ASTES

Advances in Science, Technology and Engineering Systems Journal Vol. 3, No. 6, 281-288 (2018)

www.astesj.com

Special Issue on Multidisciplinary Sciences and Engineering

ASTESJ

ISSN: 2415-6698

Probabilistic Method for Anomalies Detection Based on the Analysis of Cyber Parameters in a Group of Mobile Robots

Elena Basan*, Alexander Basan, Oleg Makarevich

Department of Information Security Southern Federal University, Taganrog, 347922, Russia

ARTICLE INFO

Article history:
Received: 15 August, 2018
Accepted: 26 September, 2018
Online: 18 November, 2018

Keywords:
Mobile robots
Abnormal behavior
Probabilistic methods
Attack
Detection

ABSTRACT

This article is devoted to the issues of ensuring the security of a group of mobile robots in the implementation of attacks aimed at the property of accessibility of information and the availability of network nodes. The article presents a method for detecting an abnormal behavior of a network node based on the analysis by the group members of the parameters: residual energy and network load. Analysis of the behavior of individual robots relative to general behavior using probabilistic methods avoids the problem of creating a reference distribution for describing the behavior of a node, as well as creating a signature database for detecting anomalies. The developed method demonstrates high detection rate of denial of service attack and distributed denial of service attack with the number of malicious nodes not exceeding or slightly exceeding the number of trusted nodes. It also provides detection of the Sybil attack.

1. Introduction

This paper is an extension of work originally presented in CyberC 2017, "9th International Conference on Cyber-enabled distributed computing and knowledge discovery" titled 'A Trust Evaluation Method for Active Attack Counteraction in Wireless Sensor Networks' [1]. Mobile robot networks are quite vulnerable to attacks both over the network and physical properties of nodes. The article [2] presented a threats model for the network of mobile robots. The authors also analyzed the attacks for a group of mobile robots. Based on the analysis, it was revealed that the main set of attacks that an attacker can implement for a group of mobile robots is denial of service (DoS), distributed denial-of-service (DDoS) attack, a man in the middle (MITM) and a Sybil attack, and exhaustion resources. In addition, there are a number of attacks aimed at the robot positioning system and on other elements of the sensor system, which are not considered in this study. The main purpose of this study is to detect these attacks with a minimum of resources of mobile robots. The offender, implementing an active attack, can influence any physical parameter of the mobile robot through a network or physical impact.

1.1. Maintaining the Integrity of the Specifications

The standard methods used in intrusion detection systems (IDS) may not always have a positive effect when anomalous behavior of mobile robot network nodes is detected. This is due to several factors: 1. IDS, as a rule, work with the TCP / IP protocol stack, which is not always applicable to mobile robots that transmit data over the radio channel and can use any radio modules and any proprietary protocols; 2. Signature analysis, which is often used in the IDS [3], may be ineffective when an intruder is detected for a group of robots. The behavior of the group robots can vary significantly depending on the task being performed, including the level of network activity, it is quite difficult to create a signature database for the behavior of nodes in the context of each individual task. 3. The computing power of mobile robots is much lower than for standard computer systems for which the IDS is developed [4]. In addition, as a rule, mobile robots can either not be equipped with an operating system or have a "cut-down" version of an operating system with limited capabilities [5]. If the first two problems can be solved by writing their own software for IDS, then the problem of limited energy resources (in the form of insufficiently capacious batteries) makes the use of standard IDS almost impossible for mobile robots [6]. In [7], the authors considered an attack detection system based on the decision tree using the C5.0 algorithm applied to a group of robotic vehicles. The advantage of the presented approach is that for detecting cyber-attacks, the authors, along with four features for analyzing the process of communication and information processing, called cyber input functions, use four parameters for analyzing the physical properties of the robot, which the authors call the physical characteristics of the input signal. Next, the authors conduct 5 types of destructive impact on the robot and get a set of rules for building a decision tree. The

* Elena Basan, E-mail: ele-barannik@yandex.ru

disadvantage of the approach is that in this paper, attacks on only one robot, and not a network of robots were considered. At the same time, the authors considered a limited set of attacks: denial-of-service attacks and attacks aimed at violating physical parameters. In addition, in such systems, there is a need to constantly add rules to detect new attacks. This system is aimed at ensuring the availability of the transmitted data. In [8] an intrusion detection system based on the signature analysis is considered. The authors conducted a series of experiments to create a standard template describing the normal behavior of the robot in the absence of any external influence, as well as random behavioral anomalies. Then a number of situations in which abnormal behaviors occurred caused by environmental conditions were simulated. A normal behavior pattern of the robot based on the collected data with the weighting coefficients calculated on the basis of the frequency of occurrence of a particular type of abnormal behavior. This approach demonstrates greater efficiency in detecting a malicious node than a simple signature analysis; however, there are some disadvantages:

- The need to constantly update the signature database to control data from the new sensors of the mobile robot.
- Conducting analysis of changes only physical parameters of the node and the absence of network analysis of data.

The article [9] considers the system for detecting attacks on unmanned aerial vehicles. The development of this system used the approach based on the creation of a signature database. The system works as follows. Each node of the network has a monitor node, which may be a neighboring unmanned device that fixes the behavior of the trusted node and writes it to the matrix. The monitor node constantly monitors the behavior of the ward node and presents it with estimates. These estimates depend on how much the behavior of the ward deviates from the normal pattern of behavior. Then a rule database is created and the behavior of the node is evaluated. At the same time, the assessment is made on 7 parameters. The authors claim that their system is adaptive and demonstrates a low level of errors of the 1st and 2nd kind when detecting attacks. The disadvantage of the system is the need to constantly monitor the nodes one by one and analyze their behavior, which involves the computational load and network bandwidth.

The article [10] considers the system for detecting the abnormal behavior of robots of the Internet-robots network. The peculiarity of this system is that it has two subsystems. One is a group of robots that collect data using a sensor system and transmit it to the central node that is connected to an external mobile network. The second is a mobile network, where the following modules are available: a data acquisition module, an anomaly classification module, a control command module. The disadvantage of this system is that it is completely centralized; robots do not communicate with each other and act only through an intermediary. Anomaly detection occurs via classifier, which is trained by using training samples preformed. Thus, as a result of studying the works devoted to the topic of detecting attacks on robots, there are three main drawbacks in the existing approaches:

- Most systems based on signature analysis, either on a rules-based system. In this regard, there are the following limitations: the difficulty of detecting new attacks that are not related to the fixed patterns of the attacker's behavior, as well as the need to keep the database of rules or sets of signatures up-to-date.
- Systems based on fully distributed detection methods require additional energy costs, computational power costs from nodes and increase bandwidth. In addition, if the distributed system is used in conjunction with the signature analysis, the information about the abnormal behavior must be constantly updated, which uses the already limited resources of the robot's memory.
- When using centralized methods, a node that performs basic functions for detecting abnormal behavior is a vulnerability of the system.

In this article, a method for detecting an abnormal behavior of an attacker or several intruders within a group of mobile robots based on probabilistic methods is being developed [11]. The main difference of this method is that it does not require the creation of a standard probability distribution, like other probabilistic methods. The absence of the need to build a reference distribution is due to the fact that the current indications of the node group are taken to reveal the anomalous behavior, then the normal distribution function is constructed and the confidence interval of values is calculated. To estimate the behavior of the Ni node, the probability of the current node indicators entering the confidence interval is calculated, based on the indices of all nodes of the group. Thus, it becomes possible to estimate the probability of the node deflection behavior of the overall behavior of a group of nodes.

2. Method for detecting abnormal behavior

The peculiarity of the proposed method for a group of robots is that for the formation of the normal distribution function it is necessary to obtain data from several nodes performing a similar set of actions. To more accurately determine the degree of deviation of the current indications of a node from a group of nodes, it is necessary that the indicators of a group of nodes are in the same range. In the case of a group of mobile robots that exchange information in one task, this method will work most efficiently. An attacker can affect both the network connection between nodes and the physical parameters of the network node. Table 1 shows the parameters that can be affected by the attacker and the attack by which he can do it.

The parameter packets with data - here it is understood the fact of transfer or redirection of the packet, that is, the availability of the transmitted information is estimated. If there is any impact on the network from the attacker, then there may be situations when packets are discarded, duplicated, etc.

Table 1. The correlation of network parameters and the attacks affecting them

Parameters (indicators of anomalies)	Attacks
Data packets	Black Hole, Gray Hole, False Redirection, Denial of Service, Packet Delay
Remaining battery power	Denial of service, depletion of resources
Network load	Denial of service, resource depletion, the Sybil attack, Flood-attack , Wormhole
Package Integrity	Modification, substitution messages, Man in the middle

The battery charge parameter is the current consumption of the battery (or power consumption), as well as the remaining energy

reserve in the battery pack, which allows the device to function in the network [12].

The Network Load - the total number of packets transmitted on the network. Either the number of packets transmitted through one of the nodes of the network [13].

When detecting attacks such as denial of service and attacks aimed at depleting resources, it is necessary to select those parameters that will be evaluated according to the claimed method. Thus, in the case of a denial of service attack changing network load for a malicious node and network load for the victim. Therefore, it is advisable to estimate the network load, which is the total number of received, sent, and redirected packets of the network node. When an attacker implements an attack aimed at depleting the resources of the node, there will be a sharp decrease in the residual energy level of the node. In addition, an attacker can have superiority in the reserves of energy resources. In the implementation of the Sibyl attack or attack redirecting the impact on themselves, the main purpose of the attacker is to change the processes and routes of data exchange in the network. In other words, an attacker achieves such a situation that all or most of the traffic of neighboring nodes passes through him. Further, the attacker can simply drop received packets, or send them to the wrong nodes. The attacker can achieve this situation in various ways, in this case it is important that the level of incoming traffic will be much higher than that of other nodes of the network. Therefore, it is also necessary to consider the network boot parameter to detect this attack. In the previous work of the authors [14], in addition to the parameters, network loading and residual energy, the parameter of the number of discarded packets P1 was considered. In this study, it will not be considered. Thus, consider two parameters: the network load P2 and the residual energy P3. Changing these parameters affects the state of both the nodes of the network and the entire group of robots in general. The state of the nodes of the network can be described as follows: S1 - the state when the node is not subject to attack and does not conduct the attack itself, i.e. is authentic at the current time; S2 - the state when the behavior of the mobile robot deviated from the behavior of the greater part of the robot group can be observed provided that the node became the victim of the attack, i.e. the node is undefined; S3 - when the behavior of the mobile robot is significantly different from the nodes of the group, i.e. most likely the site is malicious. Figure 1 shows the transition graph from one state to another, and also reflects the effect of parameters and attributes on each other.

The following attributes of the node affect the parameter $P2 = L$: A_{21} - the total number of packets sent by the node containing data. In this model, data transfer uses the UDP protocol and the CBR traffic type. $A_{21} = scbr$; A_{22} is the total number of management packs, or beacons, for testing connections. In this model, packets sent via the ARP protocol act in this role. $A_{22} = s_{arp}$; A_{23} is the total number of packets sent over the routing protocol. This model uses the AODV routing protocol. $A_{23} = s_{aodv}$; A_{24} is the total number of received CBR packets. $A_{24} = r_{cbr}$; A_{25} - the total number of ARP packets received. $A_{25} = r_{arp}$; A_{26} is the total number of received AODV packets. $A_{26} = r_{aodv}$; A_{27} is the total number of dropped CBR packets. $A_{27} = d_{cbr}$; A_{28} is the total number of dropped ARP packets. $A_{28} = d_{arp}$; A_{29} is the total number of discarded AODV packets. $A_{29} = d_{aodv}$.

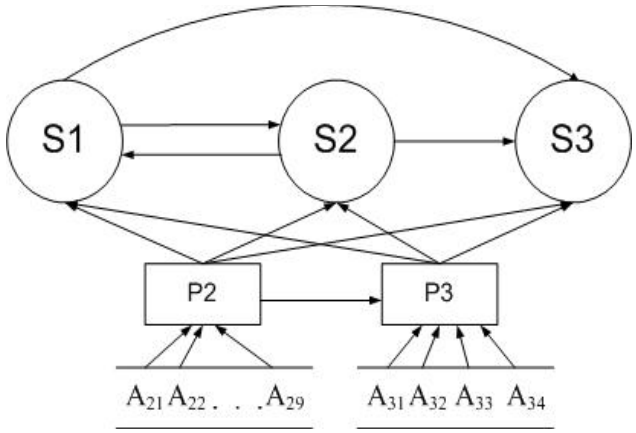


Figure.1. Graph of state of nodes in groups of mobile robots

Thus, the parameter L can be represented by the following equation:

$$L = A_{21} + A_{22} + A_{23} + A_{24} + A_{25} + A_{26} + A_{27} + A_{28} + A_{29} \quad (1)$$

Parameter $P_3 = e$ can be characterized by a finite set of attributes A_{3j}. The following attributes affect the amount of residual energy of the node, but apart from the attributes described below, the amount of residual energy is affected by the node's load, i.e. parameter $P2$: A_{31} is the initial energy reserve of the network node. $A_{31} = initialEnergy$; A_{32} is the power of the transmitted signal. $A_{32} = rxPower$; A_{33} - signal reception power, $A_{33} = txPower$; A_{34} - speed of moving the node. $A_{34} = speed$.

The residual energy is calculated by reducing the level of initial energy A_{31} for each transmitted and each received packet per unit time:

$$e_{tx} = A_{31} - (A_{33} * txtime)$$
$$e_{rx} = A_{31} - (A_{32} * rcvtime) \quad (2)$$

where e_{tx} and e_{rx} this is the level of residual energy after receiving the packet and after the transmission of the first packet; $rcvtime$ - time of packet transmission; $txtime$ - time of reception of a package. A formal description of the method is presented in Section 3, which provides an algorithm implemented in a simulation system for conducting an experimental study.

3. Implementation of the method for detecting abnormal behavior

The simulation of the developed method was carried out in the simulator NS-2.35. The procedure for detecting abnormal behavior and outputting results is called regularly at regular intervals. The start and end time of this process is set by the user in the script using a special command. The command handler plans to start a special timer for the start time of the process, and the timer and end time are written to the timer parameters [15]. To account for the parameters e and L of the mobile robot in the assembly model was added a special object that counts the number of packets transmitted / sent / forwarded node and the residual energy of the node [16]. The procedure for calculating trust works according to the following algorithm representing at the table 2.

Table 2: Calculation of the trust level for nodes in the group of mobile robots

No.	Name of equation	Equation	Description
1	**The calculation of the confidence interval boundaries**		
1.1	Variance for L parameter	$D_{Li} = \left(\sum_{i}^{N} (L_i - \overline{L})^2 \right) / n$	D_{Li}, - variance of the parameters L calculated for the group of nodes in the current time interval
1.2	Variance for e parameter	$D_{ei} = \left(\sum_{i}^{N} (e_i - \overline{e})^2 \right) / n$	D_{ei} - variance of the parameters e calculated for the group of nodes in the current time interval
1.3	The standard deviation for L parameter	$\sigma_{Li} = \sqrt{D}_{Li}$	σ_{Li} - is the standard deviation of the parameter L which calculated for the group of nodes in the current time interval.
1.4	The standard deviation for e parameter	$\sigma_{ei} = \sqrt{D}_{ei}$	σ_{ei} - is the standard deviation of the parameter e which calculated for the group of nodes in the current time interval.
1.5	Argument of the Laplace function - t	$\Phi(t) = \frac{\alpha}{2}$	$\Phi(t)$ - is the Laplace function; α is a given reliability, in this study the value of the coefficient is equal to $\alpha = 0.98$, so the argument $t = 2.34$;
1.6	The limits of the confidence interval for the e parameter	$a_{\min} = \overline{e} - t \cdot \sigma_e / \sqrt{n}$, $a_{max} = A_{31}; a_{min} < a_{max}$	The upper bound of the confidence interval of the parameter e is always equal to the maximum permissible energy value, that is, $a_{max} = initialEnergy$. This is due to the fact that nodes can migrate from one group to another; new nodes may appear with a residual energy value equal to the initial value. $a_{\min}$ - lower bound of confidence interval. $t * \sigma / \sqrt{n}$ - is the accuracy of the estimation. n - Total number of nodes.
1.7	The limits of the confidence interval for the L parameter	$b_{min} = L_{min}$, $b_{max} = \overline{L} + t \cdot \sigma_L / \sqrt{n}$	The lower bound for the parameter L is equal to the minimum required number of packets passed through the node in one time interval Lmin. These measures are taken because the mobile robot can exhibit selfish behavior, that is, refuse to participate in the network to save energy, which can artificially "understate" the boundaries of the interval. b_{max} - the upper bound of confidence interval for L parameter
2	**Determination of the probability of anomalous behavior of the mobile robot on the basis of the calculated confidence intervals.**		In order to calculate the mean square deviation and mathematical expectation, it is necessary to shorten the interval for which the value is calculated and take into account only the node parameters in the previous time interval L_{i-1}, e_{i-1} and L_i, e_i the node parameters for the current interval. Note: If you take the parameter values over the entire time interval, the standard deviation is too large, due to the large difference between the start and end values.
2.1	The mathematical expectation for the e parameter	$\overline{e_в} = (e_{i-1} + e_i) / 2$	$\overline{e_в}$ - mathematical expectation of the values of the e parameter for the sampling interval, which calculated for individual node
2.2	The mathematical expectation for the L parameter	$\overline{L_в} = (L_{i-1} + L_i) / 2$	$\overline{L_в}$ - mathematical expectation of the values of the L parameter for the sampling interval, which calculated for individual node
2.3	The variance for the e parameter	$D_{e_в} = \left(\sum_{i}^{N} (e_i - \overline{e_в})^2 \right) / n$	$D_{e_в}$ - variance for the sampling interval for e, which calculated for individual node.
2.4	The variance for the L parameter	$D_{L_в} = \left(\sum_{i}^{N} (L_i - \overline{L_в})^2 \right) / n$	$D_{L_в}$ - variance for the sampling interval for L, which calculated for individual node.
2.5	The standard deviation for the e parameter	$\sigma_{e_в} = \sqrt{D}_{e_в}$	$\sigma_{e_в}$ - the standard deviation for the sampling interval for the residual energy, which calculated for individual node.
2.6	The standard deviation for the L parameter	$\sigma_{L_в} = \sqrt{D}_{L_в}$	$\sigma_{L_в}$ - the standard deviation for the sampling interval for the L parameter, which calculated for individual node.

2.7	The probability of the value for parameter e falling into the confidence interval	$P_e(a_{\min} < e_i < a_{\max}) = = \Phi\left(\frac{a_{\max} - \overline{e_e}}{\sigma_{e_e}}\right) - \Phi\left(\frac{a_{\min} - \overline{e_e}}{\sigma_{e_e}}\right)$	P_e,- the probability of deviations the network load from confidence interval, which calculated for individual node. Φ is a Laplace function.
2.8	The probability of the value for parameter L falling into the confidence interval	$P_L(b_{\min} < L_i < b_{\max}) = = \Phi\left(\frac{b_{\max} - \overline{L_e}}{\sigma_{L_e}}\right) - \Phi\left(\frac{b_{\min} - \overline{L_e}}{\sigma_{Le}}\right)$	P_L - the probability of deviations the residual energy from confidence interval, which calculated for individual node.
2.9	The resulting probability value that the node is trusted	$P_{sum} = P_e * P_L$	To obtain the resulting probability value, it is necessary to use a combination of the values of P_e,, P_L of the direct value of trust P_{sum} in [17], an algorithm for combining confidence values using the Bayes theorem is presented.
3.	Deciding on the degree of trust in the node	$P_{sum} > 0,5;$ $P_{sum} = 0,5;$ $P_{sum} < 0,5.$	Assume threshold probability that the node is abnormal equal to 0.5. When the node reaches a value of 0.5, it is necessary to reduce its residual energy level by half, then the node is considered in an undefined state . Further, if the value of the confidence level reaches the level of 0.4, then it is necessary to consider the node malicious and reduce its energy level to zero, thus, the node is excluded from the network [18].

4. Experimental study, evaluation of the effectiveness of the developed method.

The model of a robot group in the simulation environment NS-2.35 was developed. Robots communicate with each other via wireless communication and use the TCP / IP protocol stack to transfer information. In particular, the UDP protocol is used for data transmission at the transport level, the ARP protocol is used to transmit control commands at the data link layer, the AODV protocol is used for routing the packets [19]. Figure 2 shows a group of mobile robots in the modeling system, which includes 10 nodes. Of these, one N4 node is a base station or a central server. The node N0 is the group leader and performs the functions of gathering information from the other robots and redirects it to the central server. The nodes of the group exchange information with each other and with the group leader [20]. In this case, nodes N6, N7, N8, N9 will conduct a DDoS attack starting from 50 seconds of network operation.

4.1. Implementation and detection of a DoS attack.

Conducting denial of service attack, the attacker creates a situation where the network node becomes unavailable to other nodes and cannot respond to their requests and work normally. An attack aimed at depleting resources, as a rule, creates such conditions for a node that it begins to lose more energy than in the absence of an attack. These attacks are interrelated. In fact, the goal of a DoS attack can be to completely disable a node by exhausting the node's resources. The developed model of a group of mobile robots is assumed that the nodes spend energy on the transmission and reception of packets. Therefore, an attacker "forces" trusted nodes to spend more energy than when working in normal mode, sending a large number of packets to the network.

Three types of situations were simulated. In the first case, an estimate was made of the energy consumed by network nodes in the absence of an attack. In Figure 3, this situation is represented by a blue chart marked with rhombuses.

In the second case, an attack was conducted on the network, while the traffic of the malicious node is $I_t \le I_m \le 2I_t$, where I_m is the traffic of the malicious node, It is the traffic of the authentic node. The third graph represents a situation where an attack is carried out intensively and $I_m > 2\ I_t$.

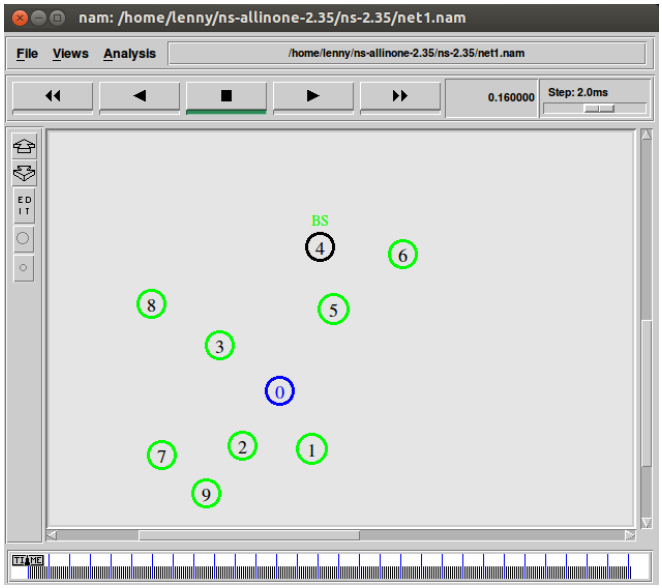


Figure 2. Group of robots in the simulation system NS-2.35

Figure 3 shows that during a non-intense attack, the energy level of the nodes will remain almost the same as for the case when the attack is not carried out. That is, in this case, the attack can be considered ineffective. The graph showing the change in the energy level during an intense attack shows a sharp drop in the energy level, which confirms the effectiveness of the attack. At the same time, the load of the attacker's node is more than twice the workload of authentic nodes. In this case, the developed method for detecting abnormal behavior allows us to identify a malicious node.

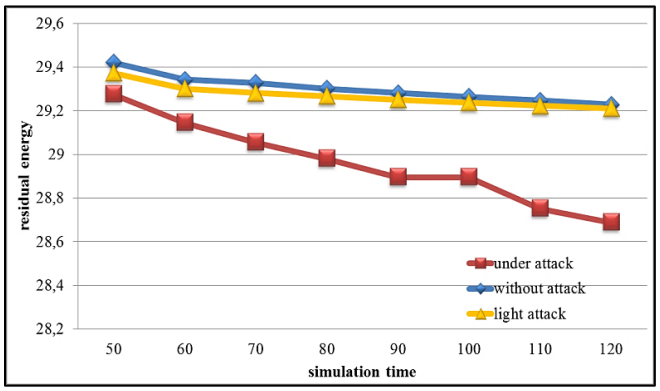


Figure 3. Change in the level of residual energy, depending on traffic intensity of network nodes.

The proposed method allows in a few seconds to detect a DoS attack, if it has a significant impact on the resources of network nodes and helps to increase the level of traffic. In Figure 4, a graph showing the level of detection of an attack, given that an attacker starts an attack after the 50th second of simulation, we can say that the attack is almost immediately detected. Since on an interval of time between 50-60th seconds the malicious node has a hit level in the confidence interval of 0.4 and is already blocked by the system for 60 seconds.

4.2. Implementation and detection of DDoS attacks.

The detection of a distributed denial of service attack is more difficult. This is due to the fact that when the number of malicious nodes prevails over the number of authentic nodes, the boundaries of the confidence interval are significantly expanded. Especially if malicious nodes conduct an attack with varying intensity. Nevertheless, the developed method is quite effective in detecting this attack. When the ratio of malicious nodes to trusted hosts is 4 to 5, the method allows to immediately detect all malicious nodes and block them already in the second time interval.

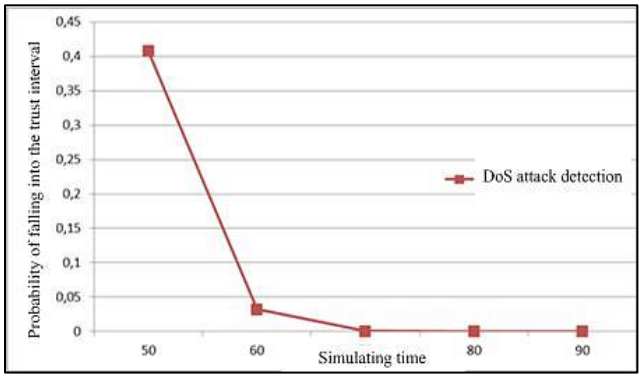
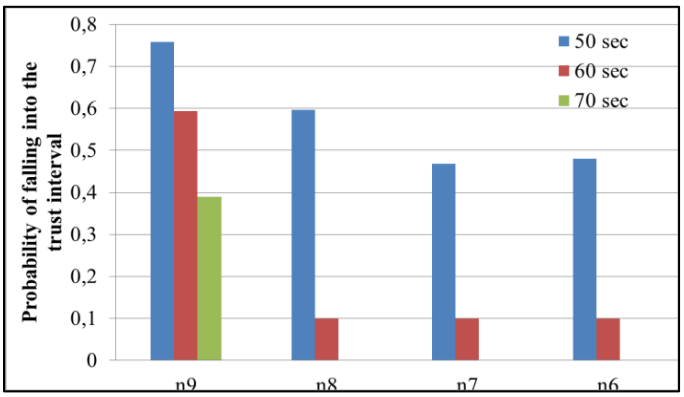


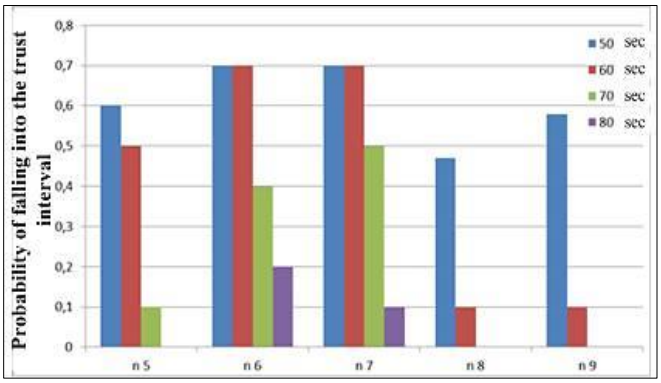
Figure 4. The probability of hit by the load and residual energy values of the malicious node in the trust interval

Figure 5 (a) presents a histogram showing the level of hit of current indicators e and L of malicious nodes in the confidence interval. When malicious and trusted hosts are in an equal ratio of 5 to 5, the quality of detection becomes worse.

Figure 5 (b) shows a histogram showing the detection level of malicious nodes. N9 and N8 nodes were also detected in the second interval, nodes N5 and N6 were detected in the third interval and node N7 in the fourth time interval, starting from the moment when the attack began. In general it can be said that the detection rate of 100%, but the rate of detection decreased.



(a)



(b)

Figure. 5. The level of detection of an attacker in a distributed denial of service attack for (a) four malicious hosts (b) for five malicious nodes and five authentic hosts

When the number of malicious nodes exceeds the number of trusted in the ratio of 6 malicious to 5 authentic, the detection level is 83%, i.e. one malicious node remains undetected. Figure 6 shows a histogram of the level of hit of current values of malicious nodes in the confidence interval. In this case, three nodes: N8, N9, N5 - are detected in the second time interval. One node N6 in the third interval and one node N10 in the 4th interval, only node n7 remains undetected on the fourth interval, most likely if the attack continues at the same rate, then this node will be detected on the 5th interval. But this time is high enough to detect an attack [21]. Nevertheless, the developed method shows a sufficiently high speed of detection of attack, even if the number of malicious nodes is more than the number of trusted ones.

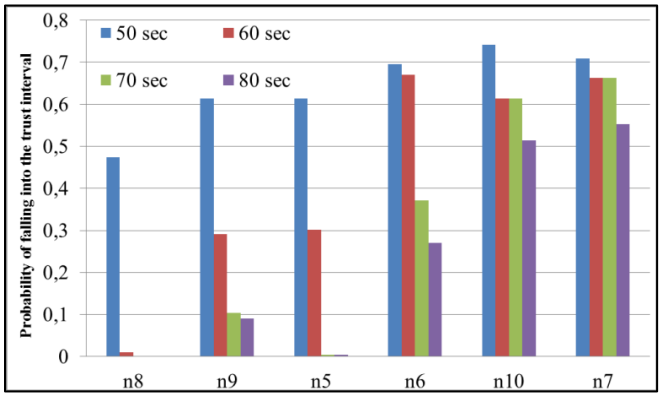


Figure. 6. The detection level of nodes with distributed attack denial of service for 6 malicious nodes and 5 trusted ones

4.3. Implementation and detection of the Sibyl attack.

The Sibyl attack is that an attacker is represented by several network nodes and tries to redirect most of the traffic to itself [22]. At the same time, it can make a destructive impact on the network by discarding messages, redirecting them to the wrong nodes, violating the routing scheme, or can passively listen for traffic.

At the same time to detect an attack, when an attacker does not have a destructive effect is quite difficult. In the works of the authors [23], as a rule, there are methods using hard protection: password protection, cryptographic protection, as well as signature analysis and group detection. These methods are used in networks MANET, IoF, P2P [24], which are not so much limited in resources as groups of mobile robots.

The developed method for detecting abnormal behavior shows the effectiveness of detection of the Sibyl attack, even if the attacker redirects the traffic to himself and does not take any further action. In this case, detection is possible by changing the load level of nodes that conduct an attack on neighboring nodes. In addition, the level of residual energy of the attacking nodes is significantly reduced. To assess the method, malicious N7-N11 nodes were added to the robot group in the NS-2.35 simulation system, which are called (Sybil1-Sybil5). Figure 7 shows the topology of the network, taking into account malicious nodes. The figure shows that the number of malicious nodes and the number of trusted ones, excluding the base station (BS) and the group leader (GL), corresponds to half of the network nodes.

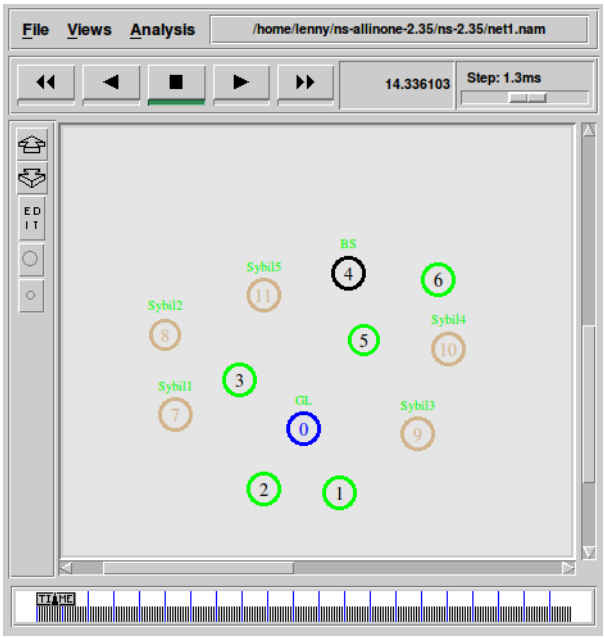


Figure. 7. The network topology for the implementation of the Sybil attack.

N7-N11 nodes redirect packets from neighboring mobile robots to themselves starting from 50 seconds, thus disrupting the network operation scheme. Initially, mobile robots will send packets to the group leader in a predetermined pattern; the leader of the base station sends packets. Thus, in the first 10 seconds of the attack, the method allows you to identify 2 malicious nodes N10 and N11. This is due to the fact that these nodes redirect more traffic to themselves. Further, starting from the 60th second, the detected nodes are blocked and nodes N7 and N8 are detected at the 70th second. The most difficult for detection was the node N9, this is due to its relatively low activity for redirecting traffic, at the time of detection the level of congestion of this node is less than twice the level of congestion of other nodes. Figure 8 shows a histogram representing the detection level of malicious nodes.

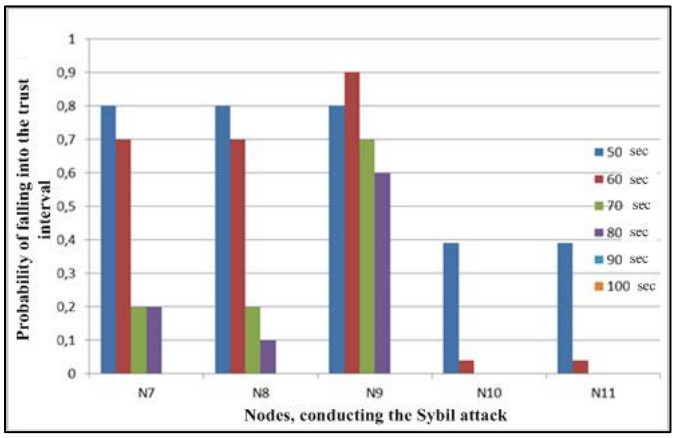


Figure. 8. detection level nodes conductive the Sybil attack

5. Conclusion

The issues related to the security of mobile robots and, in particular, group management of mobile robots, are currently being addressed by a limited number of scientists and institutions. Nevertheless, the subject of research is quite relevant, in connection with the widespread use of robotic systems. The developed method is a versatile tool for detecting anomalous behavior for a group of nodes, when it is possible to conduct an analysis of the behavior of most nodes and identify single or mass deviations from general behavior. Due to this, it is possible to increase the number of analyzed parameters for expanding the range of attacks. The method demonstrates a sufficiently high level of detection, namely it detects all malicious nodes within 30-40 seconds. Limitations of the method consist in the number of malicious nodes that conduct an attack on the network; their number should not exceed 60%, compared to the number of trusted ones. And also this method is applicable to a group of nodes that perform a similar task. In contrast to existing methods of detecting abnormal behavior, where one has to be comprehensive signature database or rules databases, store them, and then update the developed method makes it possible to detect anomalies in the current time, and depending on the current situation. This advantage is quite important because mobile robots can be used in different environments and for various tasks. In this case, in addition to networking protocols between mobile robots can change and environmental conditions, which in turn also influence the occurrence of anomalies and errors.

This method takes into account the threshold values, that is, the permissible level of anomalies, which reduces the number of false positives. In this case, the developed method allows to reduce the load on the mobile robot, it does not need to constantly exchange messages, monitor neighboring nodes and update, store the signature database. In the future study, it is proposed to add the node mobility parameter, to estimate the coordinates and speed of its movement. Evaluation of these parameters will allow to detect attacks such as interception by management, when an attacker, captures a trusted node and manages it independently.

Estimation of position and speed of movement will detect abnormal behavior nodes.

Acknowledgment

The work was supported by the Ministry of Education and Science of the Russian Federation (Initiative Science Projects No. 2.6244.2017 / 8.9).

References

[1] A. Basan, E. Basan, O. Makarevich. “A Trust Evaluation Method for Active Attack Counteraction in Wireless Sensor Networks”. in 9th International Conference on Cyber-enabled distributed computing and knowledge discovery. Nanjing, China.2017.P. 369-372. DOI: 10.1109/CyberC.2017.14.

[2] Basan A.S., Basan E.S. “Threat model for mobile robot group management systems”. System synthesis and applied synergetics. Collection of proceedings of the VIII All-Russian Scientific Conference. - Sistemnyy sintez i prikladnaya sinergetika. Sbornik nauchnykh trudov VIII Vserossiyskoy nauchnoy konferentsii. Rostov-on-Don: Southern Federal University. 2017. C. 205-212. - (In Russ.)

[3] H.S. Kim, S.W. Lee. “Enhanced novel access control protocol over wireless sensor networks”. IEEE Transactions on Consumer Electronics. 2009. № 55 (2). pp. 492 - 498.

[4] Branitsky A.A., Kotenko I.V. “Analysis and classification of methods for detecting network attacks”, Information security. Proceedings of SPIIRAN - Informatsionnaya bezopasnost'. Trudy SPIIRAN.2016. №2(45). pp.207-244.(In Russ.)

[5] Petrovsky O. “Attack on the drones”. Virus bulletin conference. 2015. pp. 16-24.

[6] Garber L. Robot OS: “A New Day for Robot Design”. Computer. № 46 (12). 2013. pp. 16-20.

[7] Kozhemyakin I.V., Putintsev I.A., Semenov N.N., Chemodanov M.N. “Development of an underwater robotic complex, using open simulation tools, supplemented with a model of hydroacoustic interaction”. News of SFedU. Technical science. Section II. Marine robotics. - Izvestiya YUFU. Tekhnicheskiye nauki. Razdel II. Morskaya robototekhnika. 2016. № 1 (174). pp.88-99.(In Russ.)

[8] Vuong T. P., Loukas G., Gan D., Bezemskij A. “Decision tree-based detection of denial of service and command injection attacks on robotic vehicles”. 2015 IEEE International Workshop on Information Forensics and Security (WIFS) 2015. pp. 1-6.

[9] Bezemskij A., Loukas G., Richard J. Gan D. “Behavior-based anomaly detection of cyber-physical attacks on a robotic vehicle”. 15th International Conference on Ubiquitous Computing and Communications and 2016 8th International Symposium on Cyberspace and Security. 2016. pp. 61-68.

[10] Mitchell R., Chen I.R. “Adaptive Intrusion Detection of Malicious Unmanned Air Vehicles Using Behavior Rule Specifications”. IEEE Transactions on Systems, Man, and Cybernetics: Systems. №44 (5). 2014. pp. 593 -599

[11] Monshizadeh M., Khatri V., Kantola R., Yan Z. “An Orchestrated Security Platform for Internet of Robots”. Springer International International Conference on Green, Pervasive, and Cloud Computing. 2017. pp. 298– 312.

[12] Basan A.S., Basan E.S., Makarevich O.B. “Method of counteracting active attacks of an attacker in wireless sensor networks”. News of SFedU. Technical science. №5 (190).2017. pp. 16-25. (In Russ.)

[13] Basan A., Basan E., Makarevich O. “Methodology of Countering Attacks for Wireless Sensor Networks Based on Trust”. 8th International Conference on Cyber-Enabled Distributed Computing and Knowledge Discovery (CyberC).Chengdu.2016. pp.409 – 412.

[14] Schoch E., Feiri M., Kargl F., Weber M. “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. 2008. pp. 34 - 41.

[15] He W., Yang S., Teng D., Hu Y. “A Link Level Load-Aware Queue Scheduling algorithm on MAC layer for wireless mesh networks”. International Conference on Wireless Communications & Signal Processing.2009. Nanjing, China.pp.1-16

[16] Basan A.S., Basan E.S., Makarevich O.B. “Development of the Hierarchal Trust management System for Mobile Cluster–based Wireless Sensor Network”. Proceeding SIN '16 Proceedings of the 9th International Conference on Security of Information and Networks. 2016. pp. 116-122.

[17] Mohammad Momani. Bayesian Fusion Algorithm for Inferring Trust in Wireless Sensor Networks // Journal of Networks 5(7). 2010; C. 815-822. DOI: 10.4304/jnw.5.7.815-822

[18] Abramov E.S., Basan E.S. “Development of a model of a protected cluster wireless sensor network”. News of SFedU. Technical science. - Izvestiya YUFU. Tekhnicheskiye nauki.2013. № 12(149). pp. 48-56. (In Russ.)

[19] Ferronato J. J. Sandini Trentin M. A. “Analysis of Routing Protocols OLSR, AODV and ZRP in Real Urban Vehicular Scenario with Density Variation”. IEEE Latin America Transactions. 2017. № 15 (9). pp. 1727 – 1734.

[20] Pshikhopov V.Kh., Soloviev V.V., Titov A.E., Finaev V.I., Shapovalov I.O. “Group management of mobile objects in uncertain environments”. Ed. V.H. Pshihopova. M.: FIZMATLIT. - Pod red. V.KH. Pshikhopova. M.: FIZMATLIюT 2015. – pp. 233-270. (In Russ.)

[21] Sargeant I., Tomlinson A. “Maliciously Manipulating a Robotic Swarm”. Int'l Conf. Embedded Systems, Cyber-physical Systems, & Applications. ESCS'16. 2016. pp. 122- 128.

[22] Abbas S., Merabti M., D. Llewellyn-Jones, K. Kifayat. “Lightweight Sybil Attack Detection in MANETs”. IEEE system journal, №. 7, (2). 2013. pp 236-248.

[23] Patel S.T., Mistry N.H. “A review: Sybil attack detection techniques in WSN”. 4th International Conference on Electronics and Communication Systems (ICECS). 2017. pp. 184 – 188.

[24] Wang G., Musau F., Guo S., Abdullahi M. B. “Neighbor Similarity Trust against Sybil Attack in P2P E-Commerce”. IEEE transactions on parallel and distributed systems. № 26 (3). 2015. pp. 824-833.