Original Article: Algorithm Based on Trap Packet to Detect Black Hole Attack in Ad-Hoc Networks Using Common Methods

Shahram Mohammadi*

Department of Computer Engineering, Mahalat Branch, Islamic Azad University, Mahalat, Iran

Use yor device to scan and read the article online

Citation S. Mohammadi*, **Algorithm Based on Trap Packet to Detect Black Hole Attack in Ad-Hoc Networks Using Common Methods.** *J. Eng. Ind. Res.* 2023; 4(1):31-43.

https://doi.org/10.48309/jeires.2023.1.4

Article info:
Received: 2023-03-30
Accepted: 2023-06-16
Available Online:
ID: JEIRES-2305-1080
Checked for Plagiarism: Yes
Editor who Approved Publication:
Alireza Bozorgian

Keywords:
Ad-Hoc network; Router; Radio waves; System.

ABSTRACT

Mobile ad hoc networks include sets of nodes that can freely communicate with each other without having any network infrastructure and through radio frequencies. These networks' speed of establishment and unstructured nature has made them critical in various fields, especially military and emergency applications. The issue of security in these networks is one of the most important research topics today. Mobility of nodes, mobility of communication, dynamic change of network structure, lack of centralized management to check behaviors and functions, lack of specific defense lines, and limitation in consumption power of nodes provide a suitable platform for various attacks against these networks. The attacks in these networks are somehow different from those in other networks, and of course, the systems used to detect attacks in these networks are different from those in common wired networks. Mobile ad hoc networks are collections of mobile nodes that can be dynamically formed anywhere and anytime without network infrastructure. Most of these node's act as routers and hosts at the same time. This property has made it possible to use these networks when forming a network with a fixed and predefined structure, such as military cases or floods, is impossible. Communication between nodes in these networks is done through radio waves, and if a node is in the radio range of another node, it is considered a neighbor of that node, and otherwise, if there is a need for communication between two nodes that are in the radio range of each other are not, the help of other nodes can be used in this case. Therefore, the communication between nodes in these networks is somehow based on trust and cooperation between nodes. What needs to be paid special attention to in the applications of these networks is the limitation of the resources used in them. Therefore, the evaluation criteria of these networks differ from those of wired networks.

Introduction

Identifying the routing protocols of mobile ad hoc networks is necessary to understand the security problems of these networks. The routing protocols of these networks differ from wired networks due to the high updating of routes, the movement of nodes, and the limitation of the communication range. Therefore, the routing protocol used in these networks is necessary to consider the following [1]:

***Corresponding Author: Shahram Mohammadi,** (*mohamadi.sh1986@gmail.com*)

1- Since centralized routing involves much overhead and is not scalable, it is necessary for its routing algorithm to be distributed entirely.

2- It should be compatible with the significant change in network alignment due to the large movement of nodes [2].

3- The calculation and maintenance of the routes must include the minimum number of routes, and the existing nodes must have the fastest access to the routes.

The demand-based distance vector protocol, which is defined as an on-demand protocol, has route request and route response packets. This protocol is not based on routing from the origin and uses the routing table for intermediate nodes [3].

The general procedure is as follows:

When a source node needs a route to a destination node, and there is no valid route in the routing table, the source node broadcasts a route request packet to the destination node. When each node receives the route request packet, it creates or updates a reverse route to the source node in the routing table, and if it does not have a valid route to the destination node in the routing table, it rebroadcasts the route request packet. When the route request packet arrives from the source node to the destination node via broadcast, the destination node creates or updates the reverse route and unicasts a route response packet with an incremented sequence number on the reverse route. When the route response packet arrives at the source node along the reverse path, it creates or updates a forward path to the destination, and communication begins [4].

Statement of the problem

The routing structure of mobile ad hoc networks, which is based on trust between nodes, provides a good and excellent opportunity for attackers to participate in the routing process, cause routing deception and ultimately disrupt the routing. The self-structuring property of mobile ad hoc networks will also cause attacks [5]. The structure of this network is such that when a node enters, it is necessary to assign an ID to it by obtaining information from other nodes. A malicious node can disrupt this or take the ID assigned to the node for itself [6]. The use of attack prevention methods in these networks faces more limitations. For example, encryption and validation methods are used in these networks for defense purposes, but due to the structure of these networks, there is a possibility that a node will be stolen, and if there is a private key for it, it will be revealed. Therefore, these methods will be useless. Since there is no centralized structure for nodes in mobile ad hoc networks, nodes cannot trust the security facilities of the network, and each node needs to consider its own security [7].

In mobile ad hoc networks, you can use a particular firewall. This firewall allows only nodes with physical addresses to connect to the network. The absence of this option for mobile ad hoc networks makes it easy for attackers to enter the network. In the case of an attack on the network, in the best case, the attacking node can find out the existence of confidential information by checking the network information, and in the worst case, it can cause a disconnection between the nodes. Due to the lack of a specific access point to control the entry and exit of packets in mobile ad hoc networks, there is no suitable place to install a firewall in a way that checks the total network traffic. Mobile nodes can easily enter or leave the network without any restrictions being imposed on them. Routing algorithms that operate on mobile ad hoc networks require complete trust between nodes, which reduces the security factor in these networks. Also, not having a centralized structure prevents the existence of a central supervisor in the system [8].

The black hole attack is one of the most known attacks in mobile ad hoc networks. This attack is applied through one of the nodes in the network. Because an attacking node from outside the network introduces itself as a node inside the network. This node sends a favorable route response to each received route request regardless of its routing table and whether it has a route to the destination node. This shortens the sending of route response packets compared to other nodes, and network nodes find this node as a suitable and short path for sending packets and sending their packets from this node's path. In this case, a black hole has been created, and a node known as a black hole, instead of sending packets to its destination, receives information or discards them. If the black hole node introduces itself as a suitable path for all network nodes, this will cause the loss of all network packets, which will ultimately cause a denial-of-service attack [9].

The importance and necessity of research

Today, moving case networks are more widely used and popular than before. Therefore, paying attention to the security category in such networks is of great importance to the extent that it has become one of the essential topics in scientific and research circles in information exchange. The presence of malicious attacks has seriously challenged the security of networks, and the black hole attack is one of these types of attacks. Therefore, it is necessary to provide suitable methods and algorithms to detect and prevent this attack [10].

Intrusion detection systems

An intrusion detection system is one or more systems that can detect specific changes and behaviors in a host or network (Figure 1).

A) History of intrusion detection systems: With the increase in speed, efficiency, number, and communication of computers in the 1970s, the need for security systems grew considerably. In 1977 and 1978, the international standard organization organized a meeting between governments and inspection bodies, the result of which was preparing a report on the state of security, inspection, and control systems at that time. At the same time, due to concerns about the security situation of its systems, the US Department of Defense started a very detailed investigation into the inspection and security of computer systems. This work was done by a person named Anderson. Anderson is the first person who presented an article on the necessity of automatic security inspection of systems.

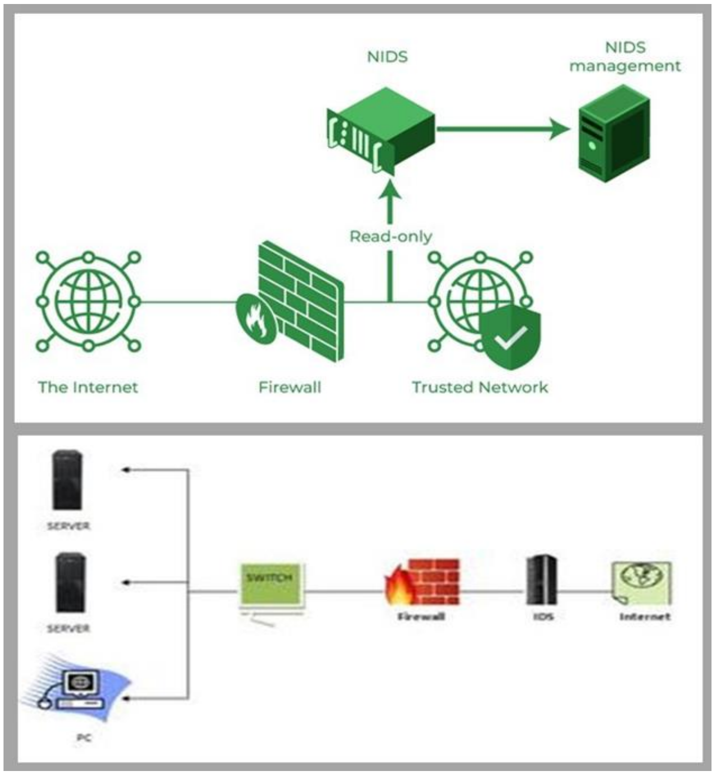

Figure 1: Intrusion detection systems

His report, prepared in 1980, can be introduced as the initial core of the concepts of intrusion detection. In this report, mechanisms were introduced to inspect the security of the systems, and it was also determined how to deal with them in the event of a malfunction in the system. From 1984 to 1986, Peter Namnen and Dorothy Denning researched the security of computer systems, the result of which was the production of a real-time intrusion detection system based on expert systems, which was named IDES. In this project, a combination of anomaly detection and abuse detection was investigated. The idea presented in this project was used as the basis of many intrusion detection systems created after that. Anderson's report and the research conducted on the IDES project started a chain of research related to intrusion detection systems. In the following, many prominent systems that came into being from that date onwards are discussed [11]:

A1- Audit Analysis Project: In 1984-1985, a project group was started by order of the US Navy. This project aimed to provide an automatic method to collect shell-level data for the Unix operating system. The collected data were then analyzed. In this project, the ability to separate desirable behavior from undesirable behavior was shown.

A2- Discovery: It is a system based on expert systems created to diagnose and prevent problems in the information bank of TRW credit company. This system was somewhat different from the intrusion detection systems of its time. In this system, unlike other intrusion detection systems that examine the activities of the operating system, examines the logs of information banks. The purpose of the Discovery work was to prepare a report of unauthorized operations with the database. In this project, statistical models were used for data analysis and written in Kobel language.

A3- Haystack: This project was carried out by the haystack laboratory (1989 to 1991) and tractor applied science (1987 to 1989) at the request of the US air force. The goal of implementing haystack was to provide security agents with the ability to detect unauthorized use of air force SBLC computers [12].

A4- MIDAS: This item was implemented by the national security center. In this system, information was collected and classified. Then this information, each class representing a relationship, was compared with the behavior of users. By making this comparison, they could identify wrong behaviors and unusual behaviors. MIDAS was used by Moore's LISP loss. In this system, statistical methods and expert systems were used for information processing.

A5- NSM: This item was implemented by the University of California. This system can be called the first intrusion detection system that uses network information as a source of information. Before this system, other intrusion detection systems performed actions based on information collected from the operating system or program logs.

A6- Wisdom and Sense: This case is an anomaly detection system that was implemented by a security group. This system is the second step in implementing network-based intrusion detection systems. This system was implemented on the Unix operating system and for VAX/VMS machines. In W&S, rule-based expert systems were used, which differed from the systems of their time in terms of performance.

A7- DIDS: Until 1990, most intrusion detection systems operated based on the host, which means that they collected information from the operating system level or applications and analyzed them. With the advent of NSM, this limitation was removed, and intrusion detection systems began to work based on information collected from network traffic (Figure 2). With the expansion of the Internet and the emergence of related security problems, it became necessary to create a system that combines host-based and network-based models [13].

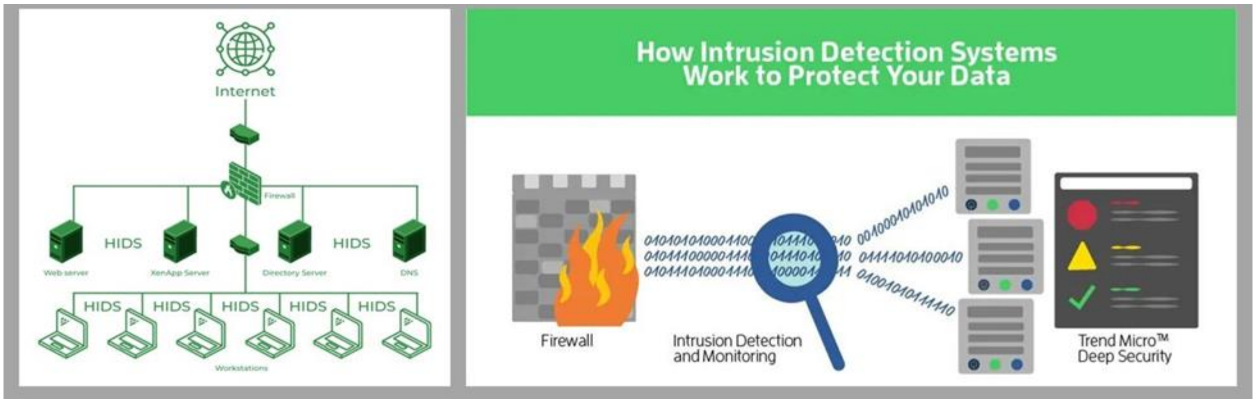
Internet
Firewall
HIDS
HIDS
Web server
XenApp Server
Directory Server
DNS
HIDS
HIDS
HIDS
HIDS
HIDS
Workstations
How Intrusion Detection Systems Work to Protect Your Data
Firewall
Intrusion Detection and Monitoring
Trend Micro™ Deep Security

Figure 2: Intrusion Detection

Architecture of intrusion detection systems

An intrusion detection system generally has the following parts [14]:

1- Information gathering department: This department is responsible for collecting information. For example, this section should be able to detect changes in the file system or network performance and collect the necessary information.

2- System review section: Every intrusion detection system must have a section that reviews the system's performance. In this way, it is possible to ensure the correct operation of the system.

3- Control and management section: through this section, the user can communicate with the intrusion detection system and give the necessary commands to it.

4- Analysis section: This section of the intrusion detection system is responsible for reviewing the collected information. According to the placement of each part of an intrusion detection system, different architectures are created for it.

Regarding the architecture of intrusion detection systems, there is another point of view; from this point of view, two general architectures can be considered:

The protected system and the intrusion detection system are in one place.

The system under protection and the intrusion detection system are placed separately.

Separating the intrusion detection system **from the protected system has advantages:**

- ✓ Preventing the deletion of records stored by the intrusion detection system.
- ✓ Preventing information from being changed by an intruder.
- ✓ Increasing efficiency by reducing the processing load on the system under protection.

Methods of receiving information

The first requirement of intrusion detection systems is the existence of an information source. This resource can be considered as an event producer. Information sources can be classified in different ways. In intrusion detection systems, these sources are classified according to their location. According to this criterion, there will be two general categories [15].

1- Based on the host: In this category, information is collected based on the resources inside the host, primarily at the level of the operating system. These sources include logs and inspection sequences if the case is viewed from a higher perspective.

2- Based on applications: In this category, information is collected based on running applications. These sources include event logs for applications or other information stored based on them.

3- Goal-based: this category is different from other categories. Because in this category, the system based on the goal produces its own information, which means that the system itself determines the essential objects of the system and obtains specifications for each one. Then it is alternately used as a source of information by comparing these specifications with the obtained values.

4- Network-based: In this category, passing packets are collected at the network level as a source of information. This action is done by placing the network card in random mode.

Analysis methods

In intrusion detection, after introducing information sources and determining their classification, the following need is to determine an analyst. In the analyzer, information is extracted from information sources and analyzed according to security policies and types of attacks. In intrusion detection systems, analysis methods are divided into two general categories: abuse detection and anomaly detection or a combination of them [16]:

1- Detection of abuse: in this method, the analyst looks for a sign that indicates a wrongful act. To do this, the information is first filtered to find patterns indicating the attack type or other security policies. In detecting abuse, this work is done by pattern detection mechanisms. Currently, most intrusion detection systems use this method.

2- Abnormality diagnosis: In this method, the analyzer looks for unusual cases. To do this, the collected data is analyzed to find patterns that indicate unusual actions. In some cases, these two methods are used together. In these systems, the anomaly detection method detects new and unknown attacks, and abuse detection assumes the task of protecting the anomaly detection system. This ensures that the collected information and patterns are safe for the anomaly detection system.

Scheduling

One of the issues related to data analysis is scheduling. Data analysis can be in real-time and batch mode [17].

1- Batch mode: The meaning of batch mode analysis is that information related to a period is collected and then given to the analyzer. The use of this type of scheduling has been used in old systems. Because the communication bandwidth and processing power in the old systems were insufficient to allow the systems to function in real-time.

2- Real-time: with increasing processing power and communication bandwidth, most new systems use this method. In this method, the source of information is given to the analyst with every event that occurs or in any short time interval.

Answer methods

Another factor in intrusion detection systems is the practical way the detector reacts. Intrusion detection systems work against incidents in two general ways. These two methods are response and active response.

1- Responsiveness: The reaction method considered for an intrusion detection system causes the creation of different plans and implementationsconcerning the person responsible for the damage. The use of this method is one of the debatable issues in the field of intrusion detection (Figure 3).

2- Active response: In intrusion detection systems, the active response occurs when the result of the analysis is actionable. The most common type of active response is storing information in a log file and preparing a report from them. These data can be used in different ways for different people. Another possible solution is to change the state of the system that has been attacked. In addition to these two cases, there are other active solutions, such as blocking the attacker, changing the firewall's configuration [18].

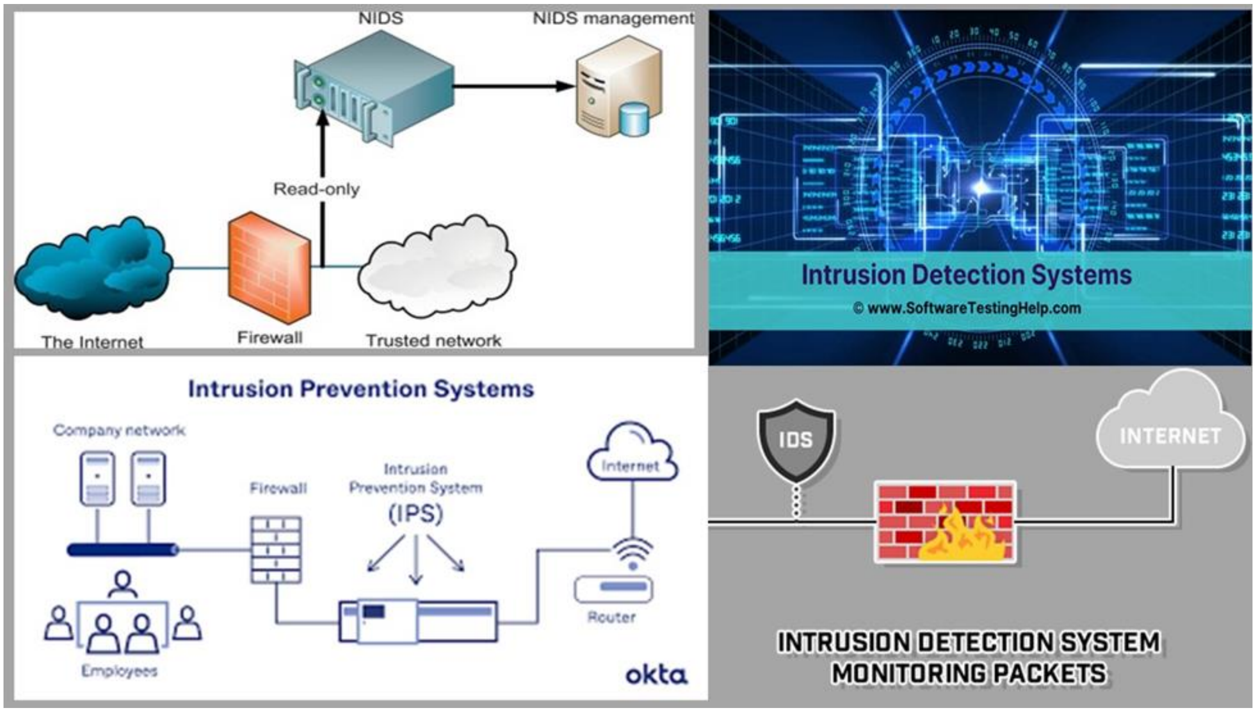
NIDS
NIDS management
Read-only
The Internet
Firewall
Trusted network
Intrusion Detection Systems
© www.SoftwareTestingHelp.com
Intrusion Prevention Systems
Company network
Firewall
Intrusion Prevention System (IPS)
Internet
Router
Employees
okta
IDS
INTERNET
INTRUSION DETECTION SYSTEM MONITORING PACKETS

Figure 3: Intrusion Prevention System

System control

Another issue related to intrusion detection systems is the issue of system control. To do this, three main methods are used [19]:

1- Central: The management system and report generation are centralized in this model. In this method, a central management system controls the intrusion detection system. Using this method has prerequisites. For example, information exchange between the center and other departments should be done safely. In addition, there must be a way to determine which part of the system is active and which part of the movement is stopped at any given moment. Another issue related to the central model is sending the final conditions to the end users as a concept.

2- Use of network management facilities: To solve the problems of the central method, intrusion detection can be made as a function of the network management system. In this method, information collected by network management systems can be used as a source of information for intrusion detection systems.

3- Distributed: Another way to solve the problem of the centralized mode is to use the distributed model. In this case, the analyzer is not centralized. The method that can be used in this model is moving agents. In this case, the analyzer moves to the network level and analyzes the results collected on different systems.

Information sources

The first requirement for any intrusion detection system is to provide input data. These data are provided in different ways from different sources. In intrusion detection systems, sources are divided into two general categories according to their distribution, based on which two types of intrusion detection systems are created:

A) Host-based intrusion detection system.

B) network-based intrusion detection system.

A) Information sources of the host-based system: In this category of intrusion detection systems, information is provided by the specifications and data of the operating system or application programs.

1- Operating system inspection sequence: The first source of information that intrusion detection systems use is operating system inspection sequences. The audit trail is provided by a section called the inspection section, which is a subset of the operating system. The audit trail includes information about system activities. This information is sorted by time and stored in one or more files called inspection files. Each audit file consists of a set of audit records, each representing an event in the system. These records are created by user activities or processes. The manufacturers of operating systems have paid attention to two issues in the design of inspection sequences [20]. One is that the records in the sequences are self-contained so that there is no need for another record to interpret it, and the other is that additional information is removed from the sequences, meaning that information for the same event is not stored in different records. Although inspection sequences are used as the most important source of information for intrusion detection systems, research has shown that these sequences may not contain important information used by intrusion detection systems. Also, the sequence transparency is low, but despite these problems, many intrusion detection systems use these sequences. The most important reason for these systems is the security of the traces and the protection that is performed on them by the operating system, and the other is that these traces are suitable detectors for system events. Audit trails are stored at both the kernel and user levels. The sequences of the kernel layer include the arguments of system calls, and their return values, and the sequences of the user layer specify the description of the higher level of events and applications.

2- System logs: System logs are files that specify system events and various system settings. These logs are at a lower level in terms of security compared to the inspection sequences produced by the kernel. This weakness is due to several reasons: First, the system log generator program is a user-level program that is less secure compared to the operating system. Second, the information generated by the log generator program is stored by the file system, which is less secure compared to the audit trails, and third, the logs prepared by the log generator are in text form, while the information of the inspection trails is They are saved in encrypted form. Despite all these weaknesses, due to the simplicity of using these logs, many intrusion detection systems use them, and in cases where using inspection sequences is not an easy task, you can benefit from the presence of logs as a source of information [21].

3- Application information: In the previous two sources, the information generated was at the system level, but the system activities are often more secure than the application programs. For this reason, it is necessary to obtain information for applications. The information generated by applications is another source of information that is used by intrusion detection systems. For example, among the sources of information generated by the application, we can refer to the information generated by information banks. In many organizations, databases are one of the most essential sources that are attacked. Therefore, the information produced by them is critical.

4- Goal-based review: The goal-based review method is a particular case of host-based review. In this case, it is assumed that if there are no-level sequences, it should be possible to generate and use logs. To do this, first of all, how to define and implement the logs should be determined. For this purpose, significant objects are generated in a specific system, and then, with a review mechanism, information about those objects is generated. This information, for example, can indicate the integrity of the object or its CRC code. In this way, any change in the information obtained from the desired objects, the corresponding event, is saved and maintained.

Network-based system information sources

Network traffic is one of the most common sources of information for intrusion detection systems. In this case, data is collected from network traffic and analyzed. The information obtained from the network traffic is important from different aspects. One of the reasons is the rate of arrival of packages. In most cases, the rate of incoming packets is insufficient to cause system performance problems. Another advantage of using network information is that receiving information is hidden from the user's view. In addition to these cases, by examining the network information, attacks can be detected that could not be detected by examining the information of the operating system or the application program. In intrusion detection systems that use network traffic as a source of information, packets passing through the network are received by the network card. This is done by placing the network card in an irregular mode. With this, in addition to receiving packages related to that system, other packages are also received by the card. Special facilities have been provided to receive packages from the network. As an example, we can mention the libpcap library. Many intrusion detection systems use this library to receive packets [22].

Intrusion analysis and detection techniques

The main work of intrusion detection systems is data analysis. The analysis process can be divided into three different phases [9]:

A) Building the analyzer engine.

B) Analyzing the data.

C) return and correction.

Each of the first two phases consists of three steps: data pre-processing, data classification, and final processing.

A) Building the analyzing engine: The first phase of the analysis is building the analyzing engine. In this phase, three actions of pre-processing, classification, and final processing occur. To do this, the following steps are performed:

1- At first, data is collected as a sample. In the case of abuse detection, this information includes characteristics of attacks, vulnerable points, and intrusions. This information for abnormality diagnosis includes system behavior in a normal state.

2- The next stage of data collection is to perform pre-processing on them so that they can be converted into a form that can be used.

3- After the pre-processing, handling, and building of the attack model are done. Abuse diagnosis data are classified based on rules and patterns, and anomaly diagnosis data are classified based on signs and behavioral characteristics of users and the operating system.

4- After making the desired models, they are stored somewhere. In this way, the analyzer engine is made.

B) Analyzing the data: The second phase is to perform the analysis. This work is done by the analyzer engine built in the previous phase and applied to the input data. The process of doing work in this phase is as follows:

1- Receiving new data that can be produced by any of the information sources.

2- Performing pre-processing on new data to be checked with the models available in the analyzer engine. In detecting abuse, this work is done by converting the information to the desired format, and in diagnosing anomalies, this work is done by modifying the signs and behavioral characteristics of users and the system.

3- Analysis is done on pre-processed information. This is done by comparing the signs and signs already stored in the analyzer engine.

C) Return and correction: In this phase, which proceeds parallel to the previous phase, correction is done on the analyzer engine. In the case of abuse detection, this work is done by updating the patterns and signs of attacks, and in the case of anomaly detection, the characteristics made of the behavior of users and the system are updated. Since intrusion detection methods are divided into two general categories of abuse and anomaly detection, specific techniques are used to detect intrusion. In this section, the techniques used in each are described.

Answer techniques

The responses that intrusion detection systems can have been classified into two general categories: active and passive. In active mode, for example, preventing an attack or blocking the system is possible. In inactive mode, the system saves problems and reports them. In a system, both types can exist at the same time. One of the essential parts of any intrusion detection system is to determine what type of attack has occurred and what response should be given according to that attack.

A) Active response: In the active response, the system must react after identifying the type of attack. There are different ways to respond, three of which are mentioned below.

1- Reciprocal action against the attacker: The first response mode is counteraction against the attacker. The most obvious way, in this case, is to go in reverse to find the source of the attack. After finding the source of the attack, you can stop it or cut off the connection with it. The responses in this regard can be automatic or activated by a person [23].

2- Changing the system: One of the active response methods is to change the system conditions. Although this type of response is the quietest, it is also the optimal mode. The general idea of this method is to cover the loopholes from which the attacks take place. The defense systems in self-healing systems are the same as the body's defense systems, so the system itself tries to repair its problems.

3- Gathering more information: The third response mode is gathering more information about the attack. This mode is used when the system under protection is of particular importance, and the main owner of the system wants to get the main treatment of the attack. Sometimes the main system is replaced by another system used as a place for an attack. This system has different names, such as "honey pot" and "fish bowls". This system is equipped with all the specifications that the main system has. In this way, collecting more information about the attack is possible based on the attacks that replace the system.

The evaluated parameters

The parameters required to evaluate the efficiency of the proposed method are as follows:

1- **Packet loss rate:** It equals the total number of packets that did not reach the destination.

$$\frac{S = \sum_{i=\text{١}}^{n} S_i - \sum_{i=\text{١}}^{n} R}{\sum_{i=\text{١}}^{n} S_i}$$

S is equal to the total number of packets sent, and R is equal to the total number of packets that reached the destination safely.

Operating power can be calculated using the following formula:

$$\text{Throughput[kbps]} = \frac{\text{R}=\sum_{i=1}^{n} R_i}{T} * \frac{\mathbf{8}}{\mathbf{1000}}$$

End-to-end delay: packet arrival time – packet sending time = E end-to-end delay

Total network delay:

$$Sum\ Delay\ of\ Network = \sum_{i=\text{١}}^{\text{n}} \text{E}$$

n is the total number of nodes that have reached the destination safely.

Normal routing load: The ratio of total routing packets that have reached the destination to the total number of packets that have reached the destination.

- ✓ Existence of a malicious node and not using the suggested method.
- ✓ The existence of two malicious nodes and not using the proposed method.
- ✓ Existence of a malicious node and using the proposed method.
- ✓ The presence of two malicious nodes and the use of the proposed method.

Conclusion

The main goal of this research was to provide a new and efficient method to detect black hole attacks. Whether the proposed method can detect the black hole attack or not is enough and acceptable to evaluate its efficiency. Because as explained further, resources are limited in mobile ad hoc networks, and the speed of establishment and low cost were among the reasons that justified the creation and use of these networks despite a series of disadvantages. So, if our proposed algorithm strengthens the advantages and covers the disadvantages of these networks, it is desirable and acceptable. In the previous chapter, some of the evaluation parameters of case networks were introduced, and the results obtained from the simulation of a case network in different modes were explained with the help of tables. Then, with the help of graphs, these results were evaluated and interpreted. At each stage, the evaluations have been made only for a specific parameter in different modes where the network was tested, and it does not challenge the overall efficiency and application of the proposed method, and this is the issue that we will discuss further. Also, when there are two malicious nodes in the network, the difference in packet loss in the states of using and not using the proposed method can be seen. Therefore, according to the above explanations, it can be concluded that the proposed method is efficient most of the time and has reduced the packet loss rate compared to the case where this method was not used, and it has effectively detected malicious nodes.

In order to more accurately evaluate the proposed method, we will compare its performance with the method used to identify the black hole attack using the fuzzy Apriori data mining algorithm. In this method, the behaviors of malicious and healthy nodes are first analyzed, and the resulting information is collected. Each node controls the behavior of its neighbors in terms of received packets. After receiving the route response packet from the neighboring node and performing a series of calculations, each node may suspect the neighboring node and request a vote about the shared node, and other nodes, upon receiving the polling packet, express their opinion about the suspicious node for They send requesters. In the following, the opinions of all nodes are collected, and the requesting node is checked for health using the fuzzy Apriori algorithm with a confidence level of 75% and fuzzing two parameters α (the rate of sending and receiving control packets) and β (the rate of sending and receiving data packets). Suspicious nodes, and finally, if the suspicious node is malicious, it is introduced to all the nodes in the network. In order to compare the proposed method with the mentioned method, both algorithms have been implemented in the NS2 simulation environment. It can also be concluded that the proposed method presented in this project is more successful than the Apriori method in preventing the loss of more packets by the black hole node and was able to detect the attack quickly and correctly and prevent the loss of data by this attack. Perhaps the most obvious reason is that in the Apriori method, the black hole node is not searched from the beginning, and this action takes place after a node suspects the performance of its neighbor node, and until then, the original data packets are discarded by the black hole node. The total delay of the network in the case where the Apriori method is used to detect the black hole attack is lower than the proposed method based on the trap packet. Since the final delay of the network is always one of the main and most obvious parameters for evaluating algorithms specific to data network transfers, it should be said that in this particular case, the proposed method is weaker and less efficient, and the overall delay of the network is higher than the other method. It can be concluded that the normal routing load in the case of using the proposed method is lower than the Apriori method in all simulation times, and since this amount is obtained from the ratio of control packets to main data packets, this amount is better. It will be more acceptable. Because the use of more control packets for routing operations will increase the cost of transmission in the network, and this will not be a favorable situation, which unfortunately shows itself more in the Apriori method. The reason for this situation can be seen as the inherent nature of this method. Because in this method, a node will send opinion packets to other nodes in the network to check and measure the health of a suspicious node, and other nodes also express their opinion to the requesting node through other control packets. The ratio of control packets to data packets will increase and add additional load to the network.

References

[1] Y. Chen, C. Bellavitis, *Journal of Business Venturing Insights*, **2020**, *13*, e00151. [Crossref], [Google Scholar], [Publisher]

[2] S.B. School, A. Group, Direct and indirect investments in Proptech firms by real estate companies worldwide in 2019, by type of technology, Statista.com, **2019**. [Publisher]

[3] Z. Zheng, S. Xie, H.N. Dai, W. Chen, X. Chen, J. Weng, M. Imran, *Future Generation Computer Systems*, **2020**, *105*, 475-491. [Crossref], [Google Scholar], [Publisher]

[4]Sheikh, Husneara, R. Meer Azmathullah, and F. Rizwan, *International Research Journal of Advanced Engineering and Science*, **2019**, *4*, 321-324. [Google Scholar], [Publisher]

[5] F. Schär, *FRB of St. Louis Review*, **2021**. [Google Scholar], [Publisher]

[6] A.D. Popescu, *Social Sciences and Education Research Review*, **2020**, *7*, 321-349. [Crossref], [Google Scholar], [Publisher]

[7]S.M. Werner, D. Perez, L. Gudgeon, A. Klages-Mundt, D. Harz, W.J. Knottenbelt, *arXiv preprint arXiv:2101.08778*, **2021**. [Crossref], [Google Scholar], [Publisher]

[8] M. Shuaib, S. Alam, M.S. Alam, M.S. Nasir, Materials Today, **2023**, *81*, 203-207. [Crossref], [Google Scholar], [Publisher]

[9]F. Firouzi, B. Farahani, M. Weinberger, G. DePace, and F. Shams Aliee. Iot fundamentals: Definitions, architectures, challenges, and promises, In Intelligent Internet of Things, pp. 3-50. Springer, Cham, **2020**. [Crossref], [Google Scholar], [Publisher]

[10] C. Glohr, Telco focus on business customers, In Future Telco, **2019**, 299-307, Springer, Cham. [Crossref], [Google Scholar], [Publisher]

[11] S. Peng, P. Souvik, and H. Lianfen, "Principles of Internet of Things (IoT) Ecosystem: Insight Paradigm," **2020**. [Crossref], [Google Scholar], [Publisher]

[12] V. Vilken, K. Olga, B. Sergei, and Z. Elizaveta, *IOP Conference Series: Materials Science and Engineering*, **2019**, *497*, 012037, IOP Publishing. [Crossref], [Google Scholar], [Publisher]

[13] K. Mekki, B. Eddy, F. Chaxel, F. Meyer, *ICT express*, **2019**, *5*, 1-7. [Crossref], [Google Scholar], [Publisher]

[14] D.D. Olatinwo, A. Adnan, H. Gerhard, , *Sensors*, **2019**, *19*, 5268. [Crossref], [Google Scholar], [Publisher]

[15] J.P. Queralta, T.N. Gia, Z. Zou, H. Tenhunen, T. Westerlund, *Procedia Computer Science*, **2019**, *155*, 343-350. [Crossref], [Google Scholar], [Publisher]

[16] Y. Kabalcı, A. Muhammad, *Energy and Communication Conference (GPECOM)*, **2019**, IEEE, 24-29. [Crossref], [Google Scholar], [Publisher]

[17] S. R. Kohroodi, G. R. S. Moorkani, M. S. Zanjani, M. Abolghasemi, *Scientific Journal of Research in Human Resources Management*, **2021**, *13*. [Google Scholar]

[18] G. Vial, *The Journal of Strategic Information Systems*, **2019**, *28*, 118-144. [Crossref], [Google Scholar], [Publisher]

[19] N. Manou, R. Astrid, M. Van Hool, How IOT is reshaping the industry: The impact for a telco and its related 5g strategy, **2019**. [Google Scholar], [Publisher]

[20] F. Putra, S. Khanagha, K. Pandza, How to Make Exploratory Unit Ambidextrous? Navigating Contradictions of Exploration, Navigating Contradictions of Exploration, **2019**. [Google Scholar]

[21] P. Krüssel, P. Krüssel, and Rauscher, "Future Telco," Springer International Publishing, **2019**. [Crossref], [Google Scholar], [Publisher]

[22] B. Horlach, P. Drews, A. Drechsler, I. Schirmer, and T. Böhmann, Reconceptualising Business-IT Alignment For Enabling Organisational Agility, **2020**. [Google Scholar]

[23] A. Engholm, A. Björkman, Y. Joelsson, I. Kristoffersson, A. Pernestål, *Transportation*

research procedia, **2020**, *49*, 145-159. [Crossref], [Google Scholar], [Publisher]