluetooth, show how the victim's activity can be monitored with the help of set of devices installed in strategic places by some attacker [7].

Also some scientists proposed solution built on pseudonyms: in the case when the identity of a device changes for each session, then it becomes considerably more dificult for attacker to trace its location as well as its activities [7, 10]. Despite that, this leads to increased complexity of the addressing schemes.

In the case when ad-hoc network is self-organized, service availability is a primary requirement. Then 2 questions arise. First question, end-users must be interested in cooperate (for example, in relaying packets for the benefit of other users). Second question, they should be dissuaded from overloading the network. In many mobile ad-hoc networks these 2 aspects relevant due to the small size of the network and the emergency situations where they were expected to be deployed. Besides, the nodes belonged to the same authority should shared same goals.

Actually protection of the models against misuse can be built on a tamper resistant hardware module in each device. Such module would manage the “nuglets” of the node in such a way that this node cannot increase its nuglets “stock” in an illegal way. Besides, this module would also be applied to provide cryptographic protection for packet purses [8, 10].

4.3. Protecting the security mechanisms

Experts show, that protecting security mechanisms for modern ad-hoc network is significant challenge for specialists.

We will focus here perhaps on the most critical and complex problem, namely key establishment. Generally, it can be realized with the help of key agreement or transport key [11-13]. In last case, one party creates or otherwise receives some secret value, and securely transfers it to the other(s). When using key agreement, a shared key is derived with the help of 2 (or more) parties as a function of information provided by or associated with each of these, then in such a way that no party can predetermine some resulting value. Both approaches can be built on SK or AK, and there are a number of well determined protocols to achieve this goal [11].

Generally identification of the appropriate solution in any ad-hoc network will depend mainly on a number of criteria. Actually asymmetric key (AK) cryptography is an

appropriate concept for this case1, since it does not require online trusted servers. Despite that, there is a disadvantage associated with key revocation. The typical scalable mechanism for achieving this goal is for authority maintains a list of revoked keys on a server, so this solution clearly not adapted to our problem. Note that alternative would be to request necessary public key directly from its owner. But all this would have to be realized for each new interaction in special secure way, and for this reason the expected benefits of the asymmetric technique would be lost.

4.3.1. Expediency of using cryptography techniques

Despite this disadvantage, in the rest of our discussion, we will focus only on key establishment using AK cryptography. As a rule in this a system, each node has a private/publickey pair. All public keys can be shared with other nodes, while private keys must be kept confidential to some individual nodes. Critical issue for a given node *A* is how to receive the authentic public key of a node *B*. Actually the most important threat is an intruder-in-the-middle attack [10].

A way to apply AK cryptosystems for transport of the SKs is to encrypt a SK created with the help of one party with the public key of the other party.

As for key agreement, scientists have proposed new key exchange technique built on AK cryptography [9, 12]. In this method, 2 parties wishing to communicate securely begin their interaction with the help of exchanging random values, based on which both compute locally the same key. Present basic version provides protection in the form of secrecy of the resulting key from passive attackers. As a means tothwart active attacks, including the intruder-in-the-middle attack, numerous proposals have been made.

They propose some way to bind the exchanged random values for the parties identities. The main issue is that this requires involving some trusted party. Generally in a self-organized ad-hoc WN, this would require that unique authority play this role. But we think that such assumption is too restrictive for this case.

In point of fact, SK schemes are applied to enable further communication after nodes have authenticated each other and than established special secret symmetric key using AK cryptography.

Note that identity-based cryptosystems are one way to circumvent the issue of binding public keys to identities [9, 11]. In such systems, all entity's public identification information (it has unique name) plays main role of its public key. This allows users to avoid the need to exchange (e.g. certify in some way) their public keys. Another benefit is that no need to store public key certificates directories. Despite that, the disadvantage is that a trusted authority is needed to create private keys of the users. In theory, this trusted authority is required only when configuring the system.

There are essentially 3 types of approaches to eliminate a centralized certification authority in any mobile ad-hoc network. Actually first consists in emulating a conventional certification authority with the help of distributing it on numerous nodes; the second consists in fully distributed solution, where all nodes have to authenticate each other with the help of establishing an appropriate context; we will consider these first 2 options.

4.3.2. Emulation of a certification authority and key agreement

Some authors propose a key management service, which distributed over a certain number of nodes known as servers [13]. In general such service has a private/public pair (here *K/k*). Note that all public key *K* is known to all nodes in this network, although the as a rule private key *k* is divided into *n* shares s_1; s_2; …s_n, one share for each server. Besides each server also has special private/public key K_i/k_i, as well as knows the public keys of all nodes. Then *n* servers are chosen arbitrarily between the nodes of the network.

As a means toprotect itself against the potential compromise of *n* servers, the system applies certain cryptography threshold. Existing (*n*; *t*+1) threshold cryptography scheme (n≥3*t*+1) permits *n* parties to share the ability to perform some cryptographic operation (such as creating a digital signature) as a means, any (*t*+1) parties can perform such operation jointly, although for at most *t* parties this cannot be done even by collusion.

Mobile attackers can gradually compromise all the servers. Proactive schemes are proposed as a means to prevent such attacks. They use share updating that allows servers to jointly compute new shares from old ones, without revealing the service private key to server. In turn new shares constitute a new (*n*; *t*+1) sharing of this service's private key.

This mechanism can be extremely robust against any sophisticated attacks, and is for this reason well suited for many military applications. Despite that, it requires that a subset of some nodes (or servers) play quite specific role at a given point in time, which is undesirable for self-organized civilian networks, where each user is expected to behave "selfishly".

4.3.3. Key agreement

According to researchers, any nodes wishing to establish a secure session should share a prior context [10]. In this case scenario considered by many researchers is quite small group of individuals gather in special meeting room for an ad-hoc meeting (conference) and wishing to set up a WN session between their laptops for the the conference period. One of the proposed solutions is freshing password and then sharing it between everyone present in the room (may be writing it on a blackboard).

Despite that, it would be a mistake to apply such password directly as the key, since protocol would then be vulnerable to repository attacks [8-10]. For this reason, the researchers propose for usage of password-authenticated key exchange. Using it they derive a strong shared key beginning from just weak shared key. This proposal only works in the case when all parties can share some password with the help of being physically present in the same meeting room.

Actually problem of public-key distribution generally speaking can be reduced in the following question: The most famous approach to solve this issue directly depends on public-key certificates. The last one is a data structure where a public key is bound to identity with the help of the digital signature of the issued certificate. In the case when user *u* wants to receive certain authentic public key of user *v*, it obtains special chain of public-key certificates such that the 1-st certificate in this chain can directly be verified with the help of *u* applying a public key that *u* holds and trusts. Note that each remaining certificate can be verified applying certain public key in the previous certificate in the chain. We're supposed to trusts everyone issued certificate *u* in the chain [12].

In many of the known certificate public-key certificates are issued with the help of trusted third parties, called Certification Authorities. This is not a self-organized approach

for obvious reasons, and for this reason, it is not appropriate for self-organized typical mobile ad-hoc networks. In other systems (such as in Pretty Good Privacy (PGP) [11]), certificates are issued with the help of the users themselves; Despite that, the distribution of certificates directly depends on publicly accessible certificate directories that reside on centrally managed servers. For this reason, this approach is not fully self-organized either.

Here new public-key distribution system suitable for present self-organized mobile ad-hoc networks is proposed. Despite that, as opposed to PGP, we do not depend on certificate directories for the distribution of certificates. Instead, in proposed system, necessary certificates are stored and then distributed with the help of the users. Each user maintains a local certificate store containing limited number of certificates chosen by the user according to certain algorithm.

4.4. Selforganized publickey infrastructure

4.4.1. Model and framework

Assume that in the case when user *u* supposes that a given public key belongs only to a given user *v*, then *u* questions a public-key certicate to *v*. Moreover, assume that all users are honest as well as cannot issue false certificates.

Then we need to model the relations between users represented with the help of the public-key certificates as a directed graph G(*V*;*E*), where *E* and *V* denote some sets of edges and vertices, respectively. Denote this graph as “trust graph”. The vertices of this trust graph represent any users and in turn edges represent public-key certificates. More exactly, there is some directed edge from vertex *u* to vertex *v* in the case when user *u* issued certain public-key certificate to user *v*.

Actually any certificate chain from user *u* to user *v* is represented with the help of some some directed path from vertex *u* to vertex *v* in *G* [13]. Here for all directed graph *H*, in the case when 2 vertices *v* and *u* are in *H*, and also there is a directed path from *u* to *v* in *H*, thus *v* can be reached from *u* in *H* and denote here as *u*, *H* and *v*.

Therefore, the certificate chain existence from user *u* to user *v* means that necessary vertex *v* is reachable from the vertex *u* in *G*.

Here in public-key distribution system, each user can maintain some local repository of public-key certificates. It has only 2 parts. First part, when each user stores some certificates that it issued. This is needed as a means to store all the certificates issued in the system in a decentralized way. Second part when each user stores some set of chosen certificates issued with the help of other users in this system. For our model, this means that each user *u* stores necessary outgoing edges from vertex *u* as wll as some set of chosen edges of the trust graph. In this case we refer to the set of chosen edges (and also vertices) as the subgraph belonging to *u*.

In the case when user *u* should to verify necessary public key of user *v*, *u* and *v* merge their repositories of chosen certificates, and *u* looks for appropriate certificate chain from *u* to *v* in its merged repository. Here, *u* and *v* merge their subgraphs, and *u* in turn looks for path from the *u* vertex to the *v* vertex in the merged subgraph, example in Fig. 4.1.

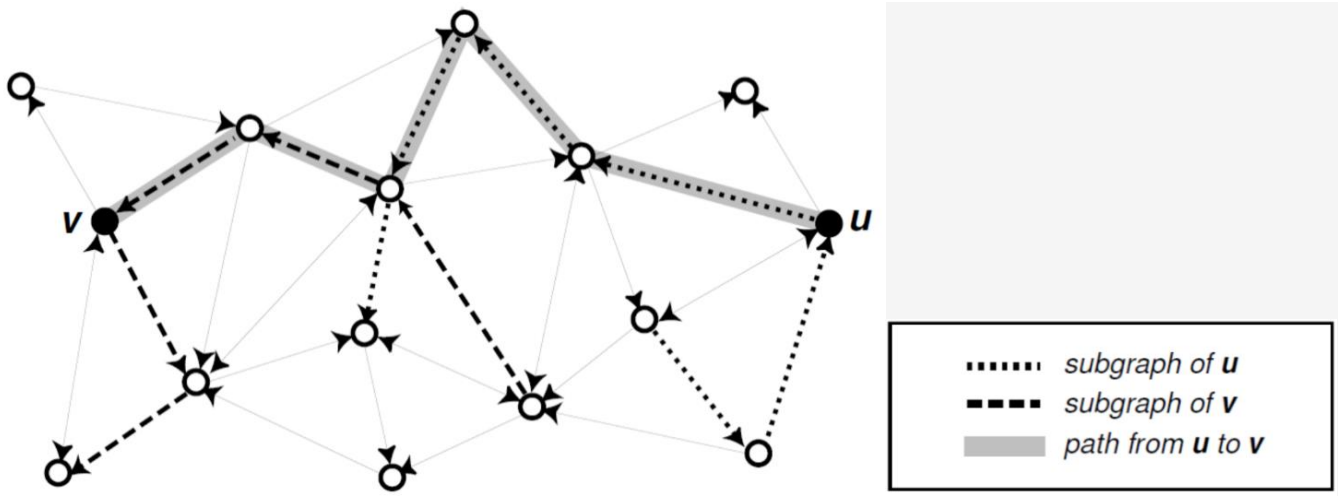


Fig. 4.1. Merging subgraphs

Assume that each user applies certain subgraph selection algorithm *A* to build its subgraph. When *A* is executed on *G* with the help of user *u*, as a result we have subgraph $S_A(G; u)$. The union of the subgraph $S_A(G; u)$ for user *u* and $S_A(G; v)$ of user *v* is denoted using $S_A(G; u; v)$. Given that operation is commutative, so $S_A(G; u; v) = S_A(G; v; u)$.

When user *u* should verify certain public key of user *v*, *u* and then *v* merge their local certificate repositories, and *u* looks for a certificate chain from *u* to *v* in the merged repository. Here, some local certificate repositories are represented with the help of subgraphs

and in turn certificate chains are represented by certain paths. For this reason, in this model, *u* and *v* mix their subgraphs, and *u* looks for some path from vertex *u* to vertex *v* in the mixed subgraph. We determine the performance $p_A(G)$ of this subgraph choice algorithm *A* on the trust graph *G* as the ratio of existing user pairs number of (*u*; *v*) where there is certain directed path from *u* to *v* in the mixed subgraph. Formally, we have:

$$p_A(G) == \frac{\#\{(u; v) \in V \times V : u \sim_{S_A(G;u;v)} v\}}{\#\{(u; v) \in V \times V : u \sim_G v\}}$$

where symbol # here denotes the power of a set. It's clear that, $p_A(G)$ expresses that fraction of the necessary directed paths in *G* can be reconstructed in the case when the subgraphs $S_A(G; v)$ and $S_A(G; u)$ are available when a path between *v* and *u* is requested.

Note that, *A* has other important features. First of all this is chosen size of the subgraphs. Obviously, the performance of *A* can be significantly increased with the help of selecting bigger subgraphs. Another important feature of *A* is the type as well as amount of knowledge required by users to perform it. Additionally, the performance of *A* can be improved with the help of using more information about any trust graph, but the obtaining this information may be dificult or sometimes infeasible. Above all, it is not desirable for each user's subgraph to contain a specific node. Nevertheless, in this case, any 2 subgraphs would intersect in this particular node, and which means the performance of *A* would be high, the security of the system would depend on a single node, and this must be avoided.

For this reason, the design objectives of subgraph selection algorithms are the following [11]:

- Performance;
- Distribution;
- Scalability;
- Robustness.

Clearly, there is no algorithm that is optimal with reference toall objectives.

4.4.2. The Shortcut Hunter algorithm

Generally shortcuts play an important role in reducing the average diameter of “small-world” graphs. Actually shortcut is determined as an edge, when removed the shortest undirected path between some nodes previously connected by that edge becomes strictly greater than 2. With the help of an undirected path is certain chain of arbitrarily directed edges. Given that shortcuts are important in “small-world” graphs, we developed a subgraph selection algorithm, known as Shortcut Hunter. It takes into account shortcuts when constructing certain subgraph.

It's clear that algorithm selects a subgraph that consists of 2 logically distinct parts: first - out-bound and second - in-bound path. The paths are chosen in several rounds. This algorithm begins from vertex *u*, and in each step, it selects an outgoing edge that belongs to the last chosen vertex. Actually, this means that *u* must request the user of the last chosen vertex for a list of its outgoing edges. As a means to make this possible, each user must have information about her incoming edges. For this reason, our algorithm requires that each user is notified whenever another user questions a certificate to her.

The next edge selection and its originating vertex *z* in each step of the presented algorithm directly depend on the number of z's shortcuts. More exactly, in each step, a vertex with highest number of shortcuts is chosen. Actually user *u* can determine the number of its shortcuts with the help of receiving information about all outgoing and incoming edges of its adjacent users.

Below, it is presented a detailed description of used selection of the out-bound path. The in-bound path selection is performed in a similar way. All vertices set as wel as the set of edges of the chosen out-bound path are denoted as $V(S)$ and $E(S)$, respectively. In addition, denote some set of edges of certain trust graph by $E(G)$ and also assume that proposed algorithm is performed with the help of user *u*. The set *N* contains only those vertices of *G* that have been processed but not chosen into this path.

1. Initialization : V (S) := {(u, v)}, E(S) := 0, N := 0, w := u, i := 0

2. T := {(w; z) E(G) : z V (S) and z N}

3. If T = 0, then backtracking :

(a) If w = u, then go to step 9

(b) Add w to N

(c) Take the edge (v; w) E(S)

(d) Remove (v; w) from E(S), and remove w from V (S)

(e) w := v, i := i - 1

(f) Go to step 2

4. Choose the edge $(w; z) \in T$ the terminating vertex z. It has the greatest number c of shortcuts (in the case there are numerous such edges).

5. In the case when $c = 0$, then choose some edge $(w; z) \in T$ the terminating vertex z. It has the greatest number of outgoing edges (in the case there are numerous such edges, then choose one randomly)

6. Add (w; z) to E(S), and add z to V (S)

7. w := z, i := i + 1

8. If i < s, then go to step 2

9. Output the path (V (S); E(S)) and stop

4.4.3. Estimation of Shortcut Hunter

We have analyzed the performance of Shortcut Hunter algorithm using real PGP trust graphs received from the web sites www.cert.org and also www.pgpi.org. Specifically, we discovered quite large strongly connected component in 3 PGP public-key databases, also we considered them as trust graphs. Then performance of Shortcut Hunter algorithm on these trust graphs for different subgraph sizes is presented in Fig. 4.2.

It's clear that Shortcut Hunter performs quite well on the 2 smaller trust graphs evenin the case when the size of the chosen subgraphs is extremely small. For example, when the size of the chosen subgraphs is only 20, the performance here is more than 0.97. This means that in the case when each user stores just 20 certificates (10 in-bound plus 10 out-bound) in its local repository that are chosen using Shortcut Hunter. After that all user can receive and verify necessary public key of any other user, using just the local certificate repositories

of the 2 users, with probability 0.97. Note that algorithm performance on the biggest trust graph is notably worse. Despite that, it illustrates significantly increasing tendency as the subgraph size increases too. Actually pure Shortcut Hunter algorithm builds necessary subgraph that consists of 2 pathes (single out-bound and also single in-bound).

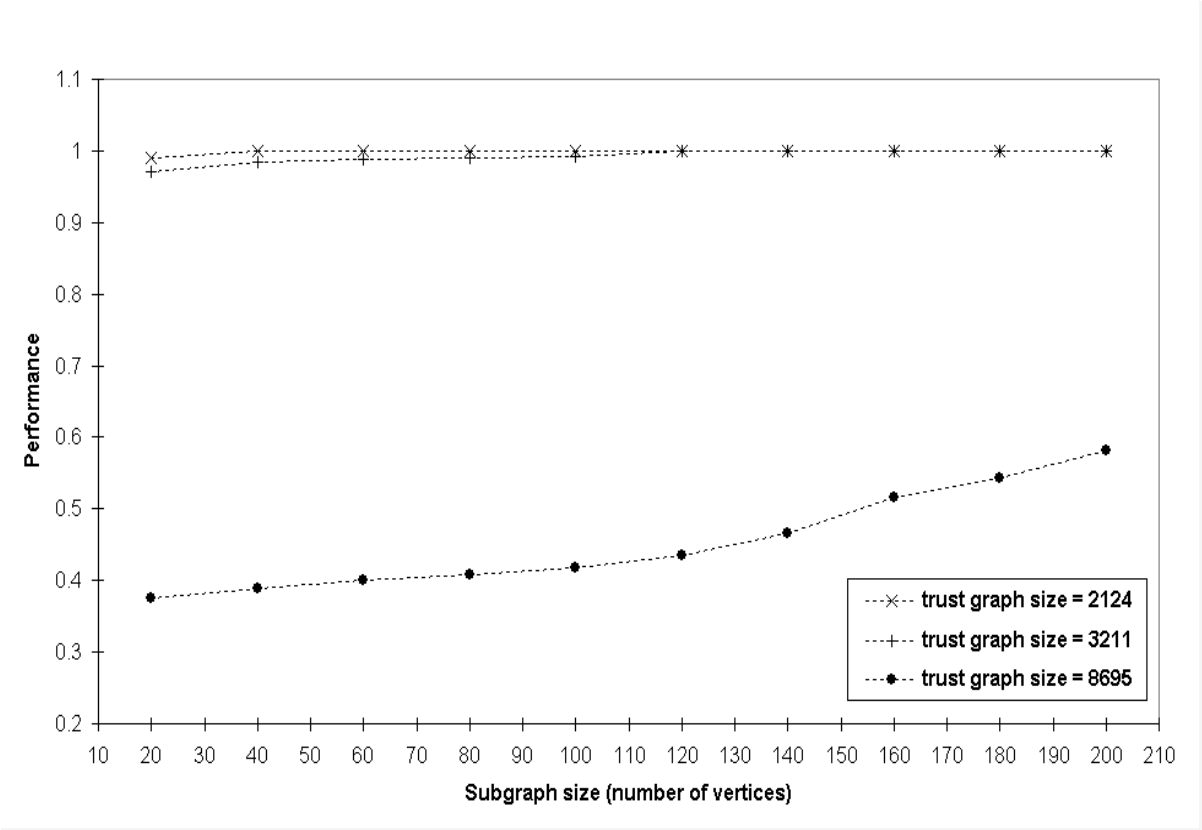


Fig. 4.2. The performance of Shortcut Hunter in real PGP trust graphs

Each path length *s* equal *to* $s=(p_{out} + p_{in})$, where *s* is necessary size of the resulting subgraph. In the case when $c = 1$, then Star Shortcut Hunter is some equivalent to the pure Shortcut Hunter algorithm.

The operation of Star Shortcut Hunter algorithm directly depends on the algorithm described above. That algorithm is completed once to build pout out-bound paths of length. As a means toensure that the chosen out-bound paths are disjoint, and at each execution start, the set *N* is initialized with some vertices set chosen so far, instead of resetting it every time. The choice of the in-bound paths directly depends on similar principles. The performance of algorithm Star Shortcut Hunter for $c = 10$ is presented below in Fig. 4.3.

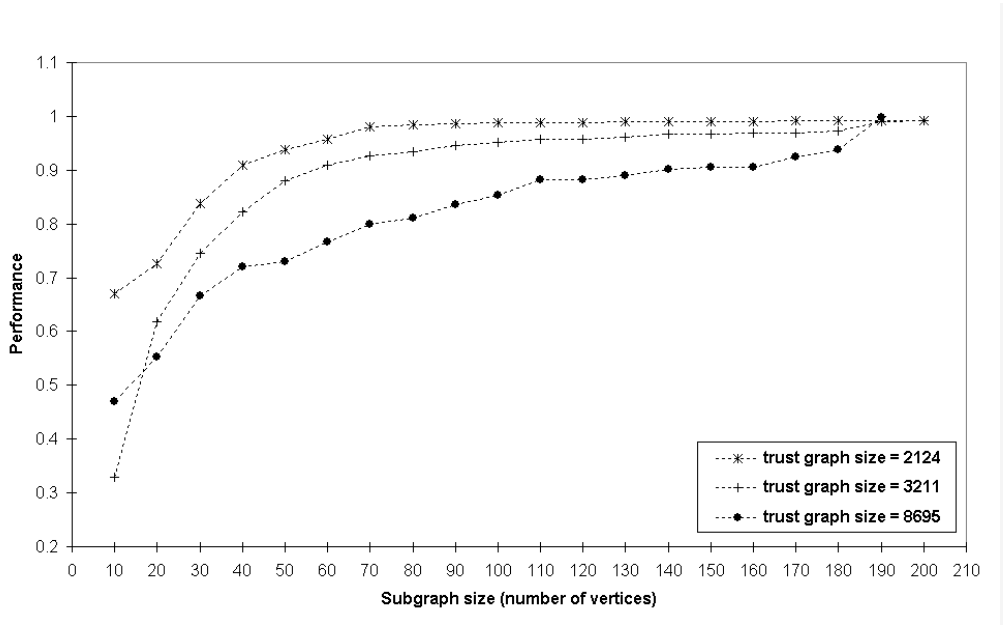


Fig. 4.3. The performance of Star Shortcut Hunter when c = 10 in real PGP trust graphs

It's clear that Star Shortcut Hunter algorithm performs its function better on the biggest trust graph compared to Shortcut Hunter one. Its performance on all 3 trust graphs is more compared to 0.95 when the size of the chosen subgraph is around 2 times the square root of using trust graph size. This illustrates that Star Shortcut Hunter can achieve a high performance, while still being scalable. So user needs information just about the number of shortcuts of the neighbors of the last chosen vertex, as a means to select the next vertex into the subgraph. Despite that, regarding Star Shortcut Hunter robustness, it appears that some vertices are chosen into the subgraphs more often than others.

4.4.4. Dishonest users

Note that each user must be honest and does not problem false certificates. Actually authentication metric is a function μ that takes 2 users (denote as *u* and *v*) and trust graph *G* as inputs, and then returns a numeric value μ(*u*; *v*; *G*). It represents certain level of assurance with which *u* can receive the authentic public key of *v* utilizing the information in *G*. Note that μ can return the number of disjoint paths of necessary vertex *u* and *v* in *G*.

If p_A;μ(G) is near to 1, then we can receive the same assurance with the help of local repositories as utilizing the whole trust graph.

CONCLUSION TO CHAPTER 4

In this chapter the threats as well as some possible solutions for the basic security mechanisms in typical mobile ad-hoc networks were analyzed. In addition, idea of a self-organized public-key infrastructure was here developed. Moreover, our system is quite similar to PGP meaning that public-key certificates are issued with the help of the users. Despite that, as opposed to PGP, method is independent of certificate directories for necessary certificates distribution. Instead of this, certificates are stored and then distributed with the help of the users in proposed system. Algorithm wgich users can apply to build certain local certificate repositories was presentedea. Actually peer-to-peer applications for this algorithm are great example of this.

The analysis performed in this chapter raises broader question. The analysis showed that, it is tempting to think about any mobile ad-hoc networks as self-organized one. The most current example of self-organization system in the field of security is PGP. Despite that PGP has so far remained limited primarily to existing community of computer competent users. Standardization bodies do accomplish very important work in clarifying “building blocks” (including such format as HTML, URLs and HTTP), but no mentioned bodies runs the Web; thus underlying IP network is operated, but the Web unfortunately does not.

CHAPTER 5
LABOR PROTECTION

Introduction.

Present-time labor protection is a system of legislative acts and normative documents of the country. It’s aimed at ensuring labor safety and corresponding organizational, socio-economic, technical as well as sanitary-hygienic measures.

There are no completely safe or harmless productions in the world. So, the main task of modern labor protection is to minimize the probability of different illness or injury of the existing staff. And at the same time provide comfort for existing staff with maximum labor productivity. Real production conditions are usually characterized by the presence of certain hazards or harmful factors.

Now the importance of the people's vital activities safety is determined by the fact that it’s aimed at solving very important social issue. It’s people's health preservation. Real improving working conditions, increasing their safety as well as harmlessness have great importance for environmental now. It affects the economic results of production, such as labor productivity, quality and cost of any manufactured products.

So, the labor productivity increases due to the preservation of human health or working capacity, saving working time at office or enterprises by increasing the level of its usage, extending the period of active labor activity of any person. This is also facilitated by saving the labor of employees by improving the products quality, improving the usage of basic production assets, as well as reducing the number of accidents.

Ensuring safety is a difficult as well as multifaceted process that includes the following protection measures, such as economic and technical, legal and organizational, sanitary and hygienic, medical and preventive [15].

The optimal working conditions at office or enterprises are also determined by the existing socio-demographic composition of the staff and actual enterprise features.

5.1. Analysis of working conditions at the engineer's workplace

5.1.1. Organization of the workplace at the laboratory

The workplaces organization is a constituent element of any labor organization at the laboratory or at the enterprise. This is done for the purpose of creating at each of them the necessary conditions (according to the normative documents of the country) for highly productive as well as high-quality work with as little physical effort as possible and minimal nervous tension of the any employee [15].

The workplace is the primary link of production. It's the area of one or more labor (in the case when the workplace is collective) employees. Such zone is determined on the basis of labor and other applicable norms. Also it's equipped with the necessary means for labor activity. It is clear that the workplace, as a place of person employment, determines the all working conditions (normal, difficult or harmful), modes of work and rest as well as the nature of operation (monotonous, diverse, etc.).

Depending on the specifics of production, workplaces can be classified according to various characteristics, in particular:

- according to degree of specialization (specialized or universal);
- according to profession (for example, the workplace of a design engineer);
- according to the number of operations performers (collective or individual);
- according to the level of mechanization (may be manual, mechanized, automated, hardware workplaces);
- according to the number of serviced equipment (may be single/ multi- machine);
- according to the specifics of working conditions (they may be stationary and mobile, underground or high-altitude, workplaces with harmful as well as dangerous working conditions).

The workplaces organization is a system of activities subordinated to the goals of any production. They are aimed at equipping them with special means or equipment, planning, placing them in a certain order (according to the normative documents of the country), maintenance and, of course, certification. The specific content of such measures is usually

determined by the nature and specialization of the workplace, its type and importance in existing production process.

The equipment of the workplace consists of whole set of the different equipment necessary to perform specific labor functions. It consists of the main technological and auxiliary equipment; as well as organizational equipment (for instance, office equipment, means of communication and signaling, work furniture, different containers along with others); technological equipment (for instance, measuring instruments, spare parts, etc.); working documentation; different means of communication supplying energy to the workplace, information, materials along with others.

In this section of the qualification work, we will consider the engineer workplace.

We will determine the area and volume of engineer room based on the following data:

The length of the selected room L=4,5 м; the width of this room D=3,5 м; and the height of this room H=2,53 м.

So we find the area of this room as:

$$S=L\times D=4{,}5\times 3{,}5=15{,}75 \text{ м}^2.$$

The volume of this room is equal to

$$V=S\times H=15{,}75\times 2{,}53=40 \text{ м}^3.$$

Since the number of employees in the selected room is equal to 1, we can obviously calculate the area and volume of the room per one employee. According to the obtained data, we get S=5.25 m^2 and V=13.33 m^3 , respectively.

Now let's compare the normative and actual values of the parameters of this room and the worker's place in laboratory. The requirements for industrial furniture at workplaces with a personal computer are determined by the current State regulatory legal acts on labor protection DNPAOP 0.00-7.15-18 "Requirements for the safety and health protection of employees when working with screen devices".

After the analysis of the received data, it can be concluded that the selected workplace meets the standards.

5.1.2. The microclimate of production premises

The microclimate in any production premises of the laboratory has a significant impact on the state of the worker's body as well as his working capacity. This means the internal environment conditions in these premises, which affect the heat exchange of workers with an environment. It's known that such conditions are determined by a combination of many parameters, such as temperature, relative humidity and speed of air movement, and the intensity of thermal (infrared) radiation. At the time of this room analysis, the relative humidity was equal to 41%, the temperature was 21°C, and the air speed was equal to 0.15 m/s. The specified parameters satisfy the requirements for the workplace for the cold period of the year for this room (current DSTU B EN 15251:2011 "Calculated parameters of the premises microclimate").

5.1.3. Harmful substances in the air of the working area

Consider the concept of maximum permissible concentration (MPC). This concept means such a concentration of a harmful substance in the working area air, the impact of which on any person in the case of its daily regulated duration does not lead to a significant decrease in illness or work capacity during the period of work activity as well as in the following life period. And it also does not have any negative impact on the offspring health. Note that the working area is considered to be a space 2 m high above the level of the floor or work plane, where the places of temporary or permanent stay of workers are located.

As you know, according to the degree of action on the human body, harmful substances are currently divided into four classes of danger:

– little dangerous (4 class); – moderately dangerous (3 class);

– highly dangerous (2 class); – extremely dangerous (1 class).

This room contains no sources of harmful substances that can cause exceeding the current value of MPC. In this way dust and paper waste can be attributed to the fourth class of harmful substances.

5.1.4. Industrial lighting

One of the factors that determine favorable working conditions is, as you know, rational lighting of the all workplaces. If the lighting of the production premises was correctly calculated and was correctly executed, then the worker's eyes for a long time will retain the ability to distinguish objects and tools quite well, without getting tired. All mentioned above helps to reduce industrial injuries as well as professional eye disease.

Combined lighting was used in this laboratory, i.e. natural (a window with dimensions of 2.5 m by 2.4 m) and artificial.

Industrial lighting must be regulated specifically on working surfaces. Illumination is measured, as you know, in lux. However, regulation of the illumination level by natural light in lux would cause great difficulties, due to the fact that illumination by natural light varies within very wide limits and depends on such parameters as time of day, the year period, cloudiness, which reflects some properties of the earth's surface (grass cover, snow, asphalt, etc.). Before calculating the lighting of any industrial premises, you must [16]:

- determine the lighting system of these premises;
- choose the type of light source and the type of using lamps;
- determine the classification of the premises in accordance with current sanitary standards and illumination standards;
- place the lamps correctly;
- calculate the lighting on all work surfaces;
- specify the required number of lamps;
- determine the unit power of the lamps.

Note that when choosing a lighting system, we take into account issues of hygiene or economy. The selected combined lighting system is more economical and allows creating sufficiently high lighting at workplaces. The general lighting system is much better from the point of view of work hygiene, because it allows us to create quite even distribution of lighting throughout the room, eliminate such parameters as sharp shadows and contrasts. In the future, with the possible growth of energy equipment, general lighting will inevitably have to replace combined lighting that is used today.

When choosing the type of light source, it is natural that preference is given to LED lamps, as the most economical. So LED lamps are used in rooms that are not illuminated by natural light, where it is necessary to have a fairly fine distinction of different colors as well as perform precise work.

When choosing a light source for general lighting of laboratory premises, it is advisable to use such type of lamps:

- for lighting only workplaces where there are increased requirements for color rendering we can used LD lamps type;

- DRL lamps, xenon, sodium types we can use exclusively for lighting open spaces.

The type of lamps is mainly determined by the nature of the laboratory premises.

Lamps in the general lighting system are placed, as a rule, in one row, in several parallel rows, or in a checkerboard pattern, along with others.

Note that a distance from the lastt row of lamps to the wall should also be regulated. When all work surfaces are located along the walls, then such distance should be equal 0.25-3 m; if there are no working surfaces near the walls, then it should be equal 0.4-5 m.

In this room we will use only three lamps. These are energy-saving lamps each with a power of 26 W. They are located in a row at a distance of 0.9 m from each other and from the walls too [17].

5.1.5. Noises and vibrations

Extensive production experience and modern research by medics testify to the adverse effect of vibrations or noise on the body of every person.

As a result of vibration, undesirable changes may occur in the cardiovascular system, central nervous system, in the bone and joint apparatus, muscle strength or weight may decrease, and blood pressure may increase. Spasms of blood vessels and the heart may also appear. In addition, the metabolism, operation of vestibular apparatus, visual acuity as well as light perception, and memory may break down.

It should be noted that the systematic effect of vibration leads to an occupational disease such as vibration disease. Symptoms of vibration disease can cause characteristic pain in the hands, instant whitening of the fingers as well as their numbness. Also it can be

changes in joints, tendons, muscles together with headache, dizziness, increased fatigue. Unfortunately, the treatment is effective only in the early stages of the disease. If the necessary measures are not taken in time, irreversible changes occur in the human body and disability may occur.

It is known that sound affects the human body differently depending on the frequency. This fact is caused both by the physical effect of sound of different frequencies range, and by the individual people sensitivity to different frequencies sounds.

Catch on to the fact that the entire frequency range of acoustic vibrations is divided into three sections, namely ultrasound, audible range sound, and infrasound.

Ultrasonic vibrations generated by low-frequency ultrasound, for example, by industrial equipment, have an adverse effect on the human body. It's known, that ultrasound mainly has a local effect on the body. This is due to the fact that it's transmitted exclusively in direct contact with any ultrasonic instrument. Under the ultrasound influence, fatigue, changes in blood pressure or blood composition, various functional disorders in the nervous system, ear pain, malfunction of the vestibular apparatus occur together with the heating of biological tissues occurs rather quickly appears in the staff [16].

It should be noted that any sound of the audible range can affect the organs of hearing or the nervous system, and thus disrupts its regulatory functions. As scientists have already proven, under such noise influence, blood pressure or heart rhythm are disturbed, headaches and dizziness can appear, visual acuity decreases, as well as gastritis and peptic ulcers occur, also can be hearing loss and professional deafness. Besides, noise leads to a weakening of attention, inhibition of person psychological reactions, which result in increase in the errors number in operation (especially during mental type operation), etc.

A certain level of infrasound can cause a headache, a feeling of vibration of internal organs together with noticeable movement of the eardrums as well as a feeling of horror plus violation of the vestibular apparatus functions.

All noise levels are regulated by the current standard DSN 3.3.6.037-99 "State sanitary standards for industrial noise, ultrasound and infrasound".

In accordance with the specified normative document, all normalized parameters of

constant noise at workplaces are equal to the mean squared value of sound pressures in octave bands with geometric mean frequencies of 31.5; 63; 125; 250; 500; 1000; 2000; 4000; 8000 Hz in dBs [16].

This room in laboratory is equipped with the possible sources of noise and vibration:

- several personal computer
- several laser printer
- one air conditioner.

The analysis of real noise sources showed that all above-mentioned devices are not dangerous sources of noise as well as vibrations, even when all operate in a complex mode.

5.1.6. Electrical safety

Find out that present-day production is inextricably linked with the usage of electricity. In the conditions of any powerful energy systems operation, electric machines together with devices, the present-day level of computer technology development and instrument building, robotization as well as computerization of production, the problem of electrical safety. This problem is the protection of electrical engineering staff and other persons who maintain electrical equipment from possible electric shock.

In this section of the master's thesis the workplace considered has electrical installations, which are sources of potential danger to the health and life of all staff/

Note that the electric current, passing through the human body, can lead to electrolytic, thermal, biological actions together with mechanical actions/

The power supply in the room is carried out, as is known, using a 3-phase network with a voltage value of 220 V (50 Hz).

For connecting portable electrical equipment, it’s recommended to use flexible wires, of course in reliable insulation. Temporary electrical wiring, for example, from portable devices to power sources is performed in the shortest way without any entanglement of wires in the constructions of different machines, devices as well as furniture.

You can increase the length of the wires exclusively due to soldering and with subsequent insulation of the connection points.

To prevent possible electric shocks, special closed sockets as well as switches and factory-made lamps (suspension height is equal to 3.0 m). All these elements, which are used in the all laboratory premises, do not have any normally open current-carrying parts. In all laboratory premises, the inaccessibility of normally current-carrying parts is ensured: first, the wires are located in special vinyl layer pipes with a diameter 50 mm (its wall thickness is 2 mm). They are usually laid with hidden wiring in the floor or walls (APV 2×2.5 is used).

Therefore, it was concluded that the electrical safety conditions in the laboratory workplace meet all the established regulatory requirements.

5.2. Development of labor protection measures

As you know, the workplace and the mutual location of all its necessary elements must meet the different requirements, in particular anthropometric, physical together with psychological. The nature of operation, of course have great importance. Without a doubt, when organizing a programmer's workplace, the following basic conditions must be met, such as optimal placement of the equipment included in the workplace together with sufficient working space. All this allows us to make all the necessary movements.

It is known that the ergonomic aspects of the design of monitor workplaces are such as, for example, the height of the work surface and legroom dimensions, the special requirements for placing documents at the workplace (the possibility of the documents different placement, the presence as well as dimensions of the document stand, the distance from the user's eyes to monitor, document or keyboard, and so on). These aspects also include the different characteristics of the work chair in addition to requirements for the surface of the table using for work, as well as the possibility of adjusting the elements of the laboratory workplace. The basic elements of a programmer's workplace are, of course, only a table and a chair (in addition to computer). Please note that the main working position is the usually sitting position.

As studies have shown such working posture causes, minimal fatigue. It’s known that the workplace rational planning involves a clear order as well as permanent objects

placement, tools or all documentation (Figure 6.1). What is needed to perform the work that is done most often on a daily work is within easy reach of the engineer's workplace.

Let's consider some special terms. First, the motor field is the space of the workplace, where the necessary motor actions of a person can be performed.

Secondly, the maximum reach zone of the hands is only some part of the motor field of the workplace, limited by certain arcs. These arcs coincide with the surface of maximally extended arms when moving them in the person shoulder joint.

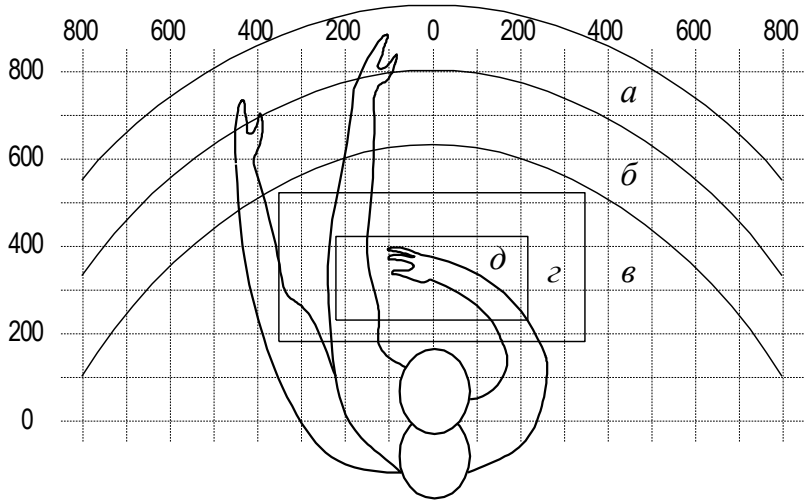
Thirdly, the optimal zone is a such part of the workplace motor field, limited by the arcs described by the person forearm when moving only in the elbow joints with support at the elbow point. at the same time. In this case the shoulders are relatively immobile.

Consider the actions regarding the optimal placement of work equipment and the necessary documentation in the reach zones in this laboratory (fig.6.1):

– display, as the main element, is placed in zone a (in the center);
– system unit is placed in a specially designed table niche;
– keyboard is located in the g/d area;
– "mouse" is placed in the zone on the right;
– printer is located in zone a (right side);
– scanner is placed in zone a/b (on the left side);

Next consider work documentation:

– necessary during work documentation is placed in the area within easy reach of the palm (zone *b*);



a - zone of maximum reach;

b - the reach zone of the fingers with an outstretched hand;

c - zone within easy reach of the palm;

d - optimal space for rough manual work;

g - the optimal space for fine handwork.

Fig. 5.1. Hands reach zones in the horizontal plane

– literature that is not constantly used in daily work is located in the desk drawers (not shown in fig. 5.1).

Fig. 5.2 shows an example of placing the computer peripheral and main components on a programmer's desktop.

As you know, for programmer or engineer comfortable work, the table must meet the following conditions:

- the table surface must have properties that exclude the any appearance of glare in the programmer's field of vision;

- the table lower part should be designed so that the any programmer can sit comfortably without having to press his legs;

- the table height should be chosen taking into account the possibility of sitting freely of programmer or engineer, in a comfortable position, leaning on the armrests if necessary;

- the table design should provide for the presence of drawers (minimum 3 for storing documentation, listings in addition to office equipment).

- the working surface height is recommended within range 680-760 mm. The surface height where the keyboard is installed should be about 650 mm.

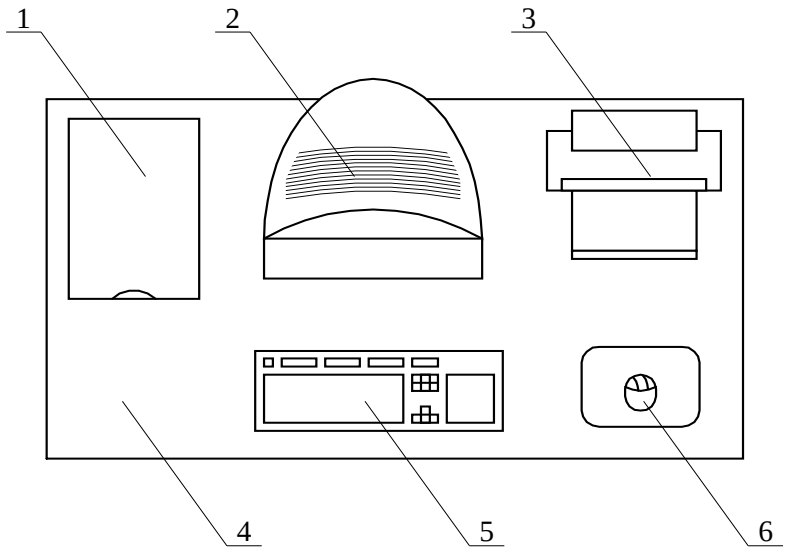


Fig. 5.2. Location of main and peripheral computer components

1 – scanner, 2 – monitor, 3 – printer, 4 – desktop surface

5 – keyboard, 6 – “mouse” type manipulator

Great importance is attached to all characteristics of the engineer work chair. Of course, the recommended value of seat height above the floor level is 420-550 mm. The seat surface should be soft; the front edge is rounded in addition to the adjustable back angle.

At designing stage, it’is necessary to provide for the possibility of documents different placement, such as, on the side of the monitor, between the keyboard and the monitor, etc. Besides, in cases where the monitor has low image quality, for example noticeable flickering, the distance from the eyes to the monitor is made greater (about 700mm) than the distance from the eye to any document (300-450mm). In general, with high image quality on the monitor, the distance from the user's eyes to the screen, document as well as keyboard can be equal.

5.3. Fire Security

Fire prevention is a set of some organizational and technical measures aimed at ensuring the people safety, preventing fires, limiting their spread, in addition to creating conditions for successful fire extinguishing.

Note that in the process of developing preventive measures to prevent fires, the object fire condition is taken into account, as it were the number of fires or their damage, the number of fires, as well as any injuries, poisonings or fatalities, the level of fire safety requirements implementation, the level of combat readiness of fire departments, as well as the state of fire prevention agitation or propaganda.

Fire safety is such object state, which excludes the fire possibility, as well as in the event of its occurrence, the effect of dangerous fire factors on people is impossible as well as the of material values protection is ensured. One of the basic factors in ensuring fire safety is, of course fire prevention.

As you know, insuring the object's fire safety involves some creation of fire prevention in addition to fire protection system. At the same time, organizational and technical measures are of great importance, which now can be conventionally divided into the following:

a) organizational (for example, organization of fire protection, training or briefings);

b) technical (for example, strict compliance with the rules and norms defined by all current regulatory documents, during the reconstruction of premises, production technical re-equipment, electrical networks operation, heating or lighting);

c) measures of a regulatory nature (for example, smoking prohibition and the usage of open flames in unauthorized places);

d) operational (for example, timely preventive inspections and equipment repairs).

In order to prevent all possible fires, their spread and fight against them, all enterprises or organizations employees, undergo training and different briefings on fire safety issues. At facilities with increased fire hazard, training, of course is mandatory.

The fire prevention system is a set of some organizational measures and technical means aimed at preventing the occurrence as well as development of fire. It provides for the detection of the fire initial stage, timely information and, if necessary, the automatic fire extinguishing systems turning on.

Prevention of the appearance ignition source in a combustible environment can be achieved by following all Fire Safety Rules, using electrical equipment that meets the requirements of the class of fire-explosive premises as well as zones, eliminating conditions for self-ignition of materials or substances.

Note that prevention of a combustible environment formation is achieved by complying with the following requirements: first, fire-placement, if possible, of combustible materials or substances in technological processes by non-combustible ones; secondly, isolation of flammable or explosive environments; using different phlegmatizing or inhibitory additives; thirdly, the devices usage for protection against damage or accidents in installations with combustible substances; fourthly, strict control over the air condition in the premises and the ventilation quality.

Next consider fire prevention system. It also provides for reducing the fuel load in the all premises, conducting fire inspections, using safety signs, timely detection of the fire initial stage, transmission of information about the place as well as time of its occurrence and, if necessary, the inclusion of automatic fire extinguishing devices. As you know industrial facilities of categories A, B and C are provided with fire-fighting automation.

5.4. Calculation part

Static electricity is a set of some phenomena associated with the emergence, accumulation as well as relaxation of free electric charge on the surface or in the volume of dielectric or semiconductor materials, substances or products. The appearance of static electricity charges is the result of complex processes of electrons or ions redistribution when 2 dissimilar bodies or substances collide.

Note that static electricity charges can be transmitted or generated (by induction or contact) to the human body. In the case when spark discharges occur, they may cause a physiological effect in the form of a prick or a slight shock. They are not dangerous for humans by themselves (pay your attention, that discharge current is very small). Nonetheless, given the unpredictability of such a discharge, any person may experience fear and, consequently, reflex movement, which in a number of cases may lead to injury (for example, working at height, near moving unprotected parts of equipment).

The systematic influence of any electrostatic field of increased tension as you know has a negative effect on the human body, causing, first of all, functional disorders of the central cardiovascular in addition to nervous systems. According to current DSTU 12.1.045-04, the maximum allowable electric field strength E at workplaces should not exceed value 60 kV/m, in the case when exposure time does not exceed 1 hour; at 1 hour $<t_{infl}$ < 9 hour (field strength E=60 kV/m).

Protection against any static electricity as well as its dangerous manifestations is achieved in 3 main ways. They are preventing the occurrence or accumulation of static electricity, accelerating the flow of electrostatic charges as well as neutralizing them.

Grounding devices, as a rule, made of pipes. These are several metal pipes with a diameter of 25-50 mm and a length of 2-3 m. Grounding devices are driven into the ground at a distance of 4-6 m from each other and, as a rule, connected to each other by special metal pipe. The last one passes into the room, connects to the internal circuit.

The calculation comes down to determining the necessary number of grounding pipes and the length of required metal pipe that connects the vertical grounding pipes.

The following formulas are used to calculate protective grounding

1) Determination of the required number of grounding pipes:

$$H = O_s \times I_s / O_g \times I_e,$$

where O_g –is the required safe grounding resistance (it used for electrical equipment 4 Ом); O_s – the resistance of one grounding conductor; I_s – seasonality factor (1,0 –1,75); I_{sh} – shielding factor (0,9);

2) Determination of the resistance of one grounding device (expressed in centimeters)

$$l = P / L \times 0{,}366 \, (\lg 2L / D + ½ \lg ((4T + L) / (4T\text{-}L)))$$

where L – the length of the grounding pipe (2-3 cm); P – soil specific resistance (10000-30000 Ω/cm); T – distance from the surface to the middle of the grounding pipe (1,6-2,3); D – pipe diameter (25-50 mm).

3) Next step is the determination of the necessary length of the connecting pipe (in meters)

$$L = 1{,}05 \times A \times H$$

where A is the distance between the pipes and H – pipes number.

4) Present the appropriate diagram of grounding devices on a scale according to the all calculations (fig. 5.3).

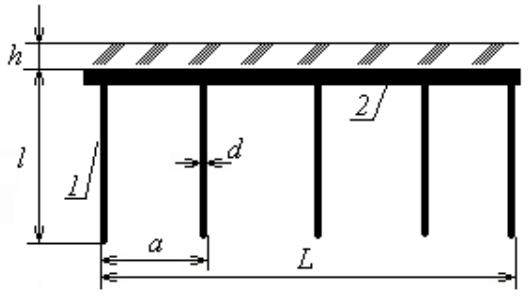


Fig. 5.3. Diagram of the location of grounding devices: 1 – grounding device; 2 – grounding conductor

Grounding calculation. We have the following parameter values:

I_c = 1,0; P = 10000 Ом·с; D = 50 мм; T = 2,3м; T = 3м; $I_е$= 0,9; A = 4м; $O_б$= 4 Ом

1) We determine the resistance of one grounding pipe, as

$O_з = P/L \times 0{,}366 \times (\lg 2L/D + ½ \lg ((4T + L) / (4T-L))) = 10000/3000{,}366 \times$

$\times (\lg 2 \times 300 / 500 + ½ \lg ((4 \times 230 + 300) / (4 \times 230\text{-}300))) = 33{,}3 \times 0{,}366 \times$

$\times$ (lg 120 + 0,5 lg 1,96) =33,3 × 0,366 (2,08 + 0,5 × 0,29) = 27,12 (Ω)

2) Next, we determine the required number of grounding pipes:

$H = (O_з \times I_c) / (O_б \times I_е) = (27{,}12 \times 1{,}0) / (4 \times 0{,}9) = 8$ (pipes)

3) The last step is to determine the length of the connecting pipe:

$L_т = 1{,}05 \times A \times H = 1{,}05 \times 4 \times 8 = 33{,}6 = 3360$ (cm)

CONCLUSIONS TO CHAPTER 5

To comply with the norms of the current legislation of Ukraine in the field of labor protection it is necessary to consider such factors as, for example, the impact of any noise and vibration in the laboratory premises, the correct workplace organization as well as the lighting organization. Special attention should be paid to the electrical safety issues in the laboratory premises because they are the most common cause of different injuries in modern production or in everyday life. Also, special attention should be paid specifically to fire safety systems during the design of the laboratory premises.

Note that violations of labor protection norms are the cause of injury or death. The implementation of existing regulatory documents guarantees the preservation of health and life of personnel.

Having analyzed the state of labor protection for the specified premises of laboratory, it can be concluded that ensuring safe conditions for personnel is possible only in the complex.

CHAPTER 6
PROTECTION OF THE ENVIRONMENT

6.1. Analysis of the technogenic factors impact on the environment

The part of our biosphere, covered by the impact of human activity and its technical means, objects that function or are built, is called the technosphere. It starts to form in the XVIII-XIX centuries with the beginning of the science and technology rapid development. Later, it became a power of a planetary scale from the second half of the 20th century. This is due to the intensification of human activity and the new factors appearance of negative impact on nature. As an example, we can cite the development of nuclear energy or the further development of all transport types. Telecommunication systems and networks also make their contribution to this problem. All this leads to a noticeable increase in pollution of all components of the environment. In particular, these are water and soils, air and the biosphere. In the last one, it led to migration processes due to human production activities. This is how the third type of circulation was formed substances in nature, namely technological. The other two cycles are geological and biological.

Let's consider the main technogenic pollutants of the natural environment. First of all, these are various gases or gaseous substances, aerosols, dust. They enter the atmosphere from various industrial and energy facilities. It also includes electromagnetic, radioactive, magnetic and thermal radiation. In addition, these are noises, fields and vibrations that have been "enriched" with harmful chemical compounds from industry, chemicals [16].

The most dangerous and widespread pollutants include such substances as

- for air - benzene and nitrogen dioxide;
- for water - nitrates and pesticides;
- for soil - hydrochloric acid and polychlorinated diphenyls.

The number of man-made pollutants nowadays is enormous. Unfortunately, this process continues to grow, especially in times of war. The so-called heavy metals, which are increasingly accumulating in the soil, water, as a result get into food products.

Such environmental pollution is recorded annually [18]:

– approximately 22 billion tons of carbon dioxide and 150 million tons of various sulfur compounds are emitted into the atmosphere of the planet as a result of the combustion of various types of fuel;

– global industry discharges harmful substances into rivers more than 160 km^3;

– about 500 million tons of mineral fertilizers as well as 4 million tons of pesticides enter the soil, which is particularly dangerous.

Note that over the past 50 years, the usage of mineral fertilizers has increased by 45 times, and the use of toxic chemicals has increased 10 times. At the same time, the yield increased only slightly (plus 15-20%). But it had a much greater impact on ecology - the pollution of natural soils and waters increased many times [18].

Consider the existing classification of pollutants and environmental pollution:

– by impact on biota - direct and indirect action;

– by origin - mechanical, chemical, physical, biological; material, energy;

– according to the duration of action, we have 4 types, namely unstable, stable, semi-stable and medium-stable;

– according to the nature of the action – intentional, incidental, emergency-accidental.

It should be noted that throughout its entire history, mankind has faced the limitation of natural resources. But, unfortunately, we have not yet realized the consequences of their uncontrolled usage. The modern economy is still extremely bridged in nature. This determines the man-made type of development and depletion of natural resources. That is why the basic task of mankind is to ensure balance in the nature. This problem must be solved on the basis of organizational, technical, legal, socio-economic, sanitary-hygienic, biological methods, etc.

The state of the environment in Ukraine is controlled by several departments. As you know, the main control is carried out by the Ministry of Ecology and Natural Resources. In turn, the Ministry of Health, hydrometeorological service, sanitary-epidemiological services and their departments carry out control in regions and districts. Additional control is carried out by the geological services of the communal economy and subsurface protection, nature conservation societies, "green" organizations, etc. [15].

6.2. The degree of computers environmental danger

The term ecological safety of the environment means of the environment state when it is guaranteed to prevent the deterioration of the ecological situation or the occurrence of danger to human health.

Now it's commonly to classify environmental factors as follows: biotic, abiotic and anthropogenic [16].

Anthropogenic factors include all forms of activity of human society that lead to negative changes in nature, the living environment of other types of the biosphere elements or directly affect the life of the person himself.

The achievements of science and technology, the rapid development of modern technologies, which affect the entire sphere of human activity, require even greater improvement of managing production methods and technological processes, improving the quality and efficiency of production organization.

The wide distribution of microelectronics, computers (PC) and various gadgets, as well as highly efficient devices for their storage and retrieval, modern means of communication and telecommunication networks allow some specialists to ask questions about the prospects for creating electronic offices of the future [16].

The work of operators, programmers and simply PC users is associated with a number of harmful factors that significantly reduce their productivity.

One of the most important tasks in the development of new technologies and production systems is the study and further resolution of existing problems associated with ensuring healthy as well as safe working conditions. It is also important to study as well as identify possible causes of occupational diseases, industrial accidents, explosions, accidents or fires. The development of measures and requirements to eliminate these causes will also be important. All these measures make it possible to create safe and favorable conditions for human work.

It's obvious that one of the main factors affecting the productivity of people working with PCs is safe and comfortable working conditions. In connection with the process of

global computerization of human life, questions arise about the negative impact of the computer on the body. First of all, it affects physical or mental health.

Let's consider the negative factors that affect a person when working with a computer:

1. Electromagnetic radiation (EMR) equipment. This question in the context of the EMR impact on the human body is complex; thousands of scientific articles are devoted to it [15-18]. The results of recent studies indicate the harmful effects of EMR of all wavelength ranges on the human body. Modern monitors, namely liquid crystal monitors, have become much safer for health than monitors with an electro-ray tube. However, there is still low-frequency EMR from transformers, electric motors and other devices that is not shielded. Note that scientists cannot predict the effects of such an impact today. But they warn that in some cases, EMR can lead to significant changes in the body's condition. At the same time, the body becomes more vulnerable to harmful factors of a different nature, including xenobiotics, viruses, etc.

2. Sitting position of a person at a computer. Although the operator is sitting in a fairly relaxed position, it is unpleasant and forced due to the static. As a result, we have tense muscles of the neck, head, arms or back. The result of prolonged exposure is muscle tension or osteochondrosis, and children often lead to scoliosis. We should also note that during prolonged sitting at the computer between the seat of the chair and the body, a thermal compress effect develops. This effect leads to stagnation of blood in the pelvic organs. As a result, you can get a number of diseases that need to be treated for a long time. In addition, a sedentary lifestyle often leads to obesity. Therefore, it is recommended to take breaks to perform physical exercises.

3. Increased load on vision. The human visual system is poorly adapted to the constant viewing of the image on the monitor screen. In addition, looking at objects at a close distance for a long time is harmful. Let's add that the eyes react to the slightest vibration of the text or picture, especially to the flickering of the screen. Congestion of the eyes leads to a rapid loss of visual acuity. We will also note the impact on the stars of the incorrect location of the screen, the unsuccessful selection of fonts, colors, and the layout of programs windows.

4. Unergonomic workplace. Here we pay attention to the quality of lighting at the workplace. Here, the light field should be evenly distributed over the entire plane of the

working space, and the light rays should not fall into the eyes directly. Choose a monitor with good characteristics, configure it correctly, use licensed programs. To reduce the negative impact of the PC on the eyes, it's recommended to take breaks for eye exercises. There are also special computer programs designed to relax the eyes. But the effectiveness of their usage has not yet been proven.

5. The appearance of stress in case of information loss. Not all users regularly make backup copies of all important information. Literary sources [15-18] provide statistics on the occurrence of heart attacks and strokes among a fairly young population due to stress. This is caused, among other things, by the loss of important information.

6. It was found that the effect of long-term work at the computer leads to changes in the immune, nervous, endocrine and reproductive systems, affects the eyesight and the entire musculoskeletal system of a person. Usually, such long and persistent changes cause harm to the body.

Nowadays, the lifespan of modern electronic equipment and telecommunication systems is rapidly decreasing. As a result, we have an aggravation of the problem of electronic waste. Therefore, humanity faces the problem of disposing of obsolete or defective equipment that cannot be repaired. There are many reasons why such equipment cannot be simply thrown into the trash can, starting from the correct write-off of material values and ending with issues of environmental safety.

Electronic waste does not rot, it cannot be burned, due to the presence of heavy metals or poisonous substances. Therefore, special technologies are needed for its processing. Ukraine aspires to be a real European country and takes measures for the competent and civilized disposal of electronic waste. For Ukraine, the problem of electronic waste processing is very acute. Especially these problems increased due to military operations.

The growing threat of ecological imbalance in our time obliges people to look for ways of equipment efficient usage, its preservation and recycling of used resources. In particular, some European countries have already adopted a law prohibiting the emission of used cartridges. A unified environmental policy has been developed in the Europe. This is the basis for the development of pan-European legislation on environmental protection and

rational usage of natural resources. This also applies to the correct disposal of telecommunications equipment.

Literary sources [15-18] note that electronic waste is increasing every year. In Germany, in particular, in 2018, more than 800,000 electrical appliances and computers that were outdated or failed were thrown away. Every year in this country, 2.2 million different office equipment is thrown away. A large variety of household appliances should also be added to them. Now every 6 months, new models of electronics are coming to the market. As you know, the average German citizen pays from 15 to 30 euros depending on the model to dispose of his computer. The situation may change radically with the adoption by the European Union of new rules for the disposal of electronics.

In Ukraine, outdated equipment has been stored at enterprises for years. In accordance with the legislation of our country, personal computers, printers, scanners are classified as basic equipment in the Disposal Rules. They are subject to accounting with an indication of the amount of precious metals contained in them. In addition, the depreciation rule applies to this equipment for 4 years. Thus, there are problems regarding write-off and disposal before this term, although this technique is actually already obsolete or not used. That is why outdated computers and printers accumulate in offices and companies.

6.3. Ecological measures to protect the environment

Consider the requirements for a video terminal device (VTD) and a computer, as an important part of the telecommunications system.

The design of the VTD should provide for the presence of buttons for adjusting the brightness and contrast, which provide the possibility of adjusting the specified parameters from minimum values to maximum values.

According to ergonomic requirements, the design of the monitors should provide for coloring in calm soft tones with diffuse scattering of light. Modern monitor designs can provide the possibility of frontal observation of the screen by rotating the body in the horizontal plane around the vertical axis within ±30° and in the vertical plane around the horizontal axis within ± 30° with fixation in the given position. It is recommended for

monitor and PC cases, the keyboard to be made with a matte surface of the same color with a reflection coefficient of 0.4 - 0.6 and without shiny parts that can create reflections.

According to the modern regulatory framework, VTD and PC must ensure the power of the exposure dose of X-ray radiation at any point at a distance of 0.05 m from the monitor at any position of the adjustment devices must not exceed 7.74×10A/kg, which corresponds to the equivalent dose, i.e. 0.2 mrem/h.

It is also desirable to have an antistatic coating on the monitor screens. It prevents the appearance of an electrostatic charge on the surface of the screen. This reduces the appearance of dust and does not have a favorable effect on the health of the user.

Another novel environmental problem is the accumulation of electronic waste. Europe's environmental policy is connected with the adoption and implementation of 6-th Environmental Action Programs. In these documents, considerable attention in the EU is paid to the legal protection of the environment from waste. In addition, to improve the coordination of scientific research of EU participants in the field of environmental protection, measures have already been taken to create a single scientific space.

Recycling of computers can be carried out only by special organizations. This is due to the fact that monitors and computer system units contain valuable metals. According to the current complex procedures, valuable materials (in particular, non-ferrous, ferrous and precious metals) are returned to the production cycle, while others go to special processing. Note that the enterprise must obtain a permit for independent processing. Otherwise, help from a professional organization is needed.

In accordance with the legislation of Ukraine, legal individuals must contact one of the specialized enterprises for the write-off and disposal of equipment and office equipment. These enterprises are engaged in the production, repair and maintenance of equipment. They also carry out examinations (upon request) to obtain a conclusion that certain equipment is morally obsolete, has already been discontinued and is not subject to repair.

Only after such a conclusion can a contract be concluded with the appropriate organization on equipment disposal.

As you can see, the process is quite confusing and complicated, but this is the official procedure for the disposal of office equipment for companies that want to avoid conflicts

with current legislation. It goes without saying that disposing of equipment costs money. However, such costs are unavoidable and help to protect the environment.

As already mentioned above, in Germany for the disposal of an old PC it is necessary to pay from 15 to 30 euros (depending on the model). In Japan, the cost of recycling one PC is higher and is $40. In Ukraine, such a fee for recycling one computer is about UAH 100. According to reference data [15-18], modern personal computers contain non-ferrous and ferrous metals (Cu – 0,1-0,2 kg, Al – 0,1-0,4 kg, Fe – 3-4 kg), valuable materials, (Ag – 0,8-1,1 g, Au – 0,053-0,072 g), as well as polymers and glass. There are enterprises in Ukraine that are engaged in this. Note that the cost of such processing and extraction of valuable metals exceeds the value of the metals themselves. But such procedures improve the state of environmental ecology.

6.4. The usage of waste as secondary material resources

Industrial wastes in terms of its chemical and mineral composition, as well as properties, are quite close to natural raw materials. Therefore, they can be used as full-fledged substitutes for natural raw materials.

Reuse of cadmium. Depreciation scrap is cadmium-plated parts of discarded motor vehicles, cadmium batteries, aircraft, home or office electrical appliances, metal products or fasteners. Nickel and cadmium alloys are also included in the contacts of switches and relays, which are widely used in telecommunications.

To reuse cadmium, the following procedures must be carried out:

- Preliminary waste treatment. This stage includes degreasing of alloyed alloy vapors. These vapors are formed as a result of heating the disposal solvents. Then they pass through the scrap tank. The fat is condensed and separated, and the solvent itself can be reused. Harmful factors present at this stage are solvents and cadmium dust.

- The next stage is melting and cleaning. After preliminary treatment, alloy waste or cadmium scrap is processed. This is done to eliminate any impurities and obtain a pure cadmium alloy or elemental cadmium. Exposure to oily and gaseous combustion products, zinc and cadmium dust is dangerous at this stage.

- The third stage is distillation in a retort. The degreased waste alloy is loaded into a retort and heated to form cadmium vapor. These pairs are collected using special devices - condensers. Condensed metal is ready for casting. At this stage, harmful effects of cadmium dust on workers are possible.

- The fourth stage is the management and removal of the zinc alloy. Cadmium metal is melted in a special crucible. Fluxes and substances with chlorine are added to remove zinc. At this stage, vapors and dust of cadmium and zinc, zinc chloride, chlorine, hydrogen chloride are potentially dangerous. High temperature is also a dangerous factor for workers.

- The last stage is casting. Casting produces the necessary range of products from purified cadmium alloy or cadmium metal. Harmful factors at this stage are dust, cadmium vapors, high temperature [17].

Reuse of silicon. It is known from literary sources [17] that silicon wafers are the starting material for the production of modern electronics (semiconductors). According to some estimates by company IBM, about 250,000 of these wafers are processed by factories around the world every day. It should be noted that about 3.3% of this number are plates with defects. And of course, according to the results of the product quality check, they have to be sent to waste (disposal).

In addition, the processed plates can be used for the manufacture of solar cells. For this task, "monitors" are also used, which have done their work. According to the estimate of the well-known company IBM, the total power of solar cells that can be made from all these plates is 13.5 MW ("monitors" rejected during the year were taken into account). It should be noted that so far solar batteries produce significantly less than 1% of the total amount of electricity consumed by humans. In recent years, this energy sector has shown steady growth of 30-40% annually. This energy sector has become the second largest consumer of refined silicon wafers. The last one is a material for which high temperatures and significant energy consumption are required. In the future, it may come to the point that the lack of raw materials will prevent the further spread of solar batteries.

The reuse of such plates has been practiced before. But previously, the preparation of plates required the use of acids, which was disadvantageous. This was due to a rather high cost, as well as additional environmental issues regarding production indicators. The latest

technology, developed at company IBM, now replaces chemical etching with mechanical grinding [18].

Reuse of nickel from radio elements and magnetic wires. t's known, that nickel-based alloys are the main raw material for recycling nickel. Depreciation scrap is usually defective parts of cars or airplanes, new scrap is lathe shavings, thin-sheet scrap or solid materials. All mentioned above are by-products in the production of alloy products. It also includes anodized electrodes, magnetic conductors and powerful magnets.

To reuse nickel, the following procedures must be carried out:

- The first stage is waste sorting. Nickel-containing materials are separated from other materials by hand. During sorting, dust may have a harmful effect on the health of personnel or the environment.

- At the second stage, degreasing takes place. Scrap is degreased with trichlorethylene. By filtering or centrifugation, nickel waste is separated. Next, the spent solution of trichlorethylene and lubricants passes through a specialized regeneration system. At this stage, the main danger lies in contact with the solvent.

- Next, the material enters the melting furnace. The furnace can be a rotary, chopper or electric arc furnace. A reducing agent is added to the molten scrap. Lime is usually used as a reducing agent. The metal obtained as a result of melting is cast into molds. Then it is sent to the reactor for additional purification. At this stage, harmful factors are noise, dust, vapors and high temperature

- The fourth stage is refining. Molten metal is fed into a special reactor. Hard scrap and flake nickel are also added there. Then comes the turn to add lime, silica. And only at the end are alloying materials added, in particular niobium, manganese or titanium. In this way, an alloy of a given composition is obtained. At this stage, harmful effects are associated with dust, vapors, high temperature and noise.

- The last stage is keeping the ingots. Molten metal from a melting furnace or a reactor for refining is poured into special forms - castings. After cooling, the ingots are extracted in the required manner. At this stage, the harmful factors are high temperature and metal vapors.

CONCLUSIONS TO CHAPTER 6

The section analyzed the impact of various man-made factors, in particular telecommunication systems, on the environment. Next, the degree of environmental danger of computers is assessed.

Ecological measures to protect the environment, in particular the usage of waste as secondary material resources, are also considered.

CONCLUSION

In the thesis, an analysis was carried out and recommendations were made for further improvement of their protection in the work process.

First, the fundamental principles, aspects of wireless transmission, which include the characteristics of a wireless communication channel, various modulation mechanisms, multiple access methods, and coding, are briefly reviewed. A wireless channel is sensitive to various transmission disturbances such as path loss, jamming, and jamming. These factors limit the range, data rate, and reliability of wireless transmission.

The need for constant monitoring of errors during the transmission of digital parcels is indicated. The main concepts and principles related to computer networks, which are the prototype of wireless radio networks created on the basis of the IEEE 802.11 standard, were also discussed.

It is noted that Bluetooth technology provides connection between devices without the use of base stations, which formed the basis for the creation of ad-hoc communication. During Bluetooth communication, devices can be authenticated and the link can be encrypted using the generated public secret key.

In an ad-hoc wireless network, in contrast to ad-hoc networks, routing and resource management are performed in a distributed manner, in which all nodes are coordinated to ensure communication between thems. This requires each node to be more intelligent, so that it can function both as a network host to transmit and receive data, and as a network router to route packets from other nodes.

Aspects of communication security are considered in detail in peer-to-peer wireless networks, with layer-by-layer analysis Classification of various types of attacks. A detailed discussion of key management technology and safe routing methods for peer-to-peer wireless networks provided. Various attacks possible in peer-to-peer wireless networks are listed as well as solutions proposed for countermeasures to these attacks.

The main methods used to overcome attacks are considered. Cryptography is one of the most common and reliable means of ensuring security. Encryption and decryption

processes are governed by keys, which are small amounts of information used by cryptographic algorithms. The four main goals of cryptography are defined - confidentiality, integrity, authentication (the recipient must be able to identify the sender and verify that the message really came from this sender) and non-repudiation.

The problem of providing secure routing in ad-hoc wireless networks is considered. Unlike traditional cellular networks, in the absence of dedicated routers, ensuring security becomes difficult. The main issues were analyzed: Requirements of a Secure, Security-Aware and AODV of ad-hoc routing protocols, secure efficient ad-hoc distance vector and authenticated routing protocols. At the same time, the general requirements of a secure routing protocol for ad-hoc networks are defined as: detection of malicious nodes, guarantee of correct route detection, confidentiality of network topology, resistance against attacks.

The idea of a self-organized public key infrastructure, where public key certificates are issued by users, is developed. However, unlike PGP encryption operations, it does not rely on certificate directories to distribute certificates. Instead, certificates are stored in our system and distributed by users.

Two algorithms are considered that users can use to create their local certificate stores, and any pair of users can find certificate chains for each other using only their local certificate stores with high probability. The size of local certificate stores is small compared to the total number of users in the system. Although the most relevant example of self-organization in the security area is PGP; however, PGP remained limited primarily to the computer literate user community.

In this way, in the qualification work, all the tasks assigned to it have been completed. The results can be used as reference material for training courses on network technologies.

REFERENCES

1. IETF MANET Working Group Information [Електронний ресурс] – Режим доступу до ресурсу: http://www.ietf.org/html.

2. Kannan Govindan, Deepthi Chander, Multihop Mobile Wireless Networks, River Publishers, 2018.

3. Akyildiz, X. Wang, W. Wang, Wireless Mesh Networks: A Survey, ComputerNetworks and ISDN Systems, Vol. 47, No. 4, 2015.

4. H. van den Berg, M. Mandjes, F. Roijers, Performance Modeling and Analysis of a Bottleneck Node in an IEEE 802.11 Ad-hoc Network, AdHoc-Now, 2006.

5. J. Bicket, Architecture and Evaluation of an Unplanned 802.11b Mesh Network,ACM Mobicom, 2015.

6. K. Chen et al., Understanding Bandwidth-Delay Product in Mobile Ad HocNetworks, Elsevier Computer Communications, Vol. 27, No. 10, 2014.

7. C. Chiasserini, M. Garetto, Modeling the Performance of Wireless Sensor Networks,IEEE Infocom, 2018.

8. J. Chang, L. Tassiulas, Maximum Lifetime Routing in Wireless Sensor Networks, IEEE/ACM Transactions on Networking, 2018.

9. N. Asokan and P. Ginzboorg. Key agreement in ad-hoc networks. Computer Communications, 2015.

10. Tzonelih Hwang. Scheme for secure digital mobile communications based on symmetric key cryptography, Volume 48, Issue 1, 2016.

11. C. Boyd and A. Mathuria. Key establishment protocols for secure mobile communications: a critical survey. Computer Communications, 2017.

12. L. Butty_an and J.-P. Hubaux. Enforcing service availability in mobile ad-hoc networks. In Proceedings of MobiHOC, 2016.

13. J.-P. Hubaux, T. Gross, J.-Y. Le Boudec, and M. Vetterli. Toward self-organized mobile ad-hoc networks: The Terminodes Project. IEEE Communications Magazine, January 2011.

14. Охорона праці [Електронний ресурс] – Режим доступу до ресурсу: http://opcb.kpi.ua/wp-content/uploads/2014/08/Binder21.pdf.

15. С. В. Лукащук-Федик, Безпека життєдіяльності, навч. посіб., Тернопіль, 2018, 162 с.

16. Протоерейский А. С. Безопасность труда в авиации: Конспект лекций К.: КМУГА, 2000. -288 с.

17. Б. В. Дзюндзюк, Охорона праці. Збірник задач. Навч. посібник, Харків, 2018, 236 с.

18. Ісаєнко В. М., Криворотько В. М., Франчук Г. М. Екологія та охорона навколишнього середовища. Дипломне проектування: Навч. Посіб – К.: Книжкове вид-во НАУ, 2005. – 192 с.