The Model of the Attack Implementation on Wireless Sensor Networks

Victoria Korzhuk, Irina Krivtsova, Ilya Shilov
ITMO University
Saint Petersburg, Russia
{vika, ikr}@cit.ifmo.ru, ilia.shilov@yandex.ru

***Abstract*—The article presents a method of wireless sensor network attacks modelling. The main ways of attack committing are briefly described. The existing modelling environments are analysed to select the most appropriate tools for model creating. In order to simplify software implementation of the model of attacks on the ZigBee wireless sensor network, the main parameters of the packet transmission at the physical layer for different frequency bands and signal modulation schemes in accordance with the standard IEEE 802.15.4 are calculated. Based on these data, the basic assumptions and limitations for the model are introduced. A software model of implementation of the various attacks on integrity and availability in wireless sensor networks based on OMNeT++ simulator is realized. Two topologies: mesh network and cluster tree are presented. For each topology its own addressing scheme and routing is provided: AODV for mesh network and domain addressing for the clustered tree. The experiment connected with the count of all packets and route packets in consecutive intervals is conducted. The described model may be used to obtain statistical information about the interactions in the wireless sensor network and about the attacks on such network.**

I. Introduction

The Internet of Things, based on the application of wireless sensor networks, represents one of the most promising directions of information technology development. Due to the proliferation of such systems more and more attention is paid to safety of its functioning.

All the existing threats are classified according to such properties of information security as confidentiality, integrity and availability. Confidentiality threats represent the interception and analysis of the information signal transmitted through the environment. Integrity threats include various ways of alteration in the transmitted packets at the network layer of the Protocol stack or violation of the integrity of the information transmission path. Examples include selective forwarding, when the network router discards part of passing packets, and spoofing – generating of fake packets in which the sender node indicates as any node in the network. Availability threats comprise the noise of the transmission environment (i.e. certain frequency range) and different ways of «denial of service» emergence.

Prevention of threats of information confidentiality and integrity is carried out using the methods of cryptographic protection: encryption the forwarded traffic, usage of the checksum and authentication fields in the headers of packets and frames.

To ensure availability some problem-oriented methods are applied. For example, to protect against the «funnel» attack it can intentionally be used the high speed connection between nodes located far enough from each other. The same approach can be used to perform the «wormhole» attack.

The detection of abnormal activity of wireless sensor networks is significant from the point of view of information security. Many of the integrity threats (routing integrity) and availability threats can be detected by analysing the statistics of network communication. First and foremost, this refers to the statistics of the network layer of the Protocol stack, on which the data routing is carried out and, consequently, the possibility of route availability and integrity harming appears for the first time.

To obtain the statistics it is necessary to construct of an adequate model of carrying out the attacks on the network layer of wireless sensor networks. In this paper the network layer of the Protocol stack of ZigBee is considered. The main criteria for selecting of this technology were:

1) The existence of various permissible network topologies, in particular, mesh network and cluster tree;
2) The existence of specifications of application layer of Protocol stack that allows creating decentralized applications based on wireless sensor networks;
3) The existence of separate standards for different levels of the Protocol stack: link and physical layers use IEEE 802.15.4 and network and application layers use specification of ZigBee.

The use of existing implementations of certain parts of the Protocol stack of ZigBee is not possible for the following reasons:

1) The part of the implementations is presented in the projects with a proprietary license and closed source. It excludes the possibility of attacking nodes creating without performing a reverse analysis of the project code;
2) Some frameworks present a simplified implementation of IEEE 802.15.4 with TCP/IP superstructure as a much more common and widely used;
3) Existing academic implementations of separate parts of the ZigBee technology are aimed at studying the energy efficiency of the modules and the correctness of the used protocols. In this situation only the most simple network topologies, such as «star», «tree» and «point-

to-point» are implemented, which, although applied in practice, represent only a special case of wireless sensor networks, precluding the possibility of carrying out many attacks which are possible in networks with the «cluster tree» and «mesh network» topology.

II. Analysis of modeling tools

There is a large number of simulation and network modelling tools. AnyLogic, OMNeT++, ns, OPNET, NetSim and GNS3 are used more often. Its comparative characteristics on the basis of criteria that are important from the point of view of development of wireless sensor network attack implementation model are given in Table I. OMNeT++ modelling environment was chosen to form the model. The determining factors were the license, programming language and integrated development environment.

TABLE I. Comparison of the modeling tools

	OMNeT++	NetSim	ns	AnyLogic	GNS3
License	Academic	Proprietary	GPLv2	Proprietary	GNU GPL
OS	Linux, Unix, Windows (MinGW), Mac OS	Windows	Linux, Unix, Mac OS	Windows, Linux, Mac OS	Windows, Linux, Mac OS
Type	Library and framework	Simulation tool	Simulator for discrete-event modelling	Simulation tool	Emulator of network interactions
Function	Network model creating	Network model creating	Network model creating	Simulation model creating	Network model creating
Development language	C++	C	C++	Java	-
IDE	+	+	-	+/-	-
Visualization	+	+	+	+	+
ZigBee implementation	-	-	-	-	-

III. Goals and limitations of modeling

As it was noted earlier, the main purpose of wireless sensor network attack modelling is to obtain statistics of network interactions. Significant attention should be paid to the specification of modelling of the processes occurring both within individual nodes and in the network as a whole.

Assumption 1

In the model it is assumed that the transmission speed between any two nodes (through one hop) is the same. Wherein the algorithm for the mesh network route constructing uses the criterion of the number of transitional nodes to the destination node. This method is often used in practice.

Let us consider two networks with the same:

1) topology;
2) number of nodes;
3) average frequency of new packets generation;
4) frequency range (and as a result, the same transfer speed).

Let the maximum number of network packets transmitted in the network during time t is k. Suppose that in time t the first network generates k packets and the second network generates k+m packets. Statistics gathering is working in the network: every N×t units of time, for example, the total number of packets transmitted in the network during this time is recorded. The dynamics of the network is presented in Table II. Given values for the time N×t are derived by means of the method of mathematical induction.

At the time N×t the accumulated statistics is recorded. The sample contains only those values that were obtained on the basis of really transmitted packets; number of packets in the queue is ignored.

TABLE II. The dynamics of the work in dependance on the packet generation frequency

Time	Network 1			Network 2		
	Generated	Transmitted	Queue	Generated	Transmitted	Queue
t	k	k	-	k+m	k	m
2×t	k	k	-	k+m	k	2×m
…	…	…	…	…	…	…
N×t	k	k	-	k+m	k	N×m

Therefore, to achieve the objectives of simulation modelling it is not necessary to describe in detail the process of data transmission through the environment. If the number of packets exceeds the maximum allowed for the data characteristics of the network, the excess will be placed in the queue; the statistics would be the same as in situation when the characteristics allow transmission of all packets to the destination node.

In other words, from the point of view of the network packet statistic collector, the network working with a maximum frequency of packet generation and the network exceeding this frequency look similar. It should be noted that for correct construction and usage of the model with this assumption it is necessary to estimate the maximum allowable average frequency of packet generation.

Assumption 2

The frequency of packet generation is understood as the reciprocal of the period, which is the time interval between the new packet generation. It is natural to assume that in wireless sensor networks the period between generation of consistent packets is either constant or slightly variable value. Therefore, in the model the period of packet generating for any node obeys a normal distribution, and besides the values of mathematical expectation and standard deviation are specified by the user.

In fact, the frequency numerator is the number of packets generated during the time interval in the denominator. When bringing all frequencies to a common denominator, in the numerator there is the number of packets produced by each node over the period of time in the denominator. The sum of these values represents the number of packets generated in the whole network during the same time interval. Therefore, the total frequency of new packet generation is obtained by algebraic sum of the frequency of packet generation by each node separately:

$$\begin{cases} T_1 = k \\ T_2 = l \\ T_3 = m \end{cases} \Longrightarrow \begin{cases} \nu_1 = \frac{1}{k} \\ \nu_2 = \frac{1}{l} \\ \nu_3 = \frac{1}{m} \end{cases} \Rightarrow \begin{cases} \nu_1 = \frac{lm}{klm} \\ \nu_2 = \frac{kl}{klm} \\ \nu_3 = \frac{km}{klm} \end{cases} \Rightarrow \nu_{gen} = \frac{lm+kl+km}{klm} \qquad (1)$$

Assumption 3

The strongest assumption made in the process of creating the model of attacks on wireless sensor network is the instant transmission of messages between two consecutive nodes of the route. For the ease of programming, the delay in sending each packet for the time calculated by the method presented below instead of reproducing the actual data transfer through the environment is implemented. This assumption has no effect on statistics accumulation because in the model, as in the real system, the message is considered to be sent only after successful transmission of the last data bit. The only significant result is the apparent assumption of the absence of collisions, which also substantiates by the following mathematical calculations.

First, let consider the process of message transmission between two neighboring nodes of the ZigBee network. The IEEE 802.15.4-2015 sets out the format of the packet on the physical layer (presented in Table III).

TABLE III. PHYSICAL LAYER PACKET OF IEEE 802.15.4

Sinchronization header (SHR)		Phisical header (PHR)	PHY payload (PSDU)		
Preamble	SFD		MAC header (MHR)	Payload	MAC footer (MFR)
4 octets	1 octet	1 octet	≤127 octets		

Let us find out the maximum packet transfer time. The standard offers several methods of signal modulation. Two methods are considered in the paper: BPSK (Binary Phase-Shift Keying) and O-QPSK (Offset Quadrature Phase-Shift Keying). The previously used method ASK (Amplitude Shift Keying) is currently assumed as outdated, and other methods are used less than chosen ones. The speed of information and symbol transmission is given in Table IV. Hereinafter, for O-QPSK consider only the frequency bands of 2.4 GHz and 868 MHz. The standard defines other frequency bands for which th e rates are equal to the rate of the 2.4 GHz band, or locate in interval of the values of 2.4 GHz and 868 MHz.

TABLE IV. THE CHARACTERISTICS OF THE DATA TRANSMISSION ENVIRONMENT

Modulation	Number of octets in the symbol	Frequency	Symbol transmission rate	Data transmission rate
BPSK	1	868 MHz	20 KS/s	20 Kbit/s
		915 MHz	40 KS/s	40 Kbit/s
O-QPSK	2	868 MHz	25 KS/s	100 Kbit/s
		2,4 GHz	62,5 KS/s	250 Kbit/s

First, let consider the transmission in the network without slots (see the Table V). In such network, the coordinator and routers do not usually go into sleep mode and are connected to a power supply. Interaction with end devices (RFD) is based on the «request-response» principle: the end nodes are autonomous, spending most of the time in sleep mode, but sometimes «wake up» and either directly transmit data according to the CSMA/CA algorithm, or ask the coordinator of the PAN (Private Area Network) for a beacon. The coordinator sends the beacon containing information about the availability of information intended for the destination host. Then standard transmission using the CSMA/CA is provided. In this case, the transmitting node:

1) waits for a random time interval from 0 to 2BE-1, where BE is the Backoff Exponent (this value defaults to 3);
2) listens environment for active transmission in the period of time *aCcaTime* (default is 8 symbols);
3) depending on the state of the environment:
   a) if the environment is busy, then increments BE value by 1 and turn to step 1;
   b) if the environment is free, then transmits the data;
   c) if the number of retries has exceeded the acceptable limit (*macMaxCsmaBackoffs*, default is 4), it stops trying to send and returns an error.

TABLE V. THE MINIMUM TRANSMISSION TIME OF ONE PACKET IN THE NETWORK WITHOUT SLOTS

	O-QPSK		BPSK	
	2,4 GHz	868 MHz	915 MHz	868 Mhz
InitialBackoff	$\frac{148}{62500} = 2{,}368\ ms$	$\frac{148}{25000} = 5{,}92\ ms$	$\frac{148}{40000} = 3{,}7\ ms$	$\frac{148}{20000} = 7{,}4\ ms$
TransmissionTim e	$\frac{1064}{250000} = 4{,}256\ ms$	$\frac{1064}{100000} = 10{,}64\ ms$	$\frac{1064}{40000} = 26{,}6\ ms$	$\frac{1064}{250000} = 53{,}2\ ms$
Rx-Tx	$\frac{12}{62500} = 192\ \mu s$	$\frac{12}{25000} = 480\ \mu s$	$\frac{12}{40000} = 300\ \mu s$	$\frac{12}{20000} = 600\ \mu s$
AckTime	$\frac{88}{250000} = 352\ \mu s$	$\frac{88}{100000} = 880\ \mu s$	$\frac{88}{40000} = 2{,}2\ ms$	$\frac{88}{20000} = 4{,}4\ ms$
Total	7,168 ms	17,92 ms	32,8 ms	65,6 ms

Total transmission time consists of the following values:

1) Initial expectation period - InitialBackoff;
2) Data transmission – TransmissionTime;

3) Switching from listening mode to transmission mode - Rx-Tx;
4) Confirmation transmission (without the use of CSMA/CA).

$$\begin{aligned} InitialBackoff &= (2^3 - 1) * aUnitBackoffPeriod + aCcaTime = \\ &= 7 * (aTurnaroundTime + aCcaTime) + aCcaTime = \\ &= 7 * 20\ symbolic\ periods + 8\ symbolic\ periods = \\ &= 148\ symbolic\ periods \end{aligned}$$

$$DataSize = 133 * 8 = 1064\ bit$$

Also the maximum transmission time of one packet is estimated (shown in Table VI). As noted earlier, if after the expiration of I*nitialBackoff* time interval environment remains busy, BE is incremented by 1, and then the waiting interval begins. The cycle can take up to 4 iterations. Then the maximum waiting time is:

$$\begin{aligned} InitialBackoff = (2^3 - 1) * aUnitInitialBackoffPeriod + aCcaTime + (2^4 - 1) \\ * aUnitInitialBackoffPeriod + aCcaTime + (2^5 - 1) \\ * aUnitInitialBackoffPeriod + aCcaTime + (2^6 - 1) \\ * aUnitInitialBackoffPeriod + aCcaTime \\ = aUnitInitialBackoffPeriod * (7 + 15 + 31 + 63) + 4 \\ * aCcaTime = 116 * 20 + 4 * 8 = 2352\ symbolic\ periods \end{aligned}$$

TABLE VI. THE MAXIMUM PACKET TRANSMISSION TIME IN THE NETWORK WITHOUT SLOTS

	O-QPSK		BPSK	
	2,4 GHz	868 MHz	915 MHz	868 MHz
InitialBackoff	$\frac{2352}{62500} = 37{,}632\ ms$	$\frac{2352}{25000} = 94{,}08\ ms$	$\frac{2352}{40000} = 58{,}8\ ms$	$\frac{2352}{20000} = 117{,}6\ ms$
…	…	…	…	…
Total	42,432 ms	106,08 ms	87,9 ms	181,2 ms

Therefore, in the worst case when network is maximally loaded, the packet will be transmitted faster than 1 second after generation (otherwise the error will be returned, and the model assumes the absence of such errors). This, in particular, explains the assumption about the extremely low probability of collisions that was made earlier: even if there is a collision, retransmission will not take more than 181,2 ms in the worst case, which is much less than time periods under investigation. Collision is possible only in the case depicted in Fig. 2: nodes, whose POS (private operating space) intersect by less than half, at the same time send messages to the third node, and thereby disrupt the transmission of each other.

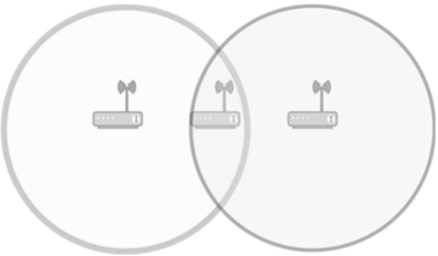

Fig. 1. CSMA/CA collision

Now let us reason about the network using slots (network with beacons). In such network there is a particular importance of types of devices and messages. Coordinators periodically send to the network some messages of a special type – the beacons, which, firstly, transmit the configuration information, and secondly, perform a synchronization function. The separation of environment between the different PAN coordinators can be implemented in different ways: by time division, by transmission in different frequency bands, etc.

The time interval between beacon transmissions is divided into active and inactive parts. The active part called superframe and consists of 16 slots. The first slot is the beacon. The start time of the first slot is the start time of the transmission of the first information bit of physical layer packet payload.

Within the superframe there is competitive access to slots using the CSMA/CA algorithm. The last 7 slots may be allocated for data transmission without contention, but this case will not be considered. Therefore, differences from the previous consist in the following:

1) There is a pre-set division into active and inactive time intervals;
2) The default channel listening is performed within the time CW*aCcaTime, where CW is 2 by default;
3) Most of the time all network devices spend in sleep mode.

For a network with slots the following ratio are valid:

$$BeaconInterval = BI = aBaseSuperframeDuration * 2^{macBeaconOrder}$$

$$\begin{aligned} SuperframeDuration = SD = \\ = aBaseSuperframeDuration * 2^{macSuperframeOrder} \\ aBaseSuperframeDuration = aBaseSlotDuration * aNumSuperframeSlots \\ = 60\ symbols * 16 = 960\ symbols \end{aligned}$$

m*acBeaconOrder* and *macSuperframeOrder* can take values between 0 and 14. Moreover, *macSuperframeOrder* must be less than macBeaconOrder. The maximum and minimum values of BI and SD in this case are given in Table VII.

TABLE VII. THE MAXIMUM AND MINIMUM VALUES OF BI AND SD

	O-QPSK		BPSK	
	2,4 GHz	868 MHz	915 MHz	868 Mhz
aBaseSlotDuration	15,36 ms	38,4 ms	24 ms	48 ms
BI_{max} и SD_{max}	251,65824 s	629,1456 s	393,216 s	786,432 s
BI_{min} и SD_{min}	15,36 ms	38,4 ms	24 ms	48 ms

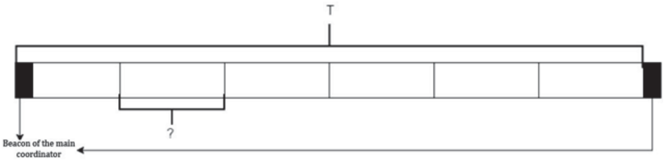

Fig. 2. The division of network channel with slots in time

The simplest case of system in which each PAN operates on its own channel is useless, because there is no fundamental difference between the case describing the network without slots: in both networks beacons can be sent even at the same time. Therefore, we present computations for the case of division in time (Table VIII). Figure 2 shows a solvable problem: it is required to evaluate the minimum time interval between beacons from the main coordinator under the following conditions:

1) Network can contain 10, 15 or 20 PAN;
2) Each PAN includes 5 nodes;
3) Collisions are excluded.

$$\begin{aligned} InitialBackoff_{best} &= (2^3 - 1) * aUnitBackoffPeriod + CW * aCcaTime \\ &= 7 * (aTurnaroundTime + aCcaTime) + CW * aCcaTime \\ &= 7 * 20\ symbolic\ periods + 2 * 8\ symbolic\ periods \\ &= 156\ symbolic\ periods \end{aligned}$$

$$DataSize = 133 * 8 = 1064\ bit$$

$$\begin{aligned} InitialBackoff_{worst} &= (2^3 - 1) * aUnitInitialBackoffPeriod + CW * aCcaTime \\ &+ (2^4 - 1) * aUnitInitialBackoffPeriod + CW \\ &* aCcaTime + (2^5 - 1) * aUnitInitialBackoffPeriod \\ &+ CW * aCcaTime + (2^6 - 1) \\ &* aUnitInitialBackoffPeriod + CW * aCcaTime \\ &= aUnitInitialBackoffPeriod * (7 + 15 + 31 + 63) + 4 \\ &* CW * aCcaTime = 116 * 20 + 4 * 2 * 8 \\ &= 2384\ symbolic\ periods \end{aligned}$$

TABLE VIII. THE ONE PACKET TRANSMISSION TIME IN THE NETWORK WITH SLOTS

	O-QPSK		BPSK	
	2,4 GHz	868 MHz	915 MGz	868 MGz
InitialBackoff best	2,496 ms	6,24 ms	3,9 ms	7,8 ms
InitialBackoff worst	38,144 ms	95,36 ms	59,6 ms	119,2 ms
TransmissionTime	4,256 ms	10,64 ms	26,6 ms	53,2 ms
Rx-Tx	195 μs	480 μs	300 μs	600 μs
Ack	352 μs	880 μs	2,2 ms	4,4 ms
Total best	7,296 ms	18,24 ms	33 ms	66 ms
Total worst	44,544 ms	107,36 ms	88,7 ms	177,4 ms

Based on assumptions about the number of PAN and the number of nodes in each PAN the required duration of BI for networks with O-QPSK modulation with frequency range of 2.4 GHz and network with BPSK modulation and frequency range 868 MHz can be evaluated by formula:

$$BI_{min} = \sum_{i=1}^{N_{PAN}} N_{node_i} \tag{2}$$

TABLE IX. THE REQUIRED BI FOR THE NETWORK WITH SLOTS

	O-QPSK (2,4 GHz)		BPSK (868 MHz)	
N	best	worst	best	worst
10	437,76 ms	2,67264 s	3,96 s	10,644 s
15	656,64 ms	4,00896 s	5,94 s	15,966 s
20	875,52 ms	5,34528 s	7,92 s	21,288 s

The obtained values (Table IX) specify the minimum required interval between the beacons from the coordinator. Each node in the network successfully transmits at least one packet. It should be noted that the described case is the worst of all possible because it contains the full intersection of all POS. In practice, PAN that are spaced apart from each other at the distance exceeding POS, can use one and the same moment of time to transmit packets. Time-sharing managing is performed by the coordinator on the basis of information about the spatial location of devices.

As it was noted earlier, the model takes into consideration the packet transmission delay between nodes: the packet is passed to the next node not immediately, but when the timer expires (the transmission time calculated for different characteristics of the network is represented above). To ensure full adequacy of the model it is necessary to select the period of packet generation and statistics collection period larger than the maximum transmission time within the hop. In this case, all generated packets during this period would either be transferred or not be transferred at all. It is also recommended to comply with the ratio:

$$\frac{1}{v_{gen}} > T_{min} \tag{3}$$

where T_{min} is the minimum time that is necessary for reliable packet transmission. Then it is guaranteed that the new packet will not appear until the previous packet would be transmitted by any other node in the network. However, this restriction is too stringent and should be used only if the POS of all nodes completely overlap, and receiving of transmitted information signal is carried out by all nodes. In addition, for reasons of energy efficiency in ZigBee wireless sensor networks, packets are almost never generated more than once in a few seconds.

Assumption 4

The model explores the issues of violation of the routing integrity and availability. The functional for network automatic rebuild is not implemented as it does not allows to argue in general case about the presence or absence of harmful impacts on the network: the evidence of, for example, the «funnel» attack is the change in the frequency of frame sending to the certain node relatively to the frequency in the normal mode of operation, but not the previous rebuild operation. In addition, in some cases, the method of the same attack realization may be the deliberate lay-out of part of routers. In this case, network rebuilding may not occur because it is sufficient for nodes to update the associated routing tables.

IV. THE STRUCTURE OF THE MODEL

OMNeT++ simulator was chosen to realize the model. It is an object-oriented library, which defines classes for the objects of the network interaction (network nodes) and messages sent between them. The significant advantages are the built-in scripting programming language for network describing (NED - Network Description Language), the graphics library for the modelling visualization and integrated development environment based on «Eclipse».

The simulator enables to realize discrete-event simulation. For this purpose the concept of the message queue is used. All interactions between objects are performed by sending messages to other nodes or to themselves. In this case, each message corresponds with the time of delivery, in which messages are stored in a priority queue: the closer to current delivery time value is, the closer to the head of the message queue it will be. Messages are extracted from the queue alternately. As soon as the message is retrieved, the time global variable takes the value corresponding to the time of message delivery.

The model uses three probability distributions:

1) The time intervals between consistent packet generations are normally distributed with parameters defined by the user;
2) The number of frames of channel layer in each network layer packet is subject to geometric distribution;
3) The addresses of the destination and the objective PAN ID are selected randomly from a uniform distribution.

Two network topologies were implemented: mesh network and cluster tree. The other topologies are explicitly reduced to these two most common network topologies. For these topologies different objects of interaction and methods of addressing were fulfilled. In addition, for each topology the attacking nodes were realized. Therefore, the model allows studying the following types of attacks:

1) Re-transmission;
2) Spoofing;
3) The Sybil attack;
4) The wormhole;
5) Funnel;
6) Selective forwarding;
7) Denial of sleep;
8) Flooding.

Mesh network

Inside of this model two types of objects are implemented:

1) The network node represents a router attached to multiple end devices. Transmission to end device is performed in the different channel from that is used for routing between the coordinators. It is assumed that end devices are connected to their PAN coordinators according to the «star» scheme.
2) The collector is node accumulating statistics. Every T seconds it writes information about the network hops to the file.

For this model the route search algorithm (AODV - Ad-hoc On-demand Distance Vector algorithm) was implemented. When generation new packet, the node checks the routing table for the entry about the next node in the route for a given destination address. If the entry does not exist, a broadcast request is carried out. It is repeated by each receiving node until it reaches the node with the given address. This node using the information from the broadcast packet (it is updated by each node) sends the packet back to the node that was the source of the query. Then message transmission can be implemented, as the route information is contained in all nodes comprised in this route. More information about the algorithm can be obtained in [6].

The screenshot of the network of 15 nodes with the mesh topology is shown in Fig. 3.

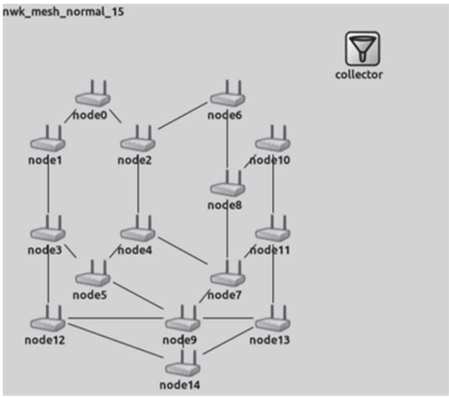

Fig. 3. Mesh network topology

The cluster tree

This model uses a simplified routing scheme. Coordinator allocates domain addresses for each node. This domain can be to share between the connected devices at the discretion of node – and so on. Objects of three types are realized:

1) The network node is similar to the node of mesh topology;
2) Collector is similar to the node of mesh topology;
3) Adresator is a node that performs addressing support functions.

For the calculation of address domain boundaries the following ratio are used (own address is removed from the selected domain, the total number of addresses is set by the user):

$$For\ the\ child\ i\ (i \in [0; NumChildren]):$$

$$First = FirstChildAddress + i * \left[\frac{1 + LastChildAddress - FirstChildAddress}{NumChildren}\right]$$

$$Last = FirstChildAddress + (i + 1) * \left[\frac{1 + LastChildAddress - FirstChildAddress}{NumChildren}\right] - 1$$

Where:

NumChildren is the number of children of the node;

FirstChildAddress is the first address from the domain (by default is over for 1 than the private address of the PAN coordinator);

LastChildAddress is the last address of the domain;

First is the first domain address allocated to the i-th child;

Last is the latest domain address allocated to the i-th child.

For example, if the main coordinator has been allocated with domain of 50 addresses (0 – 49), then it gets the address 0, and the remaining addresses are divided equally among children (for simplicity, the cluster tree is supposed to be balanced). If there are 3 children, then:

$$FirstChildAddress \coloneqq 1$$

$$LastChildAddress \coloneqq 49$$

$$i = 0 \Rightarrow First = 1; Last = 1 + 1 * \left[\frac{1 + 49 - 1}{3}\right] - 1 = 16;$$

$$i = 1 \Rightarrow First = 1 + 1 * \left\lceil \frac{1 + 49 - 1}{3} \right\rceil = 17; Last = 1 + 2 * \left\lceil \frac{1 + 49 - 1}{3} \right\rceil - 1 = 32;$$

$$i = 2 \Rightarrow First = 1 + 2 * \left\lceil \frac{1 + 49 - 1}{3} \right\rceil = 33; Last = 1 + 3 * \left\lceil \frac{1 + 49 - 1}{3} \right\rceil - 1 = 48.$$

Address «49» remains unused. As a result, all the children get to use the domain of the 16 addresses, the first of which they assign with themselves, and the rest will be divided between their children.

Addressing is simple: if the destination address in the received or in the newly generated packet belongs to the domain, then the transmission to the child is occurred, otherwise, the packet is transferred to the parent. Node presence guarantee with specified destination address in the packet is provided by adresator.

The example of «cluster tree» topology is shown in Fig. 4.

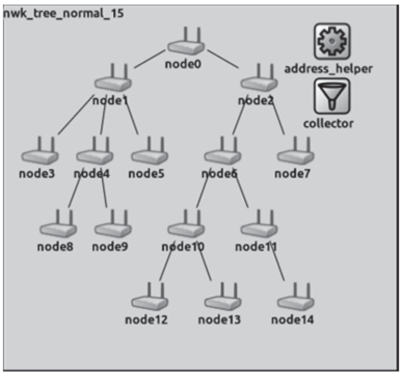

Fig. 4. The cluster tree

V. Description of experiment

The main purpose of the model construction is to study statistical characteristics of the network in the case of integrity and availability attack committing. Before obtaining and the mathematical analysis of the frequency characteristics it is necessary to generate the feature space, which is not the purpose of this work.

To illustrate the model work, the graphics of the simplest characteristics of the network are given. It describes the total number of packets and the number of packets related to routing for both topologies with 15 nodes. This value was chosen from considerations about «funnel» and «wormhole» attack modeling methods in the cluster tree. Taking into account that most of the packets passes through the root node, it is required to provide sufficient height of the tree. If we assume that the number of children at each node is equal to 2, 15 nodes are required to obtain a tree of depth 3 (1 node for 0 level, 2 nodes for 1 level, 4 nodes for 2 level, 8 nodes for 3 level). The results are presented in figures 5-6.

The following parameters were used in a run:

1) The number of nodes is 15;
2) For all nodes the period of packets generation obeys the normal distribution with parameters:
   a) Mathematical expectation is 10.0;
   b) The standard deviation is 1.0;
3) The beginning of packet generation for each node obeys the uniform distribution and takes integer values from 0 to 20.
4) The packet size in frames is determined by the geometric distribution with a constant 0.8;
5) The number of end devices in each PAN is 5;
6) Statistics collection period is 10 seconds.

Paying attention to the absence of rebuilding in the network after the beginning of work, large amount of routing messages are forwarded only in the first few seconds after generation of the first message. Because the number of nodes is small, and the packets appear relatively often, routing messages in the network are not observed further. Therefore, from the point of view of attack modelling there are two options: either to start the statistics collecting only after the routing tables formation, or to include the «number of routing messages» parameter into feature space.

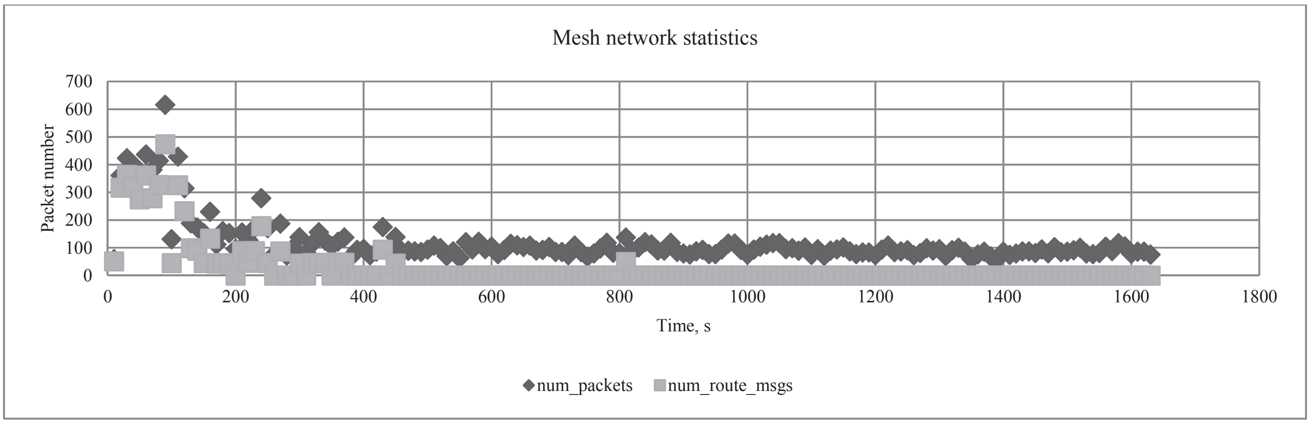

Fig. 5. Mesh network statistics

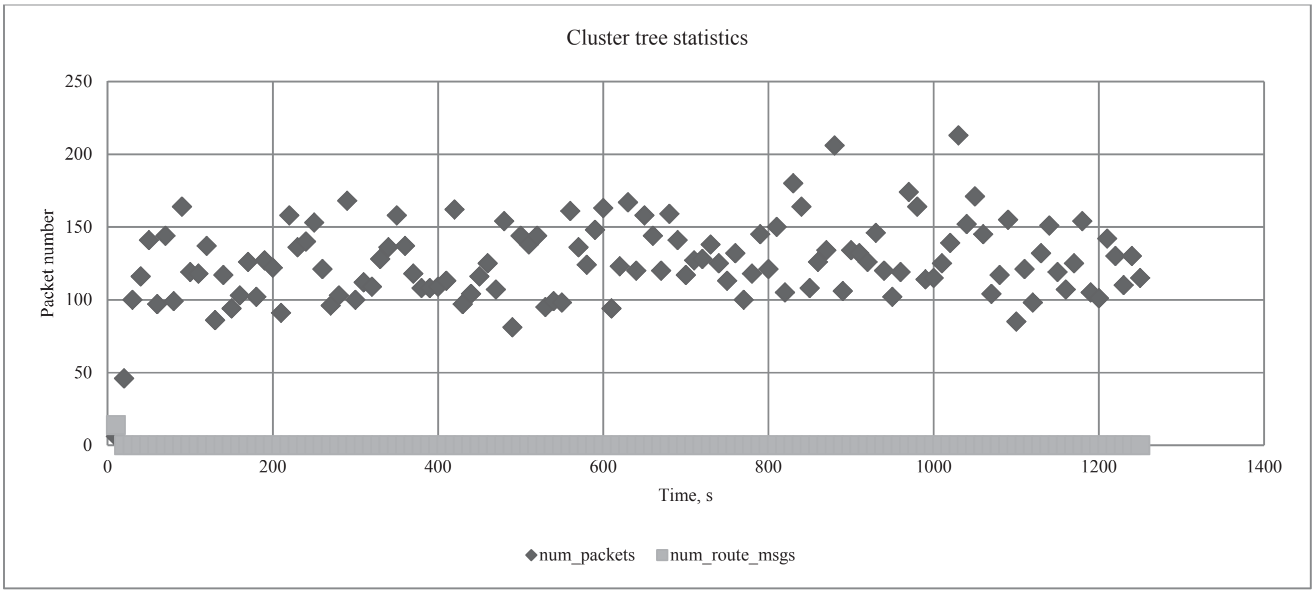

Fig. 6. Cluster tree statistics

VI. Conclusion

The paper proposes the system for modelling of the integrity and availability attacks on wireless sensor networks. For the model limitations are defined and the adequacy is proved for compliance with the real system under specified limitations. It should be noted that the obtained characteristics are related to routing and are independent from the features of link and physical layers of the stack of network protocols. Therefore, the feature space for the attack detection acquired in the further work can be used for other networks, including those that do not belong to the class of wireless sensor networks, but meet the specified limitations. In other cases, the conversion to limitations can be implemented by scaling the features.

References

[1] D.E. Comer, *Internetworking With TCP/IP Vol I: Principles, Protocols, and Architecture*. Pearson, 2014.

[2] OMNeT++ official website, *OMNeT++ simulation manual*, Web: https://omnetpp.org/doc/omnetpp/manual/

[3] A.S. Tanenbaum and D.J. Wetherall, *Computer Networks*. Prentice Hall, 2011

[4] ZigBee Alliance official website, *Low-power, low-cost, low-complexity networking for the Internet of Things*. Web: http://www.zigbee.org/zigbee-for-developers/network-specifications/

[5] IEEE Standards Association official website, 802.15.4-2015 - *IEEE Standard for Low-Rate Wireless Networks*. Web: http://standards.ieee.org/findstds/standard/802.15.4-2015.html

[6] P. Baronti, P. Pillai, V.W.C. Chook, S. Chessa, A. Gotta, Y. Fun Hu, *Wireless sensor networks: A survey on the state of the art and the 802.15.4 and ZigBee standards*, "Computer Communications", vol. 30, Dec. 2007, pp.1655–1695.

[7] F. Cuomo, S. Della Luna, E. Cipollone, P. Todorova, T. Suihko, *Topology Formation in IEEE 802.15.4: Cluster-Tree Characterization*, in Proc. PerCom Conf., March 2008, pp.276-281.

[8] F. Cuomo, E. Cipollone, A. Abbagnale, *Performance analysis of IEEE 802.15. 4 wireless sensor networks: An insight into the topology formation process*, "Computer Networks", vol.53, Dec. 2009, pp. 3057-3075.

[9] J. Zheng, M.J. Lee, *A comprehensive performance study of IEEE 802.15.4*, "Sensor Network Operations", IEEE Press, Wiley Interscience, New York, 2006, pp. 218–237, Chapter 4.

[10] I.S. Lebedev, V.Korzhuk, I.Krivtsova, K.Salakhutdinova, M.E.Sukhoparov, D.Tikhonov, *Using Preventive Measures for the Purpose of Assuring Information Security of Wireless Communication Channels,* "Proceedings of the 18th Conference of Open Innovations Association FRUCT – 2016", pp. 167-173

[11] A.M. Wyglinski, X. Huang, T. Padir, L. Lai, T.R. Eisenbarth, K. Venkatasubramanian, *Security of autonomous systems employing embedded computing and sensors*, "IEEE Micro", vol.33, Mar. 2013, pp. 80-86

[12] I.S.Lebedev, I.E.Krivtsova, V.Korzhuk, N.Bazhayev, M.E.Sukhoparov, S.Pecherkin, K.Salakhutdinova, *The Analysis of Abnormal Behavior of the System Local Segment on the Basis of Statistical Data Obtained from the Network Infrastructure Monitoring*, "Lecture Notes in Computer Science" (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics) - 2016, Vol. 9870, pp. 503-511