Research of influence of the attacks on the group of mobile wireless network nodes

Alexandr Basan
Southern Federal University
Chekov st.,2, 347922, Taganrog
asbasan@sfedu.ru

Elena Basan
Southern Federal University
Chekov st.,2, 347922, Taganrog
ebasan@sfedu.ru

Oleg Makarevich
Southern Federal University
Chekov st.,2, 347922, Taganrog
obmakarevich@sfedu.ru

Stanislav Teterevyatnikov
Southern Federal University
Chekov st.,2, 347922, Taganrog
lenny.bonus111@gmail.com

Abstract

This article focuses on the development of the methods for the analysis of the effectiveness of an active attacks on the network of mobile robots. The purpose of this study is to determine the parameters of network nodes on which the attack affects and assess the extent of the impact of the attack. To achieve this goal, the following tasks were accomplished. Firstly, a statistical analysis of the change in the parameters of the network node during the implementation of the attack and without attack. Secondly, it was identified the parameters to which the attack affects more. Thirdly, scripts are developed for denial-of-service attack and Black-hole attack with varying degrees of intensity. Fourth, an experimental study was carried out, which revealed the parameters to which the attack is more affected. To conduct an experimental study, a full-scale model of a group of mobile devices was developed. The presented attack scenarios were realized in this model, as well as in the NS-2.35 simulation system.

Keywords: mobile robots, attacks, Raspberry Pi, statistical analysis, energy consumption, network load.

1 Introduction

Vulnerabilities of wireless communication networks have been known for a long time, but the world does not stand still, as wireless networks become more used, new problems arise related to their security. Wireless networks, in many ways, simplify and reduce the cost of communication between nodes of data transmission. For this reason, they are actively used in the industrial and other fields [Bas17]. In particular, wire-less networks have

In: Marco Schaerf, Massimo Mecella, Drozdova Viktoria Igorevna, Kalmykov Igor Anatolievich (eds.): Proceedings of REMS 2018 – Russian Federation & Europe Multidisciplinary Symposium on Computer Science and ICT, Stavropol – Dombay, Russia, 15–20 October 2018, published at http://ceur-ws.org

become very popular for the interconnection of small devices such as: a network of unmanned aerial vehicles and the "Smart Home" system [Sch08]. Relevance of the work due to the rapid development of robotics and other high-intelligent technologies, as well as their active implementation in industry and everyday life. In this case, as practice shows, often robotic systems, mobile devices give a malfunction and are quite vulnerable to various kinds of impact. Before introducing a system of mobile devices or robots into operation, security analysis and the possibility of exploitation of existing vulnerabilities, mitigate risk and offer protection wireless and mobile systems. The developed methodology is based on the analysis of statistical information about the transmitted traffic in the network. The main idea is that the more effective the attack, the more it affects the change in the pattern of traffic on the network. Typically, mobile devices operating on the static type of action, for example fixation environmental parameters transmitted packets on a particular algorithm beforehand. Algorithms and group management systems are quite popular solution, allowing organizing a group of mobile devices. Therefore, such networks are sufficiently sensitive to any significant changes in the quantitative and quantitative composition of the transmitted packets. In addition, mobile devices have a limited battery charge and can operate a limited amount of time [Mak17]. Most of the energy reserve mobile devices spend on fulfilling their specific functions of fixing parameters, environment, moving, sending packets. At the same time, if an attacker performs a denial-of-service attack, forcing the node to constantly respond to its requests, then this will cause additional energy costs. This article examines the impact of an attack on the degree of change of various parameters of a wireless network and nodes. If we determine the thresholds of attack efficiency, then we can improve the quality of the intrusion prevention system. This need arises due to the fact that mobile device networks are already vulnerable to the impact of the environment. Some changes may be mistaken for an attack or abnormal activity.

2 Method for assessing the effectiveness of active attacks on wireless mobile devices

The methodology involves the following sequence of actions:

1. Calculation of the total amount of network node traffic:

$$\begin{aligned} L_{total} = \sum_N s_{data}(\Delta t) + \sum_N s_{routing}(\Delta t) + \sum_N r_{data}(\Delta t) + \sum_N r_{routing}(\Delta t) + \\ + \sum_N d_{data}(\Delta t) + \sum_N d_{routing}(\Delta t) + \sum_N f_{data}(\Delta t) + \sum_N f_{routing}(\Delta t), \end{aligned} \tag{1}$$

s_{data} - the total number of segments sent at the transport level; $s_{routing}$ - the total number of sent by routing protocol; r_{data} - the total number of segments received at the transport level; $r_{routing}$ - is the total number of received routing packets. d_{data} total number of discarded segments transmitted at the transport level;$d_{routing}$ - is the total number of discarded routing packets. f_{data} - the total number of forwarding segments at the transport level; $f_{routing}$ - the total number of forwarding routing packets. N - is the total number of nodes in the network.It is necessary to evaluate the growth of this metric. If there is a rapid growth of the number of packets in the network, it is likely to be attacked.

2. The second step is to estimate the degree of variance of the parameter, the load of the network nodes relative to the average value. For this, it is necessary to calculate the general variance for the node load value at the current interval for each node of the network:

$$D_{Lg} = \left(\sum_{i=1}^{N} (L_i - \bar{L_g})^2 \right) / N, \tag{2}$$

Where D_{Lg} is the general variance of the network load parameter, $\bar{L_g}$ this is the general average for the network load factor, L_i - the load level of the current node, N the total number of nodes in the network. If in the process of growth of a network metric values is observed, it can be concluded that the anomaly is present on the network.

3. Calculation the Ratio of sent to received packets:

$$Ratio_{r,s} = r_{i,n,data} / s_{i,n,data}, \tag{3}$$

$Ratio_{r,s}$ the ratio between received and sent packets.

In normal network operation, the number of received data packets should approximately coincide with the number of sent packets, and there may be slight deviations. Therefore, if you measure the ratio of sent and received packets, you can detect anomalous behavior of the node. If a node becomes a victim of a denial of service attack, then the received much more packet then sent, or then receive other nodes. 4. Calculation of the deviation from the overall average for each network node:

$$\begin{aligned} Dev_{N,i,s}(\Delta t) &= (s_{n,i}(\Delta t) - \bar{s_i}(\Delta t))N, \\ Dev_{N,i,r}(\Delta t) &= (r_{n,i}(\Delta t) - \bar{r_i}(\Delta t))N, \end{aligned} \tag{4}$$

$Dev_{N,i,s}(\Delta t), Dev_{N,i,r}(\Delta t)$- deviation from the overall average parameter - the number of packets sent and received for each node of the network for the current time interval. $\bar{s_i}(\Delta t), \bar{r_i}(\Delta t)$ - the mean value for parameters is the number of packets received and sent for the current time interval for all nodes. Analysis of this parameter will not give an unambiguous answer which node is im-plementing the attack. But it can serve as a good tool for determining the degree of anomalous activity of malicious nodes. 4. Calculation the ratio of dropped packets from normal network operation:

$$Ratio_{i,d}(\Delta t) = d_i(\Delta t)/d_{norm_i}(\Delta t), \tag{5}$$

5. Evaluation ratio of sent packets, received packets, and dropped packets:

$$Ratio_{sent} = \frac{\sum s_{total}(\Delta t)}{L_{total}} * 100\% \tag{6}$$

$$Ratio_{received} = \frac{\sum r_{total}(\Delta t)}{L_{total}} * 100\% \tag{7}$$

$$Ratio_{dropped} = \frac{\sum d_{total}(\Delta t)}{L_{total}} * 100\% \tag{8}$$

$Ratio_{sent}$ - percentage "content" of the sent packets in the total traffic, $Ratio_{received}$ - percentage "content" of the received packets in the total traffic, $Ratio_{dropped}$ - percent-age "content" of the dropped packets in the total traffic. $s_{total}(\Delta t)$ - the total number of sent packets for the current time interval, $r_{total}(\Delta t)$ - the total number of received packets for the current time interval, $d_{total}(\Delta t)$ - the total number of dropped packets for the current time interval.

6. The monitoring of electricity consumption was carried out using a KEWEISI KWS-V21 tester on a housing chip with an operating voltage of 3-20 V and a working current of 0-3.3 A. This tester is equipped with a bright screen and the ability to dis-play the following characteristics: voltage (U), power current (A), consumed battery capacity (mAh), timer.

3 Applying the developed method to a wireless network of mobile devices

3.1 Development of the real model of a group of mobile devices

One of the components of the experimental stand is firmware for implementing at-tacks on a wireless network. The structure and equipment of this tool are approximate to a real device for testing wireless network security. The firmware for testing the security of wireless networks must have the following properties: mobility; small dimensions; modular structure; ease of use; low price; support for Linux operating systems; low power consumption. To meet the above requirements, the single-board Raspberry Pi 3 model B platform was chosen [Sin15]. To display information, a 3.5-inch touch screen was selected. The device is managed remotely. The resulting device is very light and small in size. The computing power of this developed tool is sufficient for testing wireless networks. The device is powered by a small battery with a capacity of 10 000 mAh.

To test the security of wireless networks, the Raspberry Pi 3 platform requires an external wireless network card with support for the monitor mode, since the one al-ready built in does not support the monitor mode. The operating system installed on the device is Raspbian, Kernel version: 4.9. Also, the experimental stand includes WiFi router D-Link, model 320. Characteristics of a single-board microcomputer Raspberry Pi 3: Model: Raspberry Pi 3 model B; Operating system: Raspbian; ker-nel: Kernel version: 4.9; processor: 4 ARM Cortex-A53, 1.2GHz; RAM (Gb): 1; network controller: Broadcom BCM43438 2.4GHz 802.11n wireless LAN. The scheme of the experimental stand is shown in figure 1.

In addition to the actual model of a group of mobile devices, a model was also created in the simulator NS-2.35. Initially, all experiments were carried out on the model of a group of mobile nodes in order to determine the parameters to which the attack affects. Then the attacks were implemented on the full-scale model of mobile devices, and the results of the experiments conducted on the model were confirmed.

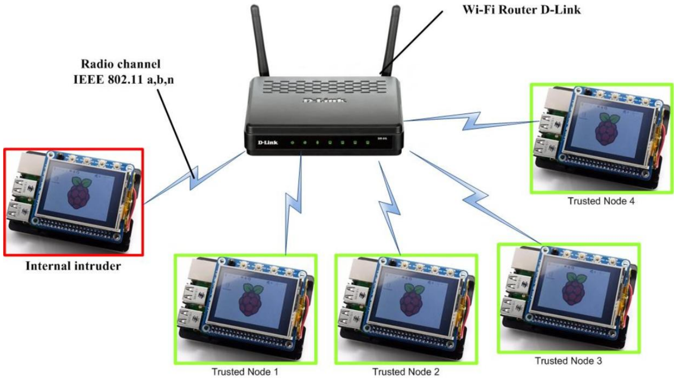

Figure 1: The developed experimental stand for realization of the method for assessing the effectiveness of active attacks on wireless mobile devices.

3.2 Scenarios of attacks on wireless mobile devices

In this study, two types of attacks were implemented. One type of attack was aimed at the availability of information. As such an attack, the denial-of-service attack was of the SYN-flood type. Another type of attack is aimed at the integrity and confidentiality of information. This is so-called Man in the middle attack. The essence of the attack is that an attacker forwarded all traffic committed between nodes through itself. Further, an attack option is suggested, when an attacker drop all packets passing through it, thereby making the network node inaccessible.

3.2.1 Scenario of denial of service attacks

The attacker creates a situation (conducting denial of service attacks), when the network node becomes unavailable to other nodes and cannot respond to their re-quests and to carry out their activities normally. To date, there are many ways to implement denial of service attacks [Vas16]. If not treated attack undertaken on the physical and data link layer which, by making noise on the signal channel is completely removed, it can be considered a denial of service attack is packet flooding network. An attacker can conduct this attack with varying intensity. One way to implement an attack for the developed experimental stand is the SYN-flood attack [Cha14]]. The attack intensity can vary depending on the interval between sending packets or depending on the number of attack victims, the attacker sends a large number of packets to the network, trying to make the connections unavailable or to exhaust the battery of nodes.

When implementing an attack on a mobile robot network, one important factor must be considered. The operation of the network of mobile robots is rather limited in time. For example, a network of drones can fully work only for 30 minutes, performing any tasks [Mah16].Therefore, the attacker does not have much time to implement the attack and disable the network nodes before it happens by itself. So the implementation of low-intensity attack or time-based attacks is not interesting. One of the objectives of the denial of service attack is the depletion of the node's resources, so increasing the victim's energy consumption is one and important purposes of the attack. Also, the second parameter that will detect abnormal activity is the number of sent packets. To analyze the effectiveness of the denial of service attack, and detection of pa-rameters that allow fixing this attack on the network, three attack scenarios were developed. The first scenario is that one attacker node actively attacks one trusted node, so that there is one attack victim on the network. In the second scenario, the attacker's node attacks two trusted hosts. In the third scenario, 4 victims are attacked, that is, all the nodes of the network. The principle of attack is that the attacker sends SYN requests and overflows the connection queue for the victim of the attack. In connection queue appear half-open connections, pending confirmation by the customer. The task of the attacker is to ensure that the queue is full to prevent new connections.

3.2.2 Scenario of Black Hole and Gray-hole Attack

Figure 2 shows the network topology, which demonstrates the scheme of the Black Hole attack. The attack consists in that the attacker is located between two trusted nodes and instead of forwarding packets, he drop them [ABas17]. As a rule, nodes that are at a significant distance from the base station, or the group leaders, can fall under such an attack. At the same time, an attacker can drop only packets transmitted by a specific protocol or according to certain time intervals, in which case a Gray Hole attack is conducted. The following situation is represented in Fig. 3 Nodes N10-15 are malicious and discard packets that trusted hosts try to pass to the group leader. In addition, the nodes can exchange packets in a two-way direction with each other. If the attacker's node is not located between them, the packets will be successfully sent and transmitted. From the figure 3 it can be seen that the nodes 8,9,7,1,4,3,5 are subject to attack. Only node 2 can communicate with the base station bypassing the group leader. Nodes 1,7,3,5 become completely isolated and can communicate only with each other. Thus, the more packets dropped by malicious nodes, the more effective the attack.

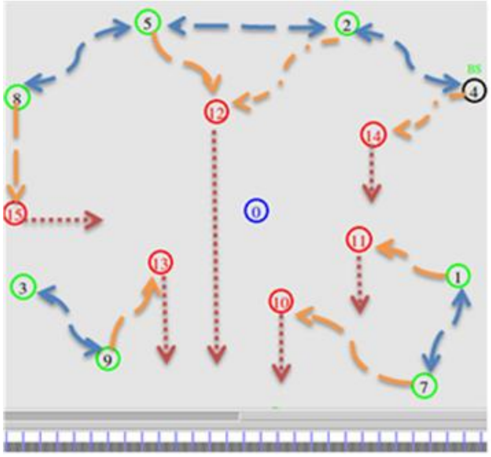

Figure 2: The Black-Hole and Gray Hole attack scheme, where the nodes 10,11,12,13,14,15 are malicious

When the network is operated in the normal mode, the discarded packets may appear, but their number is much less than in the case of an attack. To implement this attack in the NS-2.35 simulation system, the node's behavior type was added when it drop packets forwarding through it. Gray-hole attack is similar to Black-hole attack [EBas17].The difference from Black-hole attack is that malicious nodes drop packets not constantly, but with the given condition. For example, at certain time intervals, or packets that are transmitted over a specific protocol. In this study, the attack was implemented in such a way that malicious nodes dropped packets at certain time intervals. To implement this attack, an attacker was added to the NS-2.35 files, which discards packets that pass through it: `ns at 0.0 "[node(12) set ragent] malicious"` . In order to ”return” an attacker to normal behavior, a trusted type of behavior was added when the node does not discard packets: `ns at 10.0 "[node(12) set ragent]" trusted`.The following is an example for node 15, by which it will drop packets. From 1 to 17 seconds the node discards packets, then it transmits packets in normal mode. Then, starting at 33 seconds, the node again discards the packets:

```
ns at 1 "[node(15) set ragent] malicious"
ns at 17.0 "[node(15) set ragent] trusted"
ns at 33.0 "[node(15) set ragent] malicious"
ns at 50.0 "[node(15) set ragent] trusted"
ns at 60.0 "[node(15) set ragent] malicious"
ns at 110.0 "[node(15) set ragent] trusted"
ns at 180.0 "[node(15) set ragent] malicious"
ns at 200.0 "[node(15) set ragent] trusted"
ns at 210.0 "[node(15) set ragent] malicious"
```

One of the devices is a server, and the other is a client. For each of them were written the appropriate sockets (server, client) in Python. Traffic is forwarded through a rout-er (wireless access point). The purpose of the attacker is to intercept the data sent by the server in response to the client and to replace the line ”com1” with ”com2”. As a result, the server, having received the string ”com1”, will send it to the same client, but the client should receive it in the reply ”com2”. In order for an attacker acting as a router, you should enable packet forwarding. Secondly, it is necessary to substitute in the TCP-packet data string com1 on com2. For this, the nfqsed program was used. For proper operation of the program should send traffic to a nfqsed program. To do this, the following rules are introduced for iptables:

```
iptables -A OUTPUT -p tcp -m string --string "com1" --algo kmp -j NFQUEUE
```

When implementing an attack for the full-scale model of a wireless network of mobile devices, the scheme in Figure 3.

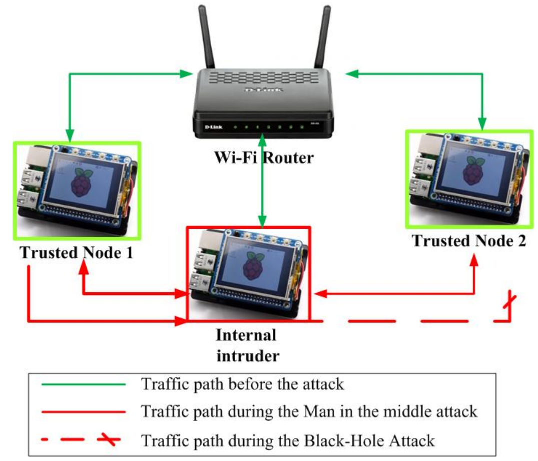
Wi-Fi Router
Trusted Node 1
Trusted Node 2
Internal intruder
Traffic path before the attack
Traffic path during the Man in the middle attack
Traffic path during the Black-Hole Attack

Figure 3: Implementation scheme the Man in the Middle and the Black hole of attacks for the full-scale model of a wireless network of mobile devices

Checking for the coincidence of the line ”com1”, if there is a match, then the packet is sent to the program input for modification:

```
iptables -A OUTPUT -p tcp -j ACCEPT
```

If there is no occurrence of the string, then running the rule, the packet is sent as is. If an attacker needs to implement a Black Hole attack, then the iptables rules are con-figured in such a way that the attacker drop packets coming to it.

```
iptables -A OUTPUT -p tcp -j DROP
```

The difference between this implementation and the one presented for the NS-2.35 model is as follows. In the case, when the attack is implemented on the real model, the node explicitly forwarded packets through itself; this is visible to other network members. In the case, the attack is implemented on simulation model, it is realized by changing the route for forwarded packets. When implementing an attack on the full-scale model, the nodes do not imply that their packets pass through an intermediary. This attack is transparent to network hosts. But in fact the result of the attack will be the same: one of the nodes is cut off from the network.

4 Experimental results

4.1 Denial of service attack

Figure 4 shows the change in the variance of the network load for nodes.

It can be seen from the figure that the variance increases significantly with increasing number of victims. This means that the load of nodes is quite different from the average. This is because the load level of the malicious node is significantly greater than the node for the load of trusted hosts. And also the load level of the victim nodes also increased in comparison with the normal state. In normal network operation, when nodes send packets according to a given algorithm and operate in the normal mode, the dispersion level can reach 7-10. Thus, it can be said that there is an abnormal activity in the network.

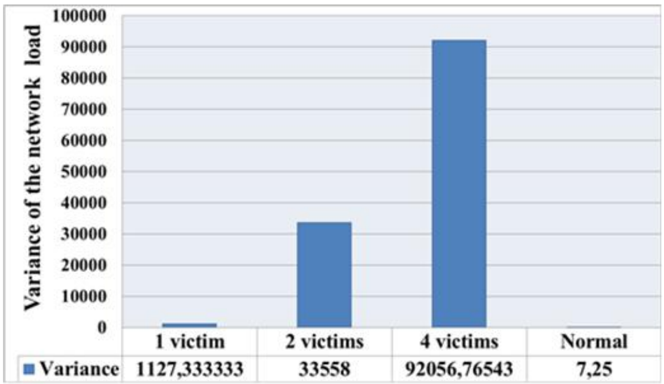

Figure 4: Variance of the load parameter for nodes under DoS attack with various number of victims.

The presence and effectiveness of a denial of service attack is fairly accurate and can be effectively determined by using Ratio of sent to receive packets. Figure 5 shows that the nodes under the attack take more packets than they send. And the difference is more than 2-2.5 times. In this case, the attack is considered effective.

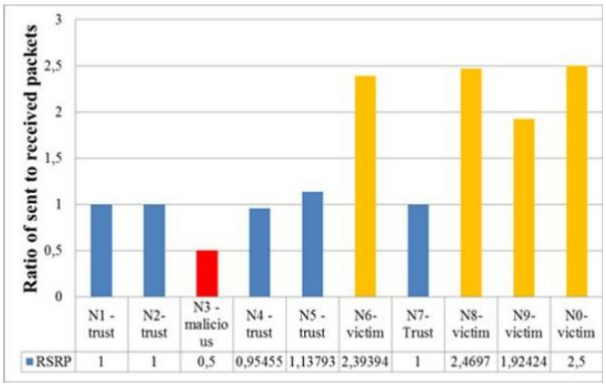

Figure 5: Ratio of sent to received packets (RSRP) for trust, victim and malicious nodes during DoS attack

As a result, the attack affects the energy consumption of the node. The result of this attack was obviously a noticeable increase in the resources consumed by the device that was attacked. During the attack, there was no availability of the communication channel.

One of the main indicators of the effectiveness of the attack is a changing in the energy consumption of the nodes. A sharp change in this indicator indicates that the node is spending resources on maintaining a large number of network connections. One of the main indicators of the effectiveness of the attack is precisely the energy consumption of the nodes. A sharp change in this indicator indicates that the node is spending resources on maintaining a large number of network connections. Figure 6 shows the situation where the level of loading an attacker is 20 times greater than in a situation where an attack is not conducted.

4.2 Black Hole and Gray-hole Attack

During the Black Hole attack, the variance level was 829.3, which greatly exceeds the variance under normal network conditions. This indicates an abnormal activity in the network. Efficient parameter in the detection of this attack is to estimate the growth of dropped packets (see Fig. 7). It can be seen from the figure that as the number of malicious nodes increases, the number of dropped packets increases, in comparison with the normal operation of the network. This suggests that the greater the numbers of nodes are attacked and are isolated from the group leader.

In addition, there was a decrease in the number of received packets, due to the fact that the attacker dropped packets sent through it by the node and the respond did not come to the node. Evaluation of the ratio between packages of different types is quite indicative. During normal operation of the network is observed ratio of sent and received packets in equal parts, in a small amount presented in dropped packets (see Fig. 8 (c)).

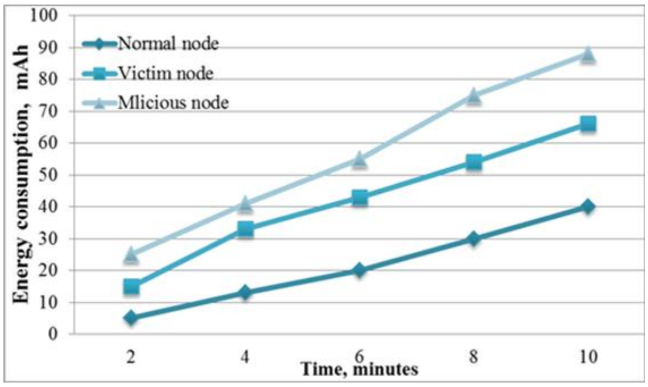

Figure 6: Energy consumption units in Denial of Service attacks

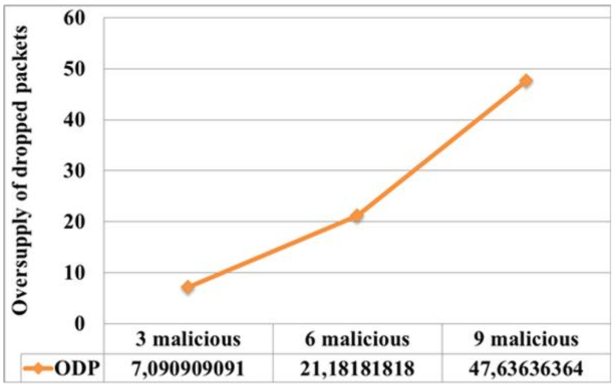

Figure 7: Change in the number of dropped packets for the network under the Black Hole attack compared to normal network operation

Also, from the figure it can be seen that as the number of malicious nodes increases, the traffic pattern changes. The ratio of the number of sent and received packets is no longer equal. This observation can be useful in developing an attack detection system. As for the level of energy consumption, it did not change significantly. It can be said that even lower consumption was observed, since the victim's node did not spend energy on receiving the package.

Acknowledgement

This work was partially supported by the Russian Foundation for Basic Research (RFBR) grant 17-07-00106 (A) Development of a method and an effective system of protection of wireless sensor networks from active malicious attacks.

5 Conclusion

In conclusion, the following should be noted. First, in order for the attack to disrupt the network operation, it must be sufficiently intensive and preferably distributed among several attackers. In the case of a denial of service attack is possible to deter-mine the degree of effectiveness of the impact on energy consumption attack victims. As well as changing the ratio of sent and received packets of victims and intruders and a general increase in the network load of nodes. In the case of Black-Hole attack we can talk about high performance when a large number of victims were observed, i.e. the blocked nodes. This influence on the ratio of sent, received and dropped packets. This attack does not affect energy consumption. Secondly, it is quite efficient to apply the calculation of the node load variance. The larger the variance value, the greater the deviation of the load of nodes from the group average. Consequently, the greater impact of the attacker on the network was observed when variance was

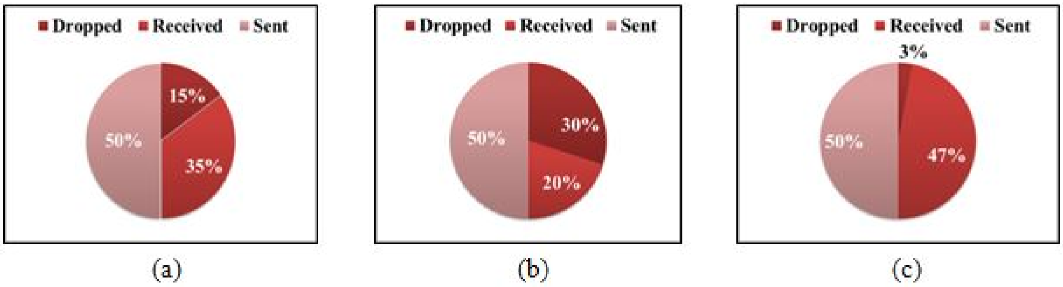

Figure 8: Changing the pattern of traffic for the network under the Black Hole by attack with a change in the number of malicious nodes (a) for 3 malicious hosts (b) for 9 malicious hosts (c) malicious nodes were missing.

in 100 times greater in comparison with normal conditions. In the future use of these parameters will provide for the development of an intrusion detection system for group of mobile robots.

References

[Bas17] A.S. Basan, E.S. Basan. The threat model for the systems of group management of mobile robots. *Proceedings of the VIII Scientific Conference System Synthesis and Applied Synergetics.*, 205-212., South Federal University. September 2017.

[Sch08] E. Schoch, M. Feiri, F. Kargl, M. Weber. Simulation of Ad Hoc Networks: ns-2 compared to JiST/SWANS SIMUTools. *First International Conference on Simulation Tools and Techniques for Communications, Networks and Systems.*34-41.2008.

[Mak17] A.S. Basan, E.S. Basan, O. Makarevich. A Trust Evaluation Method for Active Attack Counteraction in Wireless Sensor Networks. *Proceedings of 2017 International Conference on Cyber-Enabled Distributed Computing and Knowledge Discovery.*369-372, 2017.

[Sin15] M. Singh; Md. A. Khan; V. Singh; A. Patil; S. Wadar. Attendance management system. *2015 2nd International Conference on Electronics and Communication Systems (ICECS).* 418-422, 2015.

[Vas16] G. Vasconcelos; G. Carrijo; R. Miani; J. Souza; V. Guizilini. The Impact of DoS Attacks on the AR.Drone 2.0. *2016 XIII Latin American Robotics Symposium and IV Brazilian Robotics Symposium (LARS/SBR).* 127-132, 2016.

[Cha14] K. Chadha, S. Jain. Impact of black hole and gray hole attack in AODV protocol. *2016 XIII Latin American Robotics Symposium and IV Brazilian Robotics Symposium (LARS/SBR).*1-7, 2014.

[Mah16] P. Maheshwaran, S. Rajagopal A scheme for detecting the types of misbehaviour and identifying the attacks using reputation mechanism in a mobile ad-hoc network *Published in: 2016 International Conference on Communication and Electronics Systems (ICCES).*1-6.2016.

[ABas17] A.S. Basan, E.S. Basan, O. Makarevich. Analysis of Ways to Secure Group Control for Autonomous Mobile Robots. *Proceedings of 10th International Conference On Security Of Information And Networks (SIN 2017).*1-6.2017.

[EBas17] A.S. Basan, E.S. Basan, O. Makarevich. Analysis and implementation of threats for mobile robot management systems. *Proceedings of XIII - Russian. scientific-practical conference Mathematical methods and information technology means.*20-23.2017.