

# Contents

CONTENTS.....	XI
LIST OF FIGURES .....	IIIX
LIST OF TABLES .....	XV
INTRODUCTION .....	1
CHAPTER 1 .....	3
1 INTRODUCTION .....	4
2 DEFINITION.....	4
3 GOAL OF USING AD-HOC OR MOBILE AD-HOC NETWORKS.....	5
4 THE CHARACTERISTICS OF A MANET .....	5
5 THE DIFFERENT ROUTING PROTOCOLS FOR AD-HOC NETWORK .....	6
5.1. TOPOLOGY BASED .....	6
5.2 POSITION BASED .....	6
6 AD-HOC NETWORK COMPONENTS.....	8
6.1. HARDWARE .....	8
6.2. SOFTWARE.....	9
6.2.1 Destination-Sequenced Distance-Vector (DSDV) .....	9
6.2.2 Dynamics Source Routing (DSR).....	9
6.2.3 Ad-Hoc on-Demand Distance-Vector (AODV).....	10
6.2.4 Zone Routing Protocol (ZRP).....	11
6.2.5 Cluster Based Networks.....	12
7 ADVANTAGES AND DISADVANTAGES OF AD HOC NETWORK .....	14
8 COMPARING AD-HOC AND INFRASTRUCTURE NETWORKS .....	16
9 CONCLUSION .....	16
CHAPTER 2 .....	17

INTRODUCTION .....	18
I. INTRUSION DETECTION SYSTEM .....	18
1 DEFINITION.....	18
2 SIMPLE DESCRIPTION FOR INTRUSION DETECTION SYSTEM .....	18
3 WHY WE NEED INTRUSION DETECTION SYSTEM.....	19
4 CLASSIFICATION OF IDSS .....	20
5 TYPES OF INTRUSION DETECTION SYSTEMS.....	21
5.1 HOST BASED INTRUSION DETECTION SYSTEM .....	21
5.2 ADVANTAGES OF HOST BASED INTRUSION DETECTION SYSTEMS .....	22
5.3 NETWORK BASED INTRUSION DETECTION SYSTEM.....	23
5.4 ADVANTAGES OF NETWORK BASED INTRUSION DETECTION SYSTEMS .....	23
6 METHODS OF INTRUSION DETECTION SYSTEMS.....	24
6.1 SIGNATURE-BASED INTRUSION DETECTION.....	24
6.2 ANOMALY-BASED INTRUSION DETECTION SYSTEM.....	25
7 THE ADVANTAGE AND LIMITATIONS OF TWO METHODS .....	25
8 THE PROBLEM OF FALSE POSITIVES .....	26
9 TECHNIQUES TOWARD REDUCING FALSE POSITIVES.....	26
II. ALERT CORRELATION .....	27
1 DEFINITION.....	27
2 ALERT PROCESSING.....	28
CONCLUSION .....	30
CHAPTER 3.....	31
INTRUDUCTION .....	32
1 ARCHITECTURES FOR IDS IN MANETS.....	32
1.1. STAND-ALONE INTRUSION DETECTION SYSTEMS .....	32

1.2.	COOPERATIVE IDS ARCHITECTURE .....	33
1.3.	HIERARCHICAL IDS ARCHITECTURES .....	35
2.	THE RELATED WORKS .....	37
2.1.	RELATED WORKS ON STAND-ALONE INTRUSION DETECTION SYSTEMS .....	37
2.2.	RELATED WORKS ON COOPERATIVE IDS ARCHITECTURE .....	38
2.3.	RELATED WORKS ON HIERARCHICAL IDS ARCHITECTURES .....	40
3.	CONCLUSION .....	41
CHAPTER 4.....		42
1	INTRUDACTION .....	43
2	DEFINITION AND SYSTEM MODEL.....	43
3	OUR ARCHITECTURE .....	44
3.1.	CLUSTER BASED INTRUSION DETECTION FOR MANETs.....	45
3.1.1.	<i>Cluster Formation Phase</i> .....	45
3.2.1.	<i>Cluster Maintenance Phase</i> .....	48
3.2.	ALERT CORRELATION.....	48
4	THE ALGORITHMS .....	50
5	SIMULATION .....	52
6	RESULT AND ANALYZE .....	55
6.1.	THE COVERTURE OF CLUSTER HEAD .....	55
6.2.	NUMBER MALICIOUS NODE DETECT BY CLUSTER HEAD .....	56
7	CONCLUSION .....	57
CONCLUSION.....		58
REFERENCES .....		60

## List of Figures

Figure 1.2 :transmission area in ad-hoc.....	4
Figure 1.1 : IEEE 802.11.....	4
Figure 1.3: Routing Protocols in MANET.....	7
Figure 1.4: work of DSR.....	10
Figure 1.5: work of AODV .....	11
Figure 1.6: example routing zone with $\rho = 2$ .....	12
Figure 1.7 : The Link-Clustered Architecture.....	13
Figure 1.8 : The NTDR Network.....	13
Figure 1.9: Virtual Subnet Architecture.....	14
Figure 2.1: A very simple intrusion detection system.....	20
Figure 2.2 : Intrusion Detection System .....	21
Figure 2.3: the Classification of IDSs .....	21
Figure 2.4: Host based Intrusion Detection System.....	23
Figure 2.5: Host based Intrusion Detection System.....	24
Figure 2.6: General FP Reduction Approaches.....	28
Figure 2.7 : Alert Processing position.....	29
Figure 2.8: the classification of Alert Processing.....	30
Figure 3.1 : The exchange data between the neighbors in deferint IDS.....	36
Figure 3.2 : Graphical example of the Hierarchical IDS architectures.....	38
Figure 4.1: Our Topology Architecture.....	48

Figure 4.2: Network nodes Trust relationship.....	50
Figure 4.3 : present the algorithm of test of malicious node.....	54
Figure 4.4 : present the algorithm of trust values calculation.....	54
Figure 4.5 : present the algorithm of election of the Cluster heads.....	55
Figure 4.6 : present our Architecture.....	57
Figure 4.7 : present the analysed the malicious nodes.....	58
Figure 4.8: the increase of number of CH by number of nodes.....	59
Figure 4.8: Number of malicious nodes detected by the CH.....	60

## List of Tables

Table 1.1: The Characteristics of a MANET.....	6
Table 1.2: advantage and disadvantage of Proactive, Reactive and hybrid.....	8
Table 1.3: Advantages and disadvantages of ad hoc network .....	16
Table 2.1: Advantage and limitation of signature and anomaly based .....	27
Table 3.1 : The advantages and disadvantages of Stand-alone IDS .....	35
Table 3.2 : The advantages and disadvantages of Cooperative IDS Architecture .....	37
Table 3.3 : The advantages and disadvantages of Hierarchical IDS architectures .....	39
Table 4.1: number of CH by number of nodes.....	58
Table 4.2: Number of malicious nodes detected by the CH.....	59

# **INTRODUCTION**

## **Introduction**

A wireless network today is one of the most popular networks because of its unique features as mobility and the exchange data without any fixed infrastructure . Mobile ad hoc network is one kind of this network . A Mobile Ad hoc NETWORKS (MANETs) consists a group of mobile nodes that spontaneously form temporary networks without the aid of a fixed infrastructure or centralized management. They are widely used in many sensitive areas such as e-commerce, military affairs and medical records. ... etc.

However, security in MANETs is especially challenging because MANETs are highly vulnerable to attacks due to both the characteristics of the transmission medium, nodes mobility that causes topology change and the lack of centralized monitoring infrastructures.

Due to dynamic nature and the lack of any central management and monitoring of the network functions make MANETs more vulnerable to several kinds of attacks. So, security in MANET is an essential component to ensure the integrity and confidentiality of data exchanged in the network. Clustering and intrusion detection system (IDS) plays a vital role and a good monitoring architecture of MANETs security. The problem posed is how can we design a architecture to ensure the security of this type of network?. In this dissertation, in order to answer this problem, we will simulate a architecture of intrusion detection system to detect the malicious nodes. This architecture based on the cluster that considers the Trust metric in the cluster formation phase in order to improve detection accuracy.

### **Organization of the Dissertation :**

We have structured our dissertation in four chapters. The first chapter will give a brief introduction to the Mobile Ad hoc Network with some preliminary on it . In the second chapter we will highlight on the Intrusion detection and its techniques, and in particular classification of this systems. The third chapter focuses on the related work IDS in MANET with some description. In the fourth chapter we present our proposed method. Then we will end with a general conclusion and some perspective to improve the system in the future .



# **CHAPTER 1**

## **Mobile AD-HOC Network**

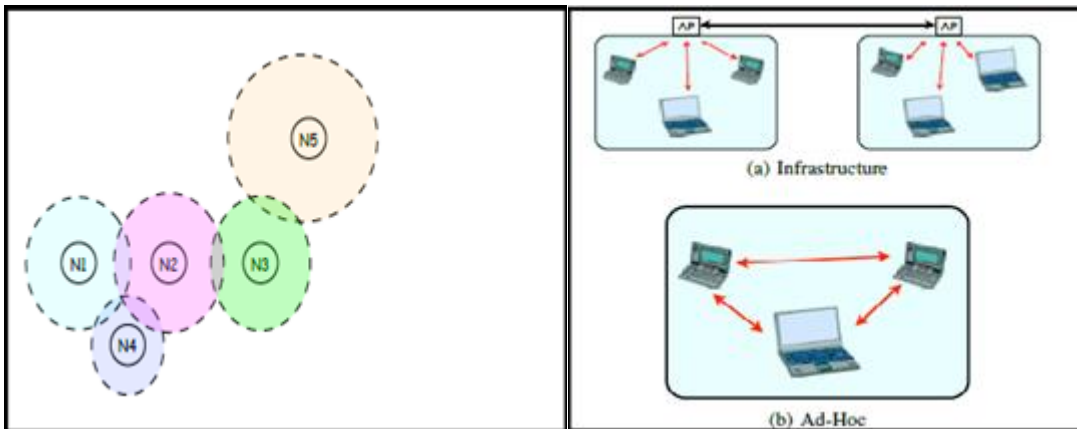
## 1 Introduction:

In this chapter we will talk about the mobile ad hoc network. First, We will give the definition of AD-HOC, and why we use it and we will present the characteristics of MANET and the different routing protocol for wireless Ad-Hoc networks, then we will mention advantages and disadvantages of ad hoc network. Finally we will give a little comparison between Ad-Hoc and infrastructure.

## 2 Definition:

*Ad hoc* is a Latin phrase which means “for this purpose”. But in the computer network it means wireless network without infrastructure. Ad hoc network are mostly used by military. [2]

Wireless AD-HOC networks are collections of wireless nodes, that communicate directly over a common wireless channel and they don't need any additional infrastructure like base station or wired access point etc. So the architecture of wireless network can be categorized into two basic architectures, the one is infrastructure (**figure 1.a**) and the second is ad-hoc network (**figure 1.b**), where the difference between them is that infrastructure network consists of access point, but in ad-hoc, each node doesn't just play the role of end system, but it also acts as a router. In this network the node can also communicate with all nodes in its area like in **figure 2**. [2]



**Figure 1.2** :transmission area in ad-hoc [2]

**Figure 1.1** : IEEE 802.11[2]

### 3 Goal of using Ad-Hoc or mobile Ad-Hoc networks:

One of the original motivations for MANET is found in the military need for battlefield survivability. In the battlefield, the soldiers (with or without their warfare) have to move freely without any of the restrictions imposed by wired communications devices. They still need communication device, so they can report their position, gathered information, and communicate with other soldiers. For this purpose they can't rely on an infrastructure. In some regions, such as the desert, the jungle, or mountain there is no torrential communications infrastructure. Therefore they have to establish networks without infrastructure and ad hoc networks specially MANETs support this case. [2]

### 4 The Characteristics of a MANET:

Characteristic	Description
Dynamics Topologies	Nodes are free to move arbitrarily with different speeds. Thus, the network topology may change randomly and at unpredictable times.
Energy- constrained Operation	Some or all of the nodes in an ad hoc network may rely on batteries or other exhaustible means for their energy. For these nodes, the most important system design optimization criteria may be energy conservation.
Limited Bandwidth	Wireless links continue to have significantly lower capacity than infrastructured networks. In addition, the realized throughput of wireless communications -after accounting for the effects of multiple access, fading, noise and interference condition, etc., is often much less than a radio's maximum transmission rate.
Security Threats	Mobile wireless networks are generally more prone to physical security threats than fixed-cable nets. The increased possibility of eavesdropping, spoofing and minimization of denial-of-service type attacks should be carefully considered.

**Table 1.1:** The Characteristics of a MANET [1]

## **5 The different routing protocols for Ad-Hoc network:**

Routing is the process of transmitting information or packets from source node to destination node. As Ad-Hoc network changes their topology very frequently and thus making packet routing difficult. Routing protocol controls the flow of data in networks and also decides the efficient path to reach the destination. There are 2 types of routing approaches:

### **5.4 Topology based:**

Topology based routing protocol perform packet routing by using the information about the nodes existing in the network. Proactive, reactive and hybrid approaches are examples of topology based routing protocol.[3]

### **5.2 Position based:**

Position-based routing protocol eliminate some of the limitations of topology-based routing by using additional information. They require information about the physical position of the participating nodes in the network their availability. Commonly, each node determines its own position through the use of GPS or some other type of positioning service. Position based routing is mainly focused on two issues:

1) a location service is used by the sender of a packet to determine the position of the destination and to include it in the packet's destination address; 2) a forwarding strategy used to forward the packets.

Topology based routing protocols are mainly divided into 3 categories:

- a) Table driven or Proactive protocols
- b) On demand or Reactive protocols
- c) Hybrid protocol [3]

### **Proactive (Table driven):**

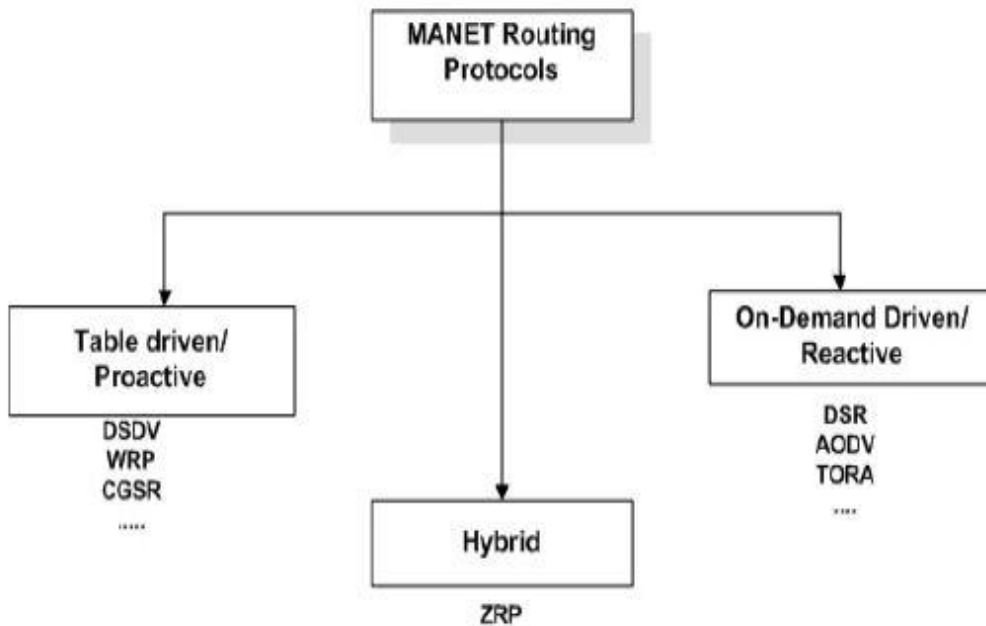
Schemes calculate the routes to various nodes in the network. So the nodes can route whenever they need it. Destination Sequenced Distance Vector (DSDV) is an example for proactive schemes.[3]

### **Reactive (on demand routing):**

Schemes will calculate the route, if the nodes need to communicate with a destination node. Ad-Hoc On-Demand Distance Vector (AODV) and Dynamic Source Routing are examples of reactive scheme.[3]

### Hybrid:

This type of protocol combines the advantages of proactive and reactive routing. The routing is initially established with some proactively prospected routes and then serves the demand from additionally activated nodes through reactive flooding. ZRP (Zone routing protocol) is hybrid algorithm.[3]



**Figure 1.3:** Routing Protocols in MANET [3]

Some of the advantages and disadvantages of Proactive, Reactive and hybrid are as follows:

	<b>Advantages</b>	<b>Disadvantages</b>
<b>Proactive</b>	<ul style="list-style-type: none"> <li>-Up-to-date routing information</li> <li>-Quick establishment of routes</li> <li>-Small delay</li> <li>-A route to every other node in the network is always available</li> </ul>	<ul style="list-style-type: none"> <li>-Slow convergence</li> <li>-Tendency of creating loops</li> <li>-Large amount of resource are needed</li> <li>-Routing information is not fully used</li> </ul>
<b>Reactive</b>	<ul style="list-style-type: none"> <li>-Reduction of routing load</li> <li>-Saving of resources</li> <li>-Loop-free</li> </ul>	<ul style="list-style-type: none"> <li>-Not always up-to-date routes</li> <li>-Large Delay</li> <li>-Control traffic and overhead cost</li> </ul>
<b>Hybrid</b>	<ul style="list-style-type: none"> <li>-Scalability</li> <li>-Limited search cost</li> <li>-Up-to-date routing information within zones</li> </ul>	<ul style="list-style-type: none"> <li>-Arbitrary proactive scheme within zones</li> <li>-Inter-zone routing latencies</li> <li>-More resources for large size zones</li> </ul>

**Table 1.2:** advantage and disadvantage of Proactive, Reactive and hybrid. [8]

## 6 Ad-Hoc NETWORK COMPONENTS:

### 6.1. Hardware:

The ad hoc networks don't have any infrastructure, except that they are combined with other networks' type. Only end devices are needed to establish ad hoc. Firstly the devices must be equipped with transceiver, so they can catch the incoming signal and send a signal. Secondly the

devices must be implemented after the standard IEEE 802.11, the devices like laptop, Personal Digital Assistant (PDA).[2]

## **6.2. Software:**

The most important software components of the ad hoc networks are routing algorithm. The following are some of most famous routing algorithms:[2]

### **6.2.1 Destination-Sequenced Distance-Vector (DSDV):**

It is based on the classic idea of the distributed algorithm of Bellman-Ford by adding some improvements. Each mobile station maintains a routing table that contains:

- All possible destinations.
- The number of nodes (or jumps) required to reach the destination.
- The sequence number (SN: sequence number) that corresponds to a destination node.[5]

### **6.2.2 Dynamics Source Routing (DSR):**

Is based on the use of the "source routing" technique. In this technique, the data source determines the complete sequence of nodes through which the data packets will be sent. [7]

That protocol consists of two major phases: route discovery and route maintenance. When a mobile node has a packet to send to some destination, it first consults its route cache determine whether it already has a route to the destination. If it has an unexpired route to the destination, it will use this route to send the packet. On the other hand, if the node does not have such a route, it initiates route discovery by broadcasting a route request packet. This route request contains the address of the destination, along with the source node's address and a unique identification number. Each node receiving the packet checks whether it knows a route to the destination. If it does not, it adds its own address to the route record of the packet and then forwards the packet along its outgoing links.

To limit the number of route requests propagated on the outgoing links of a node, a mobile node only forwards the route request if the request has not yet been seen by the mobile and if the mobile's address does not already appear in the route record.

A route reply is generated when the route request reaches either the destination itself, or an intermediate node that contains in its route cache an unexpired route to the destination. By the time the packet reaches either the destination or such an intermediate node, it contains a route record yielding the sequence of hops taken. Figure 3 show the work of DSR: [1].

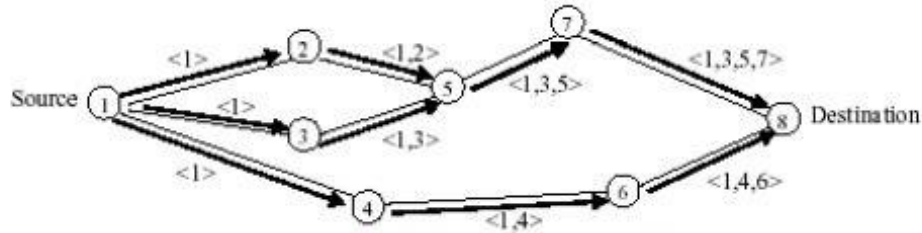


Figure – Route discovery in DSR

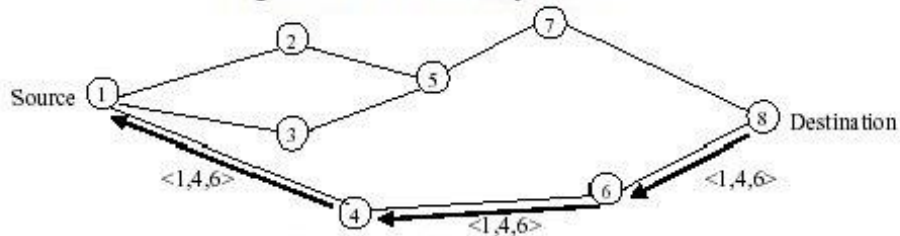


Figure – Propagation of route reply in DSR

**Figure 1.4:** work of DSR [1]

### 6.2.3 Ad-Hoc on-Demand Distance-Vector (AODV):

To improve the algorithm is essentially DSDV. It reduces the number of broadcast messages by creating paths, as needed, to the DSDV difference that continues to all routes.

Is based on the use of the "Road Discovery" and "Route Maintenance" mechanisms (used by the DSR), in addition to the node-to-node routing, the sequence number principle and the periodic exchange of DSDV. [7]

When a source node desires to send a message and does not already have a valid route to the destination, it initiates a path discovery process to locate the corresponding node. It broadcasts a route request (RREQ) packet to its neighbors, which then forwards the request to their neighbors, and so on, until either the destination or an intermediate node with a "fresh enough" route to the destination is located.

During the process forwarding the RREQ, intermediate nodes record in their route tables the address of the neighbor from which the first copy of the broadcast packet is received, thereby establishing a reverse path. If additional copies of the same RREQ are later received, these



packets are discarded. Once the RREQ reaches the destination or an intermediate node with a fresh enough route, the destination/intermediate node responds by unicasting a route reply. The Figure 5 explain the mechanism of AODV [1].

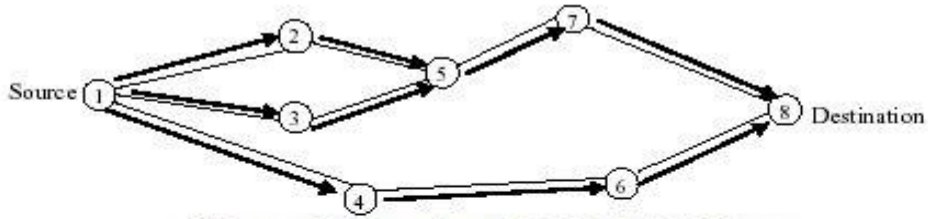


Figure – Propagation of RREQ in AODV

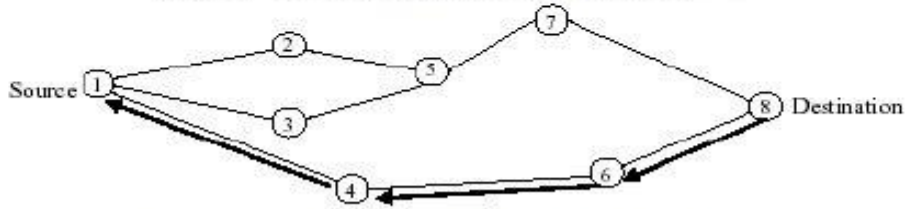
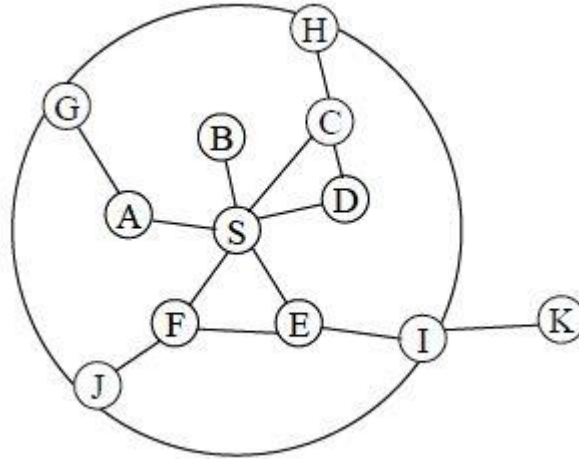


Figure – Path taken by the RREP in AODV

Figure 1.5: work of AODV [1]

#### 6.2.4 Zone Routing Protocol (ZRP):

The Zone Routing Protocol, as its name implies, is based on the concept of zones. A routing zone is defined for each node separately, and the zones of neighboring nodes overlap. The routing zone has a radius  $\rho$  expressed in hops. The zone thus includes the nodes, whose distance from the node in question is at most  $\rho$  hops. An example routing zone is shown in Figure 6, where the routing zone of S includes the nodes A–I, but not K. In the illustrations, the radius is marked as a circle around the node in question. It should however be noted that the zone is defined in hops, not as a physical distance. [9]



**Figure 1.6:** example routing zone with  $\rho = 2$  [9]

### 6.2.5 Cluster Based Networks:

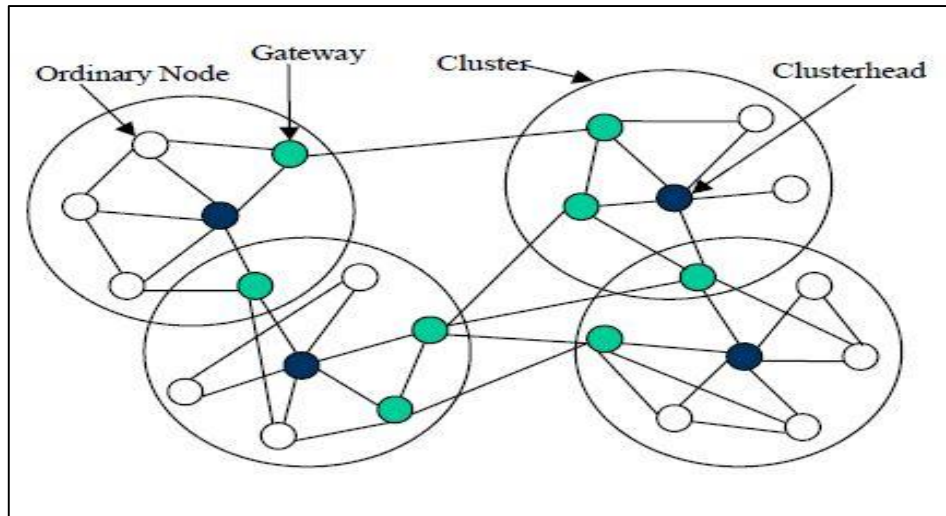
Cluster-based network is an (protocol , topology or algorithm) that controls structures promote more efficient use of resources in controlling large dynamic networks . With cluster based control, the physical network is transformed into a virtual network of interconnected node clusters. There can be one or more controllers per cluster and their functions are to make control decisions for cluster members, construct and distribute representations of cluster state for external use.

#### Cluster based network architectures:

The cluster based control structures used in ad hoc networks to achieve specific purposes are described below :

##### a) Link-cluster architecture :

This type of architecture is used in multiple-access broadcast environments. Distinct clusters of nodes are formed in such a way that transmissions are managed in a contention-free manner, thus reducing interference. In this architecture, all network nodes autonomously organize themselves into interconnected clusters each cluster contains a clusterhead, one or more gateways, and zero or more ordinary nodes as shown in Figure 6 [6].

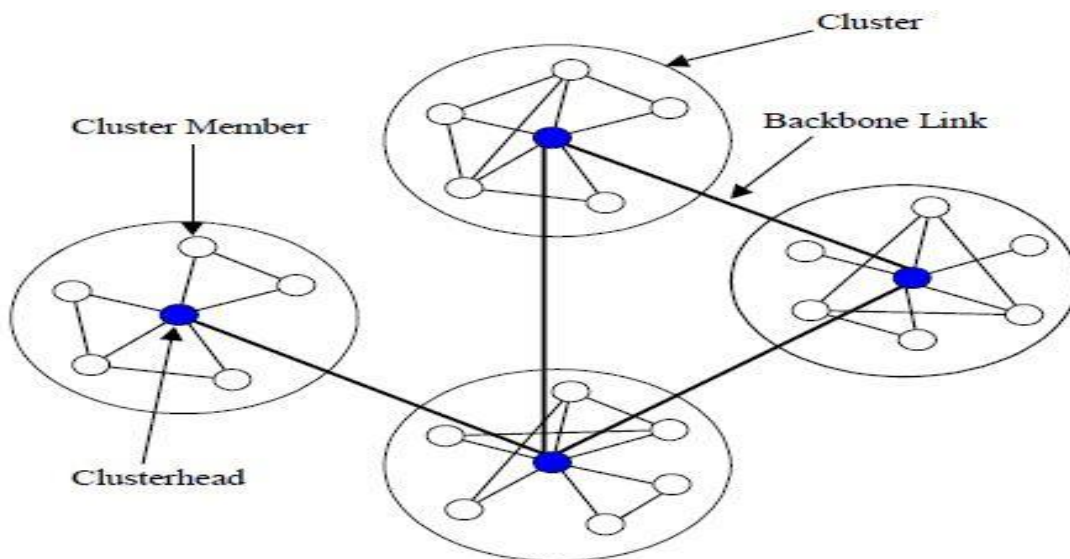


**Figure 1.7 :** The Link-Clustered Architecture [6]

**a) Near-Term Digital Radio (NTDR) Network :**

Near-Term Digital Radio (NTDR) networking has been designed for and deployed in large tactical networks. This is used as one of the clustering methods for backbone formation.

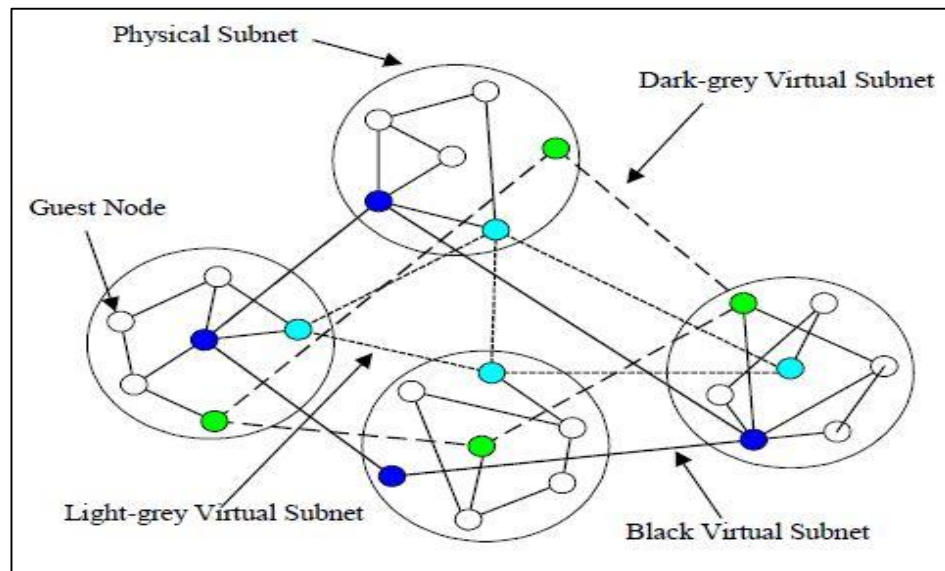
NTDR produces a set of clusters, each containing a cluster-head, which are linked together forming a routing backbone as shown in Figure 7. [6]



**Figure 1.8 :** The NTDR Network [6]

**a) Virtual Subnet Architecture :**

The virtual subnet architecture employs a set of several disjoint routing backbones to provide fault-tolerant connectivity and load balancing in a multi-hop mobile wireless network. Based on the node locality, the network is first divided into a set of physical subnets of disjoint clusters. Members of different physical subnets are clustered together to form virtual subnets, each of which spans all physical subnets. The Figure 8 represent the VSA.



**Figure1.9:** Virtual Subnet Architecture [6]

**7 Advantages and disadvantages of ad hoc network:**

	<b>Advantages</b>	<b>Disadvantages</b>
<b>Infrastructure</b>	As described in the previous sections the ad-hoc networks don't rely on any infrastructure. They work independently, are more robust, and it is cheaper to form an ad hoc network. There is no installation, maintenance cost.	Without any help from infrastructure, the nodes have to work harder. They have to hop the messages, secure their own resource from attackers, perform a routing table, etc.
<b>Mobility</b>	Unlike the infrastructure networks, in which node's moving are restricted by cell's border, in the ad hoc networks, nodes can the orifical move freely. As long as this node can hop to a node inside the network, it can also communicate with other node in this network.	In the practical, it is hard to form a network, in which a node can move freely.
<b>Scalability</b>		Depend on routing algorithm, how the ad hoc networks can perform well. In a network with a large number of nodes and high mobility a table driven algorithm won't perform well, because there will be big overhead. Generally the infrastructure networks perform better in this situation. The infrastructure networks have only specified tasks, so they can handle more nodes.
<b>Routing</b>	Given a network topology, for example we have 5 nodes. If N3 or N5 doesn't work anymore or leaves the network. N1 still can communicate with N4. In the infrastructure networks, if the access point is defect, there will be no more communication in the affected.	Mobility and increased or decreased number of nodes can force some routing algorithms to alter their routing table.
<b>Security</b>	Some attacks can cause malfunction. If one of participant is attacked and it doesn't work anymore, The network can relay the messages through other route	Internal attacks may be possible via ad hoc transmissions. It means, the attacker can disguise itself as an ad hoc participant. It can spy, modify, or delete the hopped.

**Table 1.3:** Advantages and disadvantages of ad hoc network [10]

## 8 Comparing Ad-Hoc and infrastructure networks:

There some keys used to compare between Ad-Hoc and infrastructure networks that we explain it above: [11]

- **Infrastructure:** An infrastructure is built to control the end terminals. All messages will be sent to it and it will broadcast the messages to the destination node. In absence of infrastructure the end terminals lose their connect.
- **Mobility:** This key refers how the end terminals can move. They can move freely or restricted. Perhaps the mobility can also affect network's performance too.
- **Scalability:** Scalability in the wireless networks describes the performance of the networks in the face of increased number of nodes and nodes mobility.
- **Routing:** Routing is the process of selecting paths in a network. The selection of routing algorithms is very decisive, since a routing algorithm is dedicated only for specified purposes
- **Security:** Both infrastructure and ad hoc must deal with wireless security problem. There are some differences between ad hoc and infrastructure, which are described below it.

## 9 Conclusion:

In this chapter introduced a brief introduction to Mobile Ad hoc NETWORK (MANET). First, we introduced AD-HOC and why we it is very useful in different domains, then we presented the main characteristics of MANET and their different routing protocols. We also mentioned several advantages and disadvantages of ad hoc networks. Finally, we gave a comparison between Ad-Hoc and infrastructure networks.

## **CHAPTER 2**

### **Intrusion Detection System and Alert Correlation**

## **Introduction:**

In this chapter we will talk about Intrusion Detection System and Alert Correlation. First, we will give the definition of Intrusion detection system and why we need it, and we will present the different types for IDS with their advantages and disadvantages, then we will mention methods of IDS. In the second part of the chapter, we will present alert correlation, where we give the definition to alert correlation. Finally, we will cite Alert Correlation the Algorithms

## **I. Intrusion Detection System**

### **1 Definition:**

Intrusion is any set of actions that attempt to compromise the integrity, confidentiality, or availability of a resource. [12]

Intrusion Detection System (IDS) is a device or software application that monitors a network or systems for malicious activity or policy violations. Any detected activity or violation is typically reported either to an administrator .

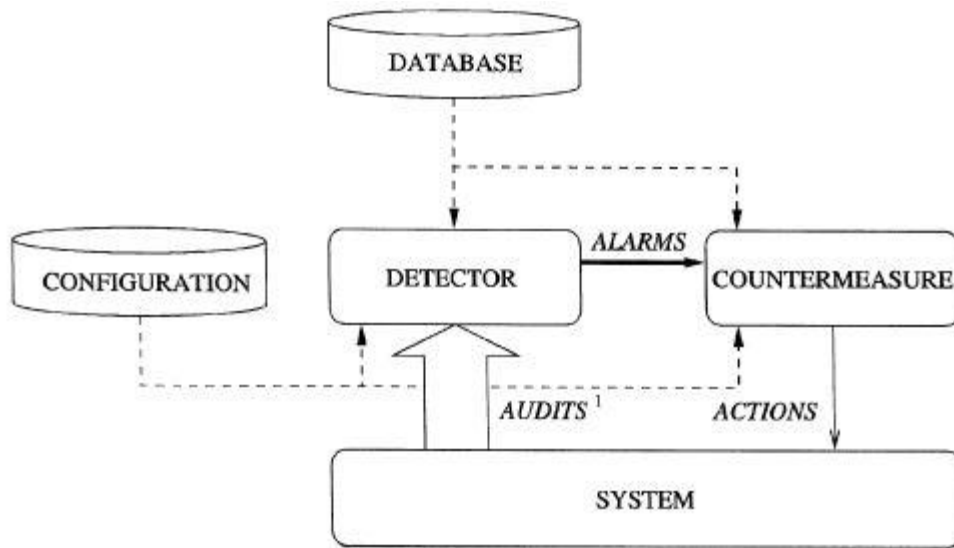
There are three main components of an IDS: data collection, detection, and response.

The data collection component is responsible for collection and pre-processing data tasks: transferring data to a common format, data storage and sending data to the detection module. IDS can use different data sources as inputs to the system: system logs, network packets, etc. In the detection component data is analyzed to detect intrusion attempts and indications of detected intrusions are sent to the response component. [13]

### **2 Simple description for Intrusion Detection System**

An intrusion-detection system can be described at a very macroscopic level as a detector that processes information coming from the system that is to be protected. **Fig 1...** This detector uses three kinds of information: long-term information related to the technique used to detect intrusions a knowledge base of attacks, for example, configuration information about the current state of the system, and audit information describing the events that occur on the system. The role of the detector is to eliminate unnecessary information from the audit trail and present a synthetic view of the security-related actions taken by users. A decision is then made to evaluate the probability that these actions can be considered symptoms of an intrusion. [19]





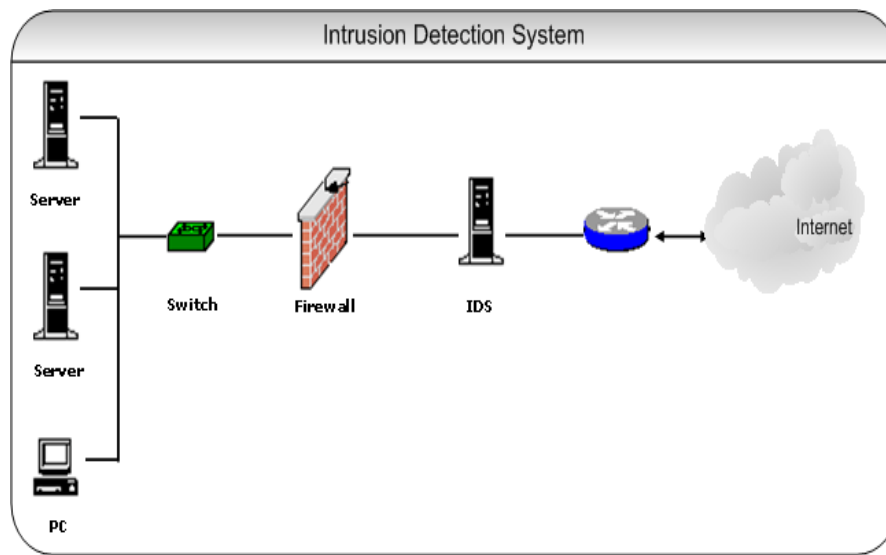
**Figure 2.1:** A very simple intrusion detection system [8]

### 3 Why we need Intrusion Detection System:

The Intrusion detection system in a similar way complements the firewall security. The firewall protects an organization from malicious attacks from the Internet and the Intrusion detection system detects if someone tries to break in through the firewall or manages to break in the firewall security and tries to have access on any system in the trusted side and alerts the system administrator in case there is a breach in security.

Moreover, Firewalls do a very good job of filtering incoming traffic from the Internet; however, there are ways to circumvent the firewall. For example, external users can connect to the Intranet by dialing in through a modem installed in the private network of the organization. This kind of access would not be seen by the firewall.

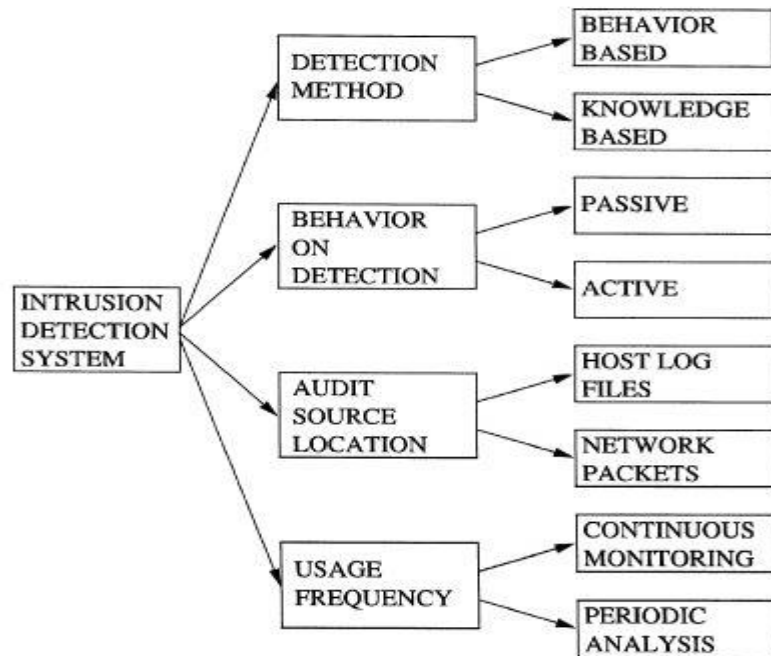
Therefore, an Intrusion detection system (IDS) is a security system that monitors computer systems and network traffic and analyzes that traffic for possible hostile attacks originating from outside the organization and also for system misuse or attacks originating from inside the organization.[4]



**Figure 2.2 :** Example for Intrusion Detection System [14]

#### 4 Classification of IDSs :

Intrusion detection systems can be classified in several ways. It is common to classify an IDS by the detection mode, the audit source, the usage frequency, and the response mechanism. Fig 2.



**Figure 2.3:** the Classification of IDSs [19]

**The detection method:** describes the characteristics of the analyzer. When the intrusion detection system uses information about the normal behavior of the system it monitors, we qualify it as behavior-based. When the intrusion detection system uses information about the attacks, we qualify it as knowledge based.

**Behavior on detection** describes the response of the intrusion-detection system to attacks. When it actively reacts to the attack by taking either corrective (closing holes), or proactive (logging out possible attackers, closing down services) actions, then the intrusion detection system is said to be active. If the intrusion detection system merely generates alarms (including paging, etc...), it is said to be passive.

**The audit source location** distinguishes among intrusion detection systems based on the kind of input information they analyze. This input information can be audit trails, system logs or network packets.

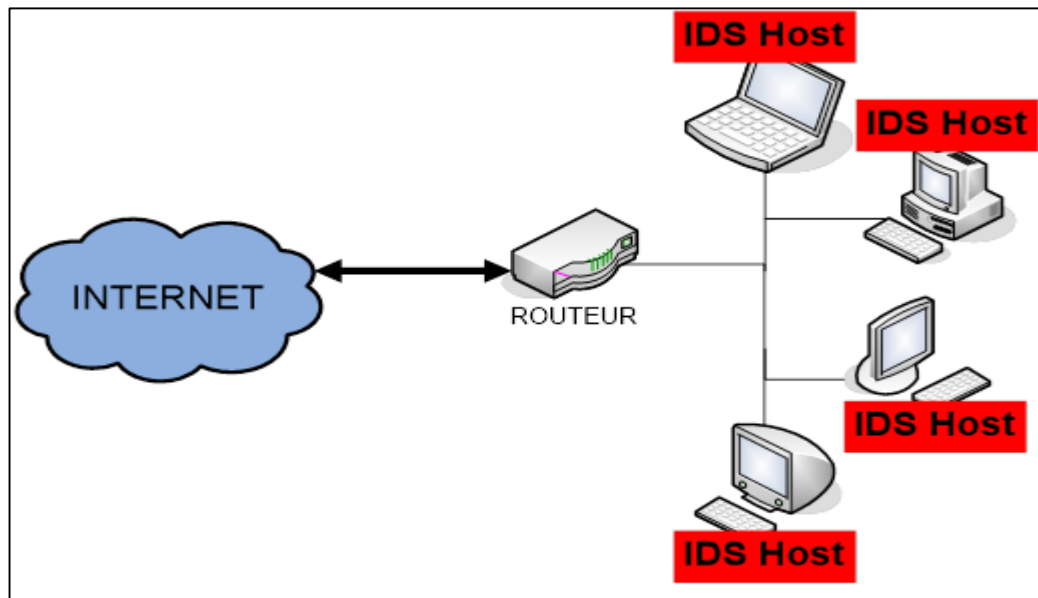
**Usage frequency** is an orthogonal concept. Certain intrusion-detection systems have real-time continuous monitoring capabilities, whereas others must be run periodically.[19]

## 5 Types of Intrusion Detection Systems:

There are broadly two types of Intrusion Detection systems. These are host based Intrusion Detection System and network based Intrusion Detection System.

### 5.1 Host based Intrusion Detection System:

Host intrusion detection systems (HIDS) run on individual hosts or devices on the network (Figure 2). A HIDS monitors the inbound and outbound packets from the device only and will alert the user or administrator if suspicious activity is detected. It takes a snapshot of existing system files and matches it to the previous snapshot. If the critical system files were modified or deleted, an alert is sent to the administrator to investigate. An example of HIDS usage can be seen on mission critical machines, which are not expected to change their configurations.[12]



**Figure 2.4:** Host based Intrusion Detection System [16]

## 5.2 Advantages of Host based Intrusion Detection Systems:

Here we have some Advantages of host based IDS: [15]

**Verifies success or failure of an attack:** Since a host based IDS uses system logs containing events that have actually occurred, they can determine whether an attack occurred or not with greater accuracy and fewer false positives than a network based system.

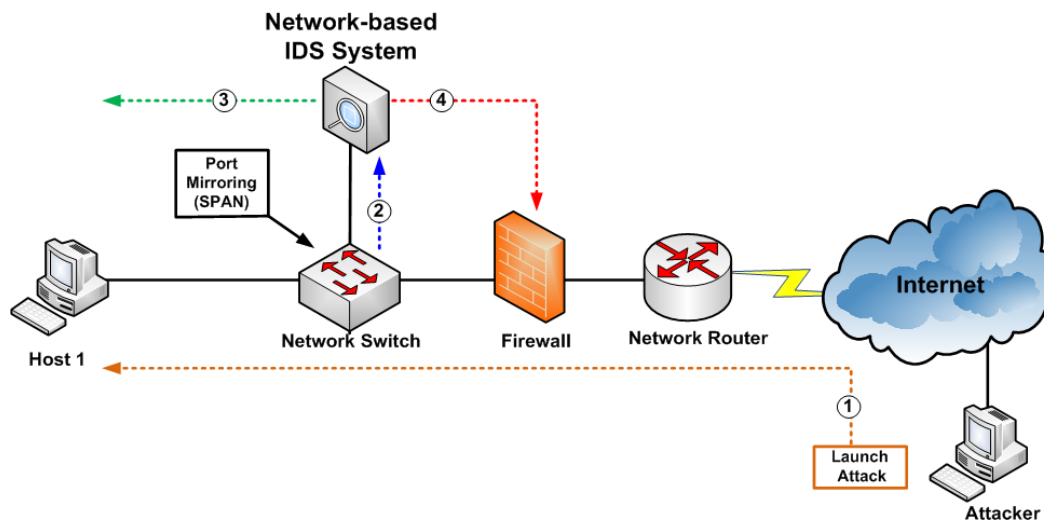
**Monitors System Activities:** A host based IDS sensor monitors user and file access activity including file accesses, changes to file permissions, attempts to install new executables etc. A host based IDS sensor can also monitor all user logon and logoff activity, user activities while connected to the network, file system changes, activities that are normally executed only by an administrator. Operating systems log any event where user accounts are added, deleted or modified. The host based IDS can detect an improper change as soon as it is executed. A network-based system cannot give so much detailed information about system activities.

**Lower entry cost:** Host based IDS sensors are far cheaper than the network based IDS sensors.

**Does not require additional hardware:** Host based IDS sensors reside on the host systems. So they do not require any additional hardware for deployment, thus reducing cost of deployment.

### 5.3 Network based Intrusion Detection System:

Network intrusion detection systems (NIDS) are placed at a strategic point or points within the network to monitor traffic to and from all devices on the network (Figure 3). It performs an analysis of passing traffic on the entire subnet, and matches the traffic that is passed on the subnets to the library of known attacks. Once an attack is identified, or abnormal behavior is sensed, the alert can be sent to the administrator. An example of an NIDS would be installing it on the subnet where firewalls are located in order to see if someone is trying to break into the firewall.[16]



**Figure 2.5:** Host based Intrusion Detection System [16]

### 5.4 Advantages of Network based Intrusion Detection Systems:

Here we have some advantages of network based IDS: [15]

**Lower Cost of Ownership:** Network based IDS can be deployed for each network segment. An IDS monitors network traffic destined for all the systems in a network segment. This nullifies

the requirement of loading software at different hosts in the network segment. This reduces management.

**Easier to deploy:** Network based IDS are easier to deploy as it does not affect existing systems or infrastructure. The network-based IDS systems are Operating system independent. A network based IDS sensor will listen for all the attacks on a network segment regardless of the type of the operating system the target host is running.

**Detect network based attacks:** Network based IDS sensors can detect attacks, which host-based sensors fail to detect. A network based IDS checks for all the packet headers for any malicious attack. Many IP-based denial of service attacks like TCP SYN attack, fragmented packet attack etc. can be identified only by looking at the packet headers as they travel across a network. A network based IDS sensor can quickly detect this type of attack by looking at the contents of the packets at the real time.

**Retaining evidence:** Network based IDS use live network traffic and does real time intrusion detection. Therefore, the attacker cannot remove evidence of attack. This data can be used for forensic analysis. On the other hand, a host-based sensor detects attacks by looking at the system log files. Lot of hackers are capable of making changes in the log files so as to remove any evidence of an attack.

**Real Time detection and quick response:** Network based IDS monitors traffic on a real time. So, network based IDS can detect malicious activity as they occur. Based on how the sensor is configured, such attack can be stopped even before they can get to a host and compromise the system. On the other hand, host based systems detect attacks by looking at changes made to system files. By this time critical systems may have already been compromised.

## 6 Methods of Intrusion Detection Systems:

There are broadly two methods of Intrusion Detection systems. These are Signature-based Intrusion Detection System and Anomaly-based Intrusion Detection System.

### 6.1 Signature-based Intrusion Detection:

Signature-based IDS refers to the detection of attacks by looking for specific patterns, such as byte sequences in network traffic, or known malicious instruction sequences used by malware. This terminology originates from anti-virus software, which refers to these detected

patterns as signatures. Although signature-based IDS can easily detect known attacks, it is impossible to detect new attacks, for which no pattern is available.[12]

## 6.2 Anomaly-based Intrusion Detection System:

An anomaly-based intrusion detection system, is an intrusion detection system for detecting both network and computer intrusions and misuse by monitoring system activity and classifying it as either normal or anomalous. The classification is based on heuristics or rules, rather than patterns or signatures, and attempts to detect any type of misuse that falls out of normal system operation. This is as opposed to signature-based systems, which can only detect attacks for which a signature has previously been created.[12]

## 7 The Advantage and Limitations of Two Methods :

	Advantage	Limitations
<b>Signature-based</b>	<p>Fewer false positives than Anomaly-based.</p> <p>Good signature design.</p> <p>Fairly fast.</p>	<p>No detection of unknown signatures.</p> <p>Signatures must be created, updated, and tuned.</p> <p>New attack variant can be created by changing a single string.</p>
<b>Anomaly-based</b>	<p>Can detect unknown attacks.</p> <p>Can detect attempts to exploit new and unforeseen vulnerabilities.</p> <p>Can recognize authorized usage that fall outside the normal pattern</p>	<p>Generally slower, more resource intensive compared to signature-based.</p> <p>Difficult to profile typical activity in large networks.</p> <p>Traffic profile must be constant.</p> <p>Higher percentages of false alerts.</p>

**Table 2.1:** Advantage and limitation of signature and anomaly based [20]

## **8 The Problem of False Positives:**

One of the main problems with intrusion detection systems is that they tend to generate a lot of false positives. A false positive occurs when the system generates an alert based on what it thinks is bad or suspicious activity but is actually normal traffic for that LAN. Generally, when you set up an NIDS with its default settings, it is going to look for anything and everything that is even slightly unusual. Most network intrusion detections systems have large default databases of thousands of signatures of possible suspicious activities. The IDS vendors have no way of knowing what your network traffic looks like, so they throw in everything to be on the safe side. [21]

## **9 Techniques toward Reducing False Positives:**

Many methods have been proposed in order to reduce false positives. All these methods can be divided into two general approaches. The first approach includes methods that operate during detection phase, we call them detection techniques and the second refers to the methods that operate on produced alerts after detection phase, we call them alerts processing techniques. Researches related to the first approach, propose different configuration of IDSs and detection methods and try to reduce false alerts with providing more accurate detection method. Since false positives are unavoidable because of the nature of anomaly detection method, in most of researches related to detection technique approach, the main target is maximizing detection rate and accuracy. It is obvious that a higher detection rate and higher accuracy will result lower false positives rate. These researches often use data mining techniques for better detection to maximize their detection rate and minimize false positives rate.

Toward reducing false alerts, some researches propose different configuration of IDSs but most of them propose alerts processing. Alert processing approach is the main solution to alerts handling and false positives reduction. Through alert processing techniques, data mining based techniques are the most used techniques that are exploited to reduce alerts and false positives. [22]



## II. Alert Correlation:

### 1 Definition:

The term “correlation” is relatively vague and has been used in many different ways. Correlation stems from the Medieval Latin and is composed of two Latin roots: “cum” which means ‘with’ (relationship) and relation from “relates”, the past participle of “referre”, which means ‘to carry back’.

So correlation can be defined as an “action to carry back relations with each other. [23]

Correlation has been used in several domains, to denote the various treatments to be applied on large input sets, potentially created by a small amount of common causes.

This is the case in areas such as:

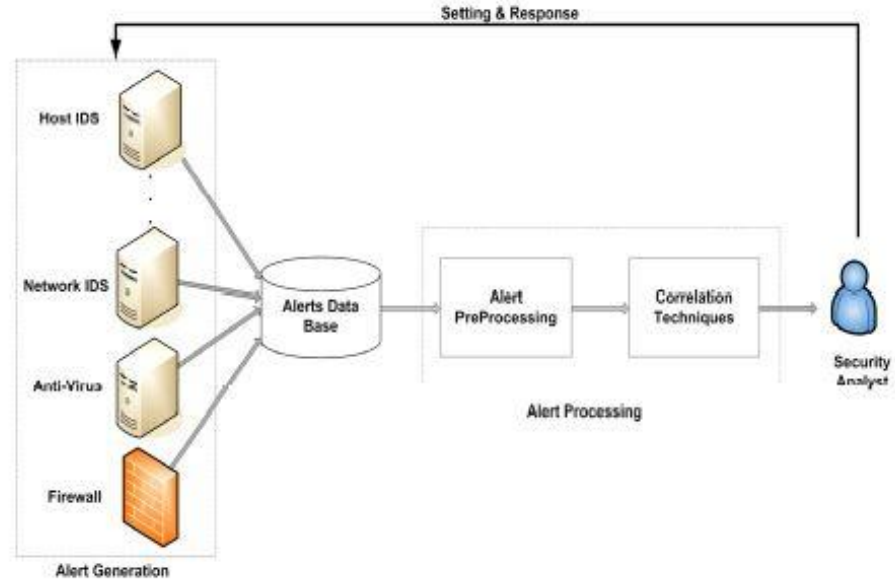
- event correlation
- alert correlation
- alarm correlation
- attack correlation

**Event Correlation** is a widely accepted technology for managing the complexity of modern telecommunication and data networks.

**Alarm correlation** is used in Network Management but in Security also. The principle remains similar. Alarms are external manifestations of faults, where a fault is a disorder occurring in an element of the managed network.

**Attack correlation** is used in a very specific situation: some security experts try to model attacks by building some scenarios. The process which aims at building these scenarios from primary attacks models is called attack correlation.

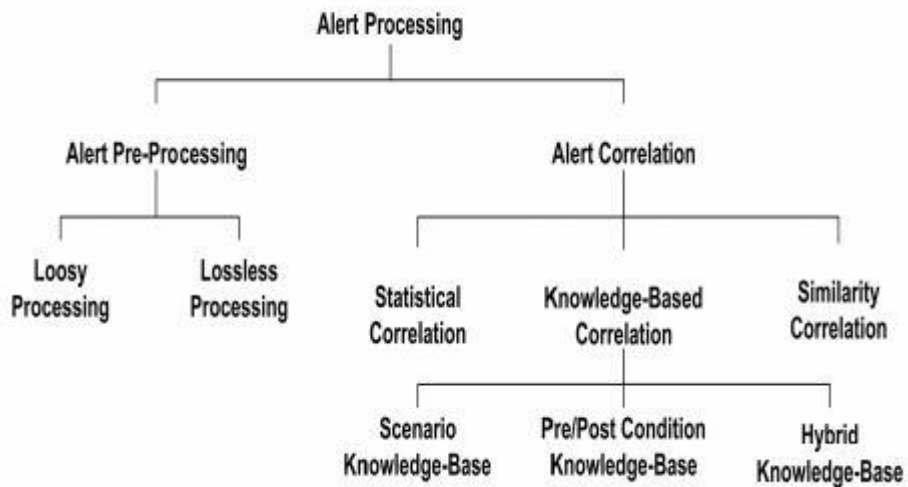
**Alert Correlation** is Multi step process that receives alerts from one or more intrusion detection systems as input and produces a high-level description of the malicious activity on the network.[23]



**Figure 2.7 :** Alert Processing position [24]

## 2 Alert Processing

The Alert Processing can be classified in two main steps: Alert Pre-Processing and Alert Correlation.



**Figure 2.8:** the classification of Alert Processing [24]

### **Alert Pre-Processing:**

This type of alert processing tries to mitigate the influence of false alerts and to make the next step (i.e. correlation process) more accurate.

There are many methods in this class of processing, all of which try to remove the noise from the stream of alerts and make it more meaningful.

Generally speaking, two main categories in the Alert Pre-Processing are Loosy Pre-Processing and Lossless Pre-Processing.[24]

#### **Loosy Pre-Processing:**

The main techniques of this type of processing are "the alert prioritization" and "alert aggregation", both of them try to reduce alert flooding and they are always used as components in the systems.

Alert prioritization is performed to assess the relative importance of alerts generated by the sensors. This method has to take into account the security policy and the security requirements of the site where the correlation system is deployed.

Alert Aggregation consists of detecting, from the observation of the alerts received in a given time window, multiple occurrences of the same alert and substituting the corresponding alerts, possibly indicating how many times the alert occurred during the observation period.

#### **Lossless Pre-Processing:**

Sometimes this type of techniques is called "filters" and it mainly uses rules to filter the alerts. These rules are built either by experts or by automated programs. It is designed to remove the false alerts that make the correlation process inaccurate. In this subsection, we examine three of these methods that is "Alert Verification", "Root Cause Discovery and Machine Learning".

### **Alert Correlation:**

Generally speaking, three main categories in the correlation process are distinguished are Statistical Correlation, knowledge-based correlation and Similarity Correlation.[24]

Statistical Correlation gathers all approaches that do not require a specific knowledge because it does not need predefined knowledge about attack scenarios, thus completely new attack scenarios can also be recognized.

Knowledge-Based Correlation can be considered as a misuse correlation because this type of correlation matches the alerts with a prior knowledge and search for fixed patterns of alerts (like

misuse IDSs). Unlike misuse IDSs that often provide only “late warning” (they report when a system has been compromised), misuse correlation respond to attacks before its completion.

Similarity Correlation tries to group the alerts in a meaningful way to conclude the attacks.

### **Conclusion :**

In this chapter we presented Intrusion Detection Systems and Alert Correlation. First, We give the definition to Intrusion detection system and its importance in security. Then, we presented the different types for IDS with their advantages and disadvantages, and we also mentioned the main types of IDS methods. In the second part of the chapter, Alert Correlation concept was presented, where we gave the definition to Alert Correlation. Finally we cited the techniques used for Alert Correlation.

# **CHAPTER 3**

## **Intrusion Detection System In MANET**

## **Intruduction :**

A Mobile ad hoc networks (MANETs) as described in chapter 1 consist of a group of mobile nodes that spontaneously form temporary networks without the aid of a fixed infrastructure or centralized management. Due to dynamic nature and the lack of any central management and monitoring of the network functions make MANETs are more vulnerable to several kinds of attacks. So security in MANETs are an component to ensure to the integrity and confidentiality of data exchanged in network.

Intrusion detection system is the process of monitoring the events occurring in network, so it can be deployed in mobile ad hoc network to protect them against a number of attacks by offering auditing and monitoring capabilities to a node.

In this chapter we will talk about the architectures for IDS in MANETs , we will briefly present the definition for each architecture and gives some related work on it

## **1 ARCHITECTURES FOR IDS IN MANETS:**

The configuration of MANET infrastructures can be configured are either flat or multilayer, depending on the application . Therefore, the optimal IDS architecture for a MANET may depend on the network infrastructure itself . In a flat network infrastructure, all nodes are considered equal, thus it may be suitable for applications such as virtual classrooms or conferences. On the contrary, all nodes are not considered equal in a multi-layered network. Nodes may be partitioned into clusters with one cluster head for each cluster and they can communicate directly in same cluster , but with other node from other clusters it must be done through the clusterhead [25].

In the follwing we will present the most famous architecture IDS in MANET

### **1.1. Stand-alone Intrusion Detection Systems :**

In this architecture , each node runs an IDS that independently to determine the intrusions.

Thus, the architecture is based on a self-contained approach for detecting malicious actions at each network node. Since stand-alone IDS do not cooperate or share information with other systems, all intrusion detection decisions are based on information available to the individual node. Therefore, no data is exchanged. Besides, nodes in the same network do not know anything about the situation on other nodes in the network as no alert information is passed. In general, these features limit them in terms of detection accuracy and the type of attacks that they detect [26].

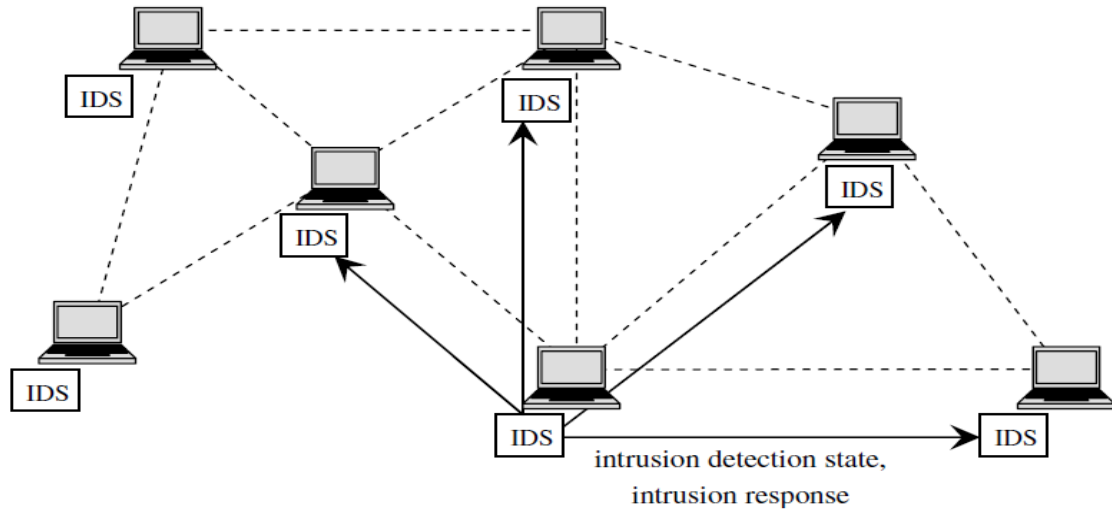
The advantages and disadvantages of this architecture are present in Table 1.

Advantages	Disadvantages
It is not prone to man in the middle and blackmail attacks	utilizes only the nodes local audit data
	Every node maintains one or more comprehensive engines therefore increases processing overhead
No communication overhead, no unfair workload distribution and no points of failure because there is no cooperation and no data exchanged among them on the network	No cooperation and no data exchanged among them on the network
	Impacts of nodes mobility decreases the detection accuracy, increases the rate of false positives and creates new security weaknesses
It is also more suitable for flat network infrastructure	Detects a limited set of attacks due to the lack of cooperation
	Coordinated attacks by multiple attackers are not detectable

**Table 3.1 :** The advantages and disadvantages of Stand-alone IDS [26]

## 1.2. Cooperative IDS Architecture :

In the cooperative IDS architectures an intrusion detection engine is installed in every node monitoring local audit data and providing intrusion detection. To resolve inconclusive intrusion detections and detect more accurately advanced types of attacks and benefited the features of MANET, detection engines may cooperate with engines of neighboring nodes through the exchange of audit data or detection outcomes. The figure 1 explains the exchange. And the advantages and disadvantages of this architecture are present in Table 2.



**Figure 3.1 :** The exchange data between the nieghbors in different IDS [28]

Advantages	Disadvantages
Detection based on social network analysis distribution of detection tasks among nodes	Multiple or multi-layer engines increase processing overhead and the exchange of audit data also imposes communication overhead
No unfair workload distribution and no points of failure	
Use more than one or multi-layer detection engines exchange of detection results instead of audit data in order to provide increased detection accuracy and detect a wide of possible attack	Impacts of nodes mobility decreases the detection accuracy, increases the rate of false positives and creates new security weaknesses
Some of them attempt to minimize the imposed processing and communication overheads through task distribution or the exchange of detection results	Extra communication overhead, new security vulnerabilities and social network analysis is negatively affected by nodes mobility
A few of them try to defeat certain attacks by employing trust or secure communication channels	
limit the negative impacts of nodes mobility on intrusion detection, adjustable thresholds have been used for it	It is prone to man in the middle and blackmail attack
It is more suitable for flat network infrastructure	

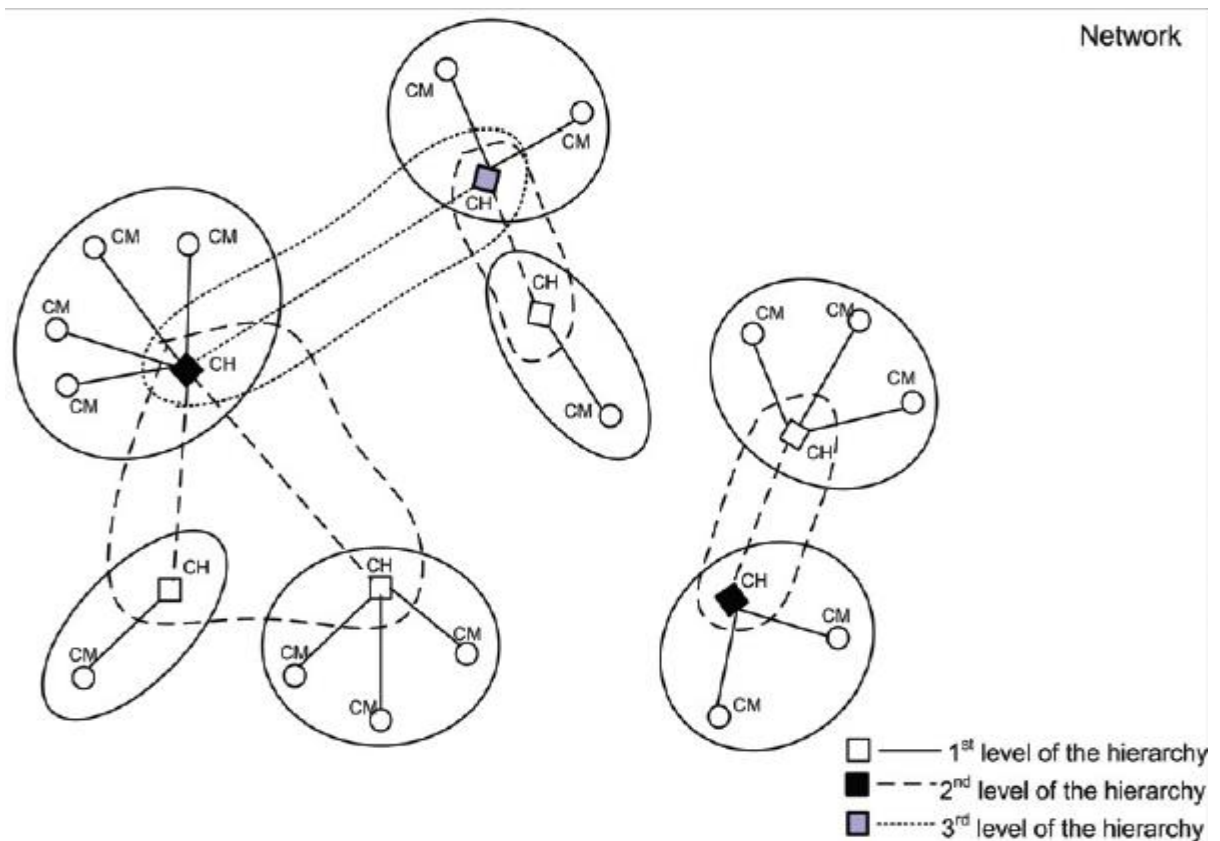
**Table 3.2 :** The advantages and disadvantages of Cooperative IDS Architecture [27]



### 1.3. Hierarchical IDS architectures :

The hierarchical architecture is an extended version of the distributed and cooperative IDS architecture, and have been proposed for multi-layered network infrastructures where the network is divided into clusters and nodes are divided into cluster-heads and cluster members. Specific nodes are selected (based on specific criteria) to act as cluster-heads and undertake various responsibilities and roles in intrusion detection that are usually different from those of the simple cluster members. Thus, these cluster heads, in some sense, act as control points which are similar to switches, routers, or gateways in wired networks. The cluster members typically run a lightweight local intrusion detection engine that performs detection only on local audit data, while the cluster-heads run a more comprehensive engine that acts as a second layer of detection based on audit data from all the cluster members. [27]

The following figure present Graphical example of the Hierarchical IDS architectures.



**Figure 3.2 :** Graphical example of the Hierarchical IDS architectures [36]

The advantages and disadvantages of this architecture are present in Table 3.

Advantages	Disadvantages
Use of collective decisions for intrusion detection	Cluster-heads become points of failure
It is more suitable for multi-layer network infrastructure	In some of them the elected cluster-head are unfairly overloaded
Use of hierarchical structures that are robust to network changes, limit the negative impacts of nodes mobility on intrusion detection	The formation of clustered /hierarchical structures creates new security risks and increase further the processing and communication overhead
The majority of them attempt to increase detection accuracy (either by employing multiple layers of detection or by employing one cluster-head to monitor large portions of a network, or by monitoring the elected cluster-heads)	A few of them detect only specific type of attacks and are negatively affected by high nodes mobility
	Impacts of nodes mobility Decreases the detection accuracy Increases the rate of false positives Increases the processing and communication overhead
Some of them focus on the fair distribution of the processing workload among nodes (either by considering nodes battery power, or by rotating cluster-heads)	In many of them , The election of cluster heads The movement of cluster Members, The exchange of audit data between a cluster-head and the cluster-members and The rotation of cluster-heads increase Communication overhead and processing overhead
A few of them try to eliminate the imposed processing and communication overhead (either by employing a detection mechanism based on voting or by selecting cluster- heads with the objective of last longer	It is vulnerable to a variety of attacks (i.e., man in the middle, blackmail, exploitation of the employed election scheme, malicious nodes may hinder or mislead detection, etc.)

**Table 3.3** : The advantages and disadvantages of Hierarchical IDS architectures [27]

## **2. The related works :**

In the last few years, a number of research papers in mobile ad hoc network have been published and fall in various aspects such as clustering, QoS and security in MANETs. Among those, MANET security with intrusion detection has emerged as one of the key challenges. Therefore, some papers recently reveal a growing interest in this topic, in both the industrial and academic communities. In this section we review a few papers on this topic.

### **2.1. Related works on Stand-alone Intrusion Detection Systems :**

In this architecture, an intrusion detection system runs on each node independently to determine intrusions. Every decision made is based only on information collected at its own node, since there is no cooperation among nodes in the network. In this type of architectures, some interesting methods have been proposed, we choose some to represent.

Jacoby and Davis in [29] have proposed a Battery Based stand-alone architecture for detecting malicious actions in MANETs, by monitoring power consumption in every node's battery. Detection is achieved by comparing a node's power consumption with a set of power consumption patterns induced by known attacks, using smart battery technology. In an experimental implementation, the proposed IDS detected 99% of the attacks in cases that only one type of them occurred. It also detected multiple attacks, but only in cases that the nodes were idle and no other activity was present.

They use B-BID approche (Battery-based intrusion detection) that's offers a completely host-centric intrusion protection scheme for any mobile device using a smart battery, that is, a battery with an internal circuit that enables communication of battery conditions to the user. B-BID measures energy expended over a period of time to identify an attack. Specifically, it either measures energy levels instantaneously or averages them over time by pulling data from the smart batteries.

Lauf et al. (2010) [30] proposed a Two Staged, stand-alone IDS architecture which is a combination of two detection engines, known as HybriIDS. The first one (referred to as the maxima detection system (MDS)) is an anomaly detection engine that identifies statistical oddities in the observed interactions of the application layer. This is achieved by maintaining the history of the

application layer interactions and comparing them with a normalcy profile created offline. If a possible attack is identified, the MDS activates CCDS a second (referred to as the cross-correlative detection system (CCDS)) engine that calibrates a threshold value considering the attack. Then, calculates average values of the application behavior of every node and compares them with the threshold.

Behaviors that exceed the threshold are marked as malicious. By employing two detection engines at each node, the proposed IDS increases detection accuracy, compared to other single engine IDSs because the one engine supplements the other. However, CCDS is prone to false positives and negatives, since it calibrates the threshold value only once during startup. Thus, dynamic changes of the network, induced by nodes mobility, are not accommodated by CCDS.d.

Nadkarni and Mishra in [31] have proposed a novel intrusion detection approach for wireless ad hoc networks, this approach is a stand-alone IDS architecture that uses compound detection aiming at reducing the amount of false positive alerts, which typically appear in anomaly detection. It employs adjusting thresholds to determine malicious behaviors. During initialization, the intrusion detection engine installed in every node creates the normalcy profile of the network traffic. Based on this, it estimates threshold values, beyond of which there is an indication of possible attacks. Every time a symptom of a known attack is detected, a counter called mis-incident is incremented and the node responsible for the symptom is marked as suspicious. If the incident repeats and the mis-incident counter exceeds the threshold value for the specific attack, the node from where the incident originates is labeled as malicious. After a preset period of time in which there are no malicious behaviors detected, the threshold is raised; otherwise is lowered.

## **2.2. Related works on Cooperative IDS Architecture :**

W.Wang, H.Man, Y. Liu in [32] have proposed a cooperative IDS architecture, it's a framework for intrusion detection systems by social network analysis methods in ad hoc networks.

In this architecture, each node deploys an intrusion detection engine that performs detections using audit data received from its "ego" network. An "ego" network consists of a hosting node ("ego") and the nodes ("alters") that are directly connected to it. The deployed engines operate similarly to anomaly detection, but they utilize social relations as metrics of interest, which require less computational overhead compared to standard anomaly detection engines. Moreover, a training phase is also required to create normal profiles (i.e., as in anomaly detection), and

according to the authors, the detection engines monitor the Medium Access Control (MAC) and network layers. The proposed IDS is composed of three modules: (a) the data pre-processing module that collects and pre-processes audit data; (b) the social analysis module that performs intrusion detection; and (c) the response module that integrates local and global (i.e., gathered from neighboring nodes) intrusion alerts. During the IDS operation, the data pre-processing module collects audit data from its neighboring nodes in intervals of 5 s. The social analysis module, then, processes the collected data in order to realize social relations between the “ego” network nodes, which represent the behavior of these nodes at a certain time. Subsequently, the realized relations are compared to the normal profile of expected behaviors, and any variation from these constitutes an intrusion. If an intrusion is detected, the response module notifies the neighboring nodes.

Jieying Zhou et al in [33] proposed an improved weight based clustering algorithm for intrusion detection in MANET (IWCA). IWCA uses a combination of metrics (mobility, fairness and security) to build clusters. IWCA algorithm divided into cluster formation and cluster maintenance stages. During cluster formation stage, each node broadcasts a HELLO message. Upon receiving the HELLO packets, each node updates its neighborhood table, calculates its combined weight and broadcasts it to its neighbors. The node with lowest combined weight in its neighborhood is elected as CH. Upon reception of CH message (once a node elected as CH informs its neighbors) each node joins its favorite cluster. Cluster maintenance is invoked when a new node joins a cluster or moves outside the boundaries of its cluster and/or when cluster head weight value increase (If cluster head weight is larger than its neighbor nodes, it will give up its role as a cluster head and all nodes will return to initial state). IWCA has better adaptability for MANET and be suitable for IDS in MANET. This algorithm has a drawback which it has to get the weights of all the nodes before starting the clustering process. So increase of the overhead.

S.Bose, S.Bharathimurugan, A.Kannan in [34] proposed a cooperative IDS architecture that uses a Multi-layer integrated anomaly intrusion detection system for mobile ad hoc networks. This architecture that uses three parallel anomaly detection engines, named as MAC layer detection engine, routing detection engine, and application layer detection engine, installed in every node.

The use of multi-layer detection aims at increasing detection accuracy, since attacks that target upper-layer protocols can be seen as legitimate events at lower-layers, and vice versa. The MAC

layer detection engine monitors both access control and addressing at the data-link layer. The routing detection engine monitors the network layer and keeps track of the packet delivery and routing information. Finally, the application layer engine monitors the application layer. Each engine collects the appropriate audit data, processes them and looks for malicious behaviors within them. In every node, a local integration module combines the results from the three different detection engines, while a global integration module combines the results received from the neighboring nodes.

### **2.3. Related works on Hierarchical IDS architectures :**

M.Chuan-xiang, F.Ze-ming in [35] proposed a hierarchical IDS architecture, follows a modular approach based on clusters. The goal is to provide a clustered structure where cluster-heads are always hosted by nodes with the highest battery power. During network initialization, each node reports its battery power to its neighbors. Then, the node with the highest available battery power is elected as cluster-head. A clusterhead re-election process is triggered as soon as one of the following events occurs: (i) a new node joins the network, (ii) the elected cluster-head leaves the network, or (iii) the battery power of the cluster-head is lower than a predefined threshold. When a new node joins the network, it should first notify all of its neighboring nodes. Likewise, if a cluster-head leaves the network, it broadcasts a packet to notify its cluster member nodes in order to initiate the cluster-head re-election procedure.

In this IDS architecture, each network node contains four different modules, described below:

First, the network detection module that provides network packet monitoring within a cluster. It is activated only when the hosting node is elected as cluster-head. After, the local detection module that monitors the hosting node and generates local alerts if malicious activities are detected. This module is always active at every node. Then, the resource management module that monitors the energy resources of a node acting as cluster-head. When the battery power is lower than a predefined threshold, the module first notifies the monitoring state management module, and then initiates the cluster-head re-election procedure. Finally, the monitoring state management module that manages whether

the network detection module is active (i.e., the hosting node is elected as cluster-head).

E.Darra, C.Ntantogian, C.Xenakis and S.Katsikas in [36] proposed a Architecture on hierachical cluster-based IDS for MANET that considers the mobility and energy of nodes in the cluster formation in the order to improve detection accuracy and reduce energy consumption.

The IDS architecture is organized into autonomous and distributed multileveled hierarchies. Each level of them consists of several clusters in which specific nodes act as CHs gathering local audit data from its CMs, analyzing them and extracting conclusions about the integrity of the nodes in the cluster. The autonomous clusters- based hierarchies are formed using the Mobility and Energy Aware Clustering Algorithm (MEACA) which can be applied in dynamically changed network topologies.

Initially, the algorithm creates the first level of hierarchies by forming autonomous clusters. Afterwards, the CHs of the previously formed clusters are selected to participate in the next level of hierarchies. Some of them will keep their attributes acting as CHs in the new level, while many others will act as CMs. Generally, the algorithm is repeated until the higher level of each hierarchy consists of a single node (i.e., hierarchy CH).

### **3. Conclusion :**

In this chapter we presented main approaches for IDS in MANETs. We gave first some definitions and concepts for each architecture with their advantages and disadvantages, then we choose some interesting related works.

## **CHAPTER 4**

### **The Intrusion Detection Approach**



## 1 Intrudaction :

As described in the last chapter, MANETs suffer from the vulnerabilities that arise in wired networks such as spoofing, DDOS, passive eavesdropping, access control ...etc, also MANETs suffer from the vulnerabilities due to wireless nature of the network such as wormhole, blackhole , sinkhole, selfishness ...etc. So MANET needs a system to detect those vulnerabilities and Intrusion detection system is a good solution to prevent the different kinds of attacks, identify the malicious nodes and eliminate them from the network.

In this chapter we will present our architecture that is based on the creation of a new topology in mobile Adhoc network, this new method is based on the cluster topology where we put some metrics to build it and create a new IDS system to detect the malicious nodes. Our proposed approach is based directly on an unpublished work of A. Bentaleb, H. Debbi [37]. In this work, they presented a novel cluster-based approach for IDS in MANET using the notion of trust, this approach is directly employed here. We aim here to extend their approach through focusing on some metrics such as forwarding packet and link rate. In addition, we deliver an implementation of the proposed approach based on C++. Finally, we give some promising simulation results about our approach.

## 2 Definition and system model

A mobile ad hoc network can be represented by an oriented graph or un-oriented, depending on the nature of the links,  $G(t) = (V(t), E(t))$  where  $V(t)$  represent the set of nodes at time  $t$  and  $E(t)$  represent the set of links between nodes at time  $t$ .

— **Definition 1 :** Set  $n = |V(t)|$ ,  $s = |E(t)|$ , edge  $e_{ij} \in E(t)$ ,  $e_{ij} = (v_i, v_j)$ , it represents a link between two nodes  $v_i$  and  $v_j$  at time  $t$ ,  $(v_i, v_j) \in V(t)$ ,  $i, j = 1, 2, \dots, n$ .

— **Definition 2:** For any node  $v$ , set  $\Gamma(v)$  is the neighbor nodes set of node  $v$ ,  $E(v)$  is link set connecting node  $v$  with its neighbor nodes.

— **Definition 3:** A non-overlapping clusters defined as each node belongs to a single cluster. Set  $C_i$  is the cluster  $i$  with  $C_i \subset V$ .  $h(v_i, v_j)$  is the least hops between  $v_i$  and  $v_j$ . And any two nodes  $v_i, v_j \in C_a$  fill that  $h(v_i, v_j)$ . We call that  $C_a$  and  $C_b$  are non-overlapped clusters if  $C_a \cap C_b = \Phi$ , with  $(a \neq b)$ .

– **Definition 4:** Set  $dv$  the node degree that represents the number of neighbor nodes in a  $k$ -neighborhood.

### 3 The Architecture

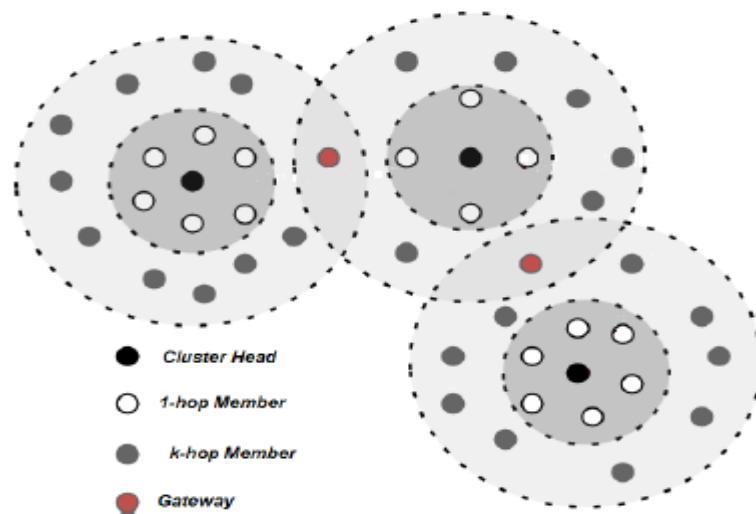
The network topology as proposed in [37] and employed here is organized in clusters. Each node has one of the following statuses: Cluster head, member nodes, not-decided, gateway node. Initially all nodes are in the not-decided state. As time progresses, each node tries to join a cluster by being of one of the three status CH, member or gateway.

□ *Cluster Head (CH)*: it's the coordinator of the group (cluster). It has additional functions such as: channel access, routing data, bandwidth and channel allocation, cluster security, forwarding inter-cluster packets, etc.

□ *Gateway*: is a node not CH state which works as the common or distributed access point for two or more cluster heads, when a node remains within the transmission range of two cluster heads.

□ *Member Node*: is a node that is not CH or gateway and acts only as an ordinary node. Each node belongs exclusively to a cluster independently of its neighbors that might reside in a different cluster.

Fig. 1 illustrates the main features and elements of our structure.



**Figure 4.1:** Our Topology Architecture

### 3.1. Cluster Based intrusion detection for MANETs

#### 3.1.1. Cluster Formation Phase

**Step1:** Initially, all network nodes in not-decided state exchange the HELLO messages periodically to notify its presence to the neighbor nodes. The HELLO message contains the status of the node. After, each node builds their neighbors list based on the received HELLO messages from other nodes and record the information about its neighbor nodes in its neighbor table.

The message HELLO can received by other node if those node been in a circule area with a radius of 250 meters and the center of this area is the sender node .

**Step2:** After neighbor nodes discovery stage, the cluster head election process invoked. Each node  $vi$  calculates its Trust value  $T_{vi}$  using *Node Trust value calculation (A)* and broadcasts its Trust value to its k-neighbor nodes through *Trust-val* message.

**Step3:** On reception of *Trust-val* messages, each node updates its neighborhood table and compares the received Trust values of all its k-hop neighbors with its own trust value. If its own trust value is the highest, it declares itself to be a cluster head. In case of equality, the node that has the lowest *ID* is selected as cluster head. The CH elected broadcasts a *CH\_elect* message with its *ID* as cluster *ID* to its k-neighbors.

#### A. Node Trust value calculation

Trust is an important metric to the design and deployment of security systems. In MANET node trust value calculation can be applied for node authentication, access control and trust routing. By calculation the trustworthiness of the related nodes, it does not only enhance the system security, but also may improve the routing performance in MANETs [38]. Trust is an important aspect in the conception and analysis of networks as it is an essential component by which the relations between the nodes can grow or stop. Trust can be defined as : “a set of relations among entities that participate in a protocol. These relations are based on the evidence generated by the previous interactions of entities within a protocol. In general, if the interactions have been faithful to the protocol, then trust will accumulate between these entities.” [39]. Trust value  $T_{vi}$  of node  $vi$  defines the level of confidence of a node  $vi$  on neighbor node  $vj$  depending on the performance evaluation of the assigned task. The trust model [39] used in our algorithm is distributed over the network

nodes. Each node will calculate trust values for all its neighbor nodes and store these values. For calculating the trust value for each node, it is necessary to calculate direct trust value, indirect trust value and total trust value (Fig.2).

*The direct trust (DT)* or called *Experience* representing the direct interactions relationship between two nodes (1-hop neighbor nodes). Direct trust of node  $vi$  on node  $vj$  can be calculated as:

$$DT_{vi}(vj) = \sum_{k=1}^n W_k [R_{vi}]_k(vj) \quad (1)$$

Where  $DT_{vi}(vj)$  represents the direct trust of node  $vi$  on node  $vj$ ,  $[R_{vi}]_k(vj)$  is the trust value of  $kth$  trust metric,  $W_k$  is the weight value of  $kth$  trust metric and  $n$  is number of different trust metrics. The direct trust is the sum of trust values node  $vi$  is having on node  $vi$  for different trust metrics.

The trust metrics represent such as Control packet/ message forwarded, Control packet/ message precision, Availability based on control message/hello messages, Reputation, Packet address modified, energy consumption ...etc.

*The indirect trust (IT)* or called *Recommendation* representing direct interactions between two nodes (there is no direct experience between two nodes). Indirect trust of node  $vi$  on node  $vj$  can be calculated as:

$$IT_{vi}(vj) = \frac{1}{m} \times \sum_{i=1}^m DT_{vi}(vj) \quad (2)$$

Where  $IT_{vi}(vj)$  represents the indirect trust of node  $vi$  on node  $vj$ . The indirect trust is on node  $vj$  represent the average of direct trust values of  $m$  neighbor nodes on  $vj$ .

*The total trust (TT)* representing the combination of Direct Trust (DT) and Indirect Trust (IT). Total Trust of node  $vi$  on node  $vj$  can be calculated as:

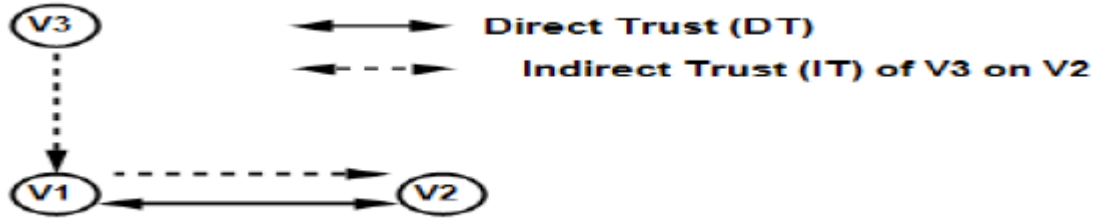
$$TT_{vi}(Vj) = W_{DT} \times DT_{vi}(vj) + W_{IT} \times IT_{vi}(vj) \quad (3)$$

Where  $TT_{vi}(vj)$  represent the total trust of node  $vi$  on node  $vj$ . and  $W_{DT}$ ,  $W_{IT}$  are the weighting factors.

In our proposed algorithm we have proposed and calculated the trust value  $T_{vi}$  of node  $vi$  that represents the sum of total trust values on node  $vi$ . The trust value of node  $vi$  can be calculated as:

$$T_{vi} = \sum_{j=1}^n TT_{vj}(v_i) \quad (4)$$

Where  $T_{vi}$  represent the trust value of node  $vi$ ,  $n$  is the number of k-hop neighbor nodes of node  $vi$  and represent the total trust of neighbor nodes  $v1, v2, v3, \dots, vn$  on  $vi$ .



**Figure 4.2:** Network nodes Trust relationship

**Step4:** Once a node receives a *CH\_elect* message and if it wishes to join the cluster it sends a *Join Request* message to the corresponding cluster head. The cluster head sends an *Accept* message and this node updates their status to member node.

**Step5:** After Cluster heads election in the network, each cluster head choses its gateway nodes to communicate other clusters. Each CH selects its gateway nodes using the gateway nodes election process (B).

### B. Gateway nodes election process

In our algorithm, we propose a gateway nodes election algorithm to ensure a certain level of security because gateway nodes have a critical role (data routing between two or more clusters). Our gateways election algorithm based on the trust value calculated in node trust value calculation step. Among the gateway nodes candidate, each cluster head choses its gateway nodes to communicate other clusters using the trust value related to each gateway candidate. The gateway node  $gi$  with highest trust value  $T_{gi}$  among other gateway nodes candidate is selected by the CH as its gateway. In case of equality, the highest ID gateway is selected.

### 3.2.1. Cluster Maintenance Phase

The clusters maintenance phase trying to adapt the structure of clusters at all topology changes that can occur caused by nodes mobility. The Trust value changes over time based on interactions between nodes. Mobility can also change the status of clusters and trust relationships between nodes. In fact, when a node acquires new neighbors or loses some due to mobility, the trust value of this node changes. In our algorithm, the cluster maintenance is invoked in the following cases:

- A new node joins cluster, when a new node enters the range of the cluster head it is properly authenticated by the cluster head in order to ensure a certain level of security. The new node sends Join Request message to the corresponding cluster head and waiting the response.

- A node moves outside the boundaries of its cluster, whenever this happens, the status of the node should be updated and this node tries to find an existing cluster to join it. Otherwise, the cluster formation invoked.

- Two cluster heads become neighbors, the node with the highest ID give up its role as CH and becomes a member node after it sends a HELLO message to their neighbors to inform them of its new status.

- The Trust value of cluster head modified. So, in normal case, if there is a member node has a highest trust value than the trust value of its cluster head then the CH give up its role and becomes a member node and the member node that has the highest trust value becomes a CH. But, since we are dealing with a vulnerable network, each cluster head could become malicious node. In our algorithm, a node should change its cluster head when the latter becomes malicious by reinvoking locally the cluster formation phase to avoid the reclustering (more overhead) of the whole network. The node seeking to change its malicious cluster head, finds the node with highest trust value amongst its k-hop neighbors to be its CH.

**Step6:** Each cluster head in the network generate alerts and sends it to the stationary server.

### 3.2. Alert Correlation

The number alerts generated from the clusters heads could be very huge causing what we call flooding alerts. Therefore, the aggregation of these local alerts is highly re-quired, in order to get

global view on the progress of attacks across the entire net-work, which will result in improving the detection ratio and reducing the false alarms. To this end, we use the CEP engine, ESPER as alert correlation engine to cope with the large number of alerts in real-time.

Complex Event Processing (CEP) consists of processing different events within the distributed enterprise system attempting to discover interesting information in timely manner. For enterprises, it is very necessary to react immediately for this information, because this information might represent an opportunity or threat. CEP is an Event Driven Architecture (EDA) style. EDA is software architecture, refers to generation, reaction, detection and consumption of events that represent notable changes in the state of enterprise's activities.

ESPER is the most known and used open source CEP engine. ESPER is a scalable engine has the ability to analyze thousands of events per second across all enterprise layers. The engine uses the Event Processing Language (EPL) for dealing with the high frequency event data. ESPER provides two principal mechanisms to process events: event stream queries and event patterns. The first mechanism addresses the event stream analysis requirements using windows, joining and analysis functions. The second mechanism addresses the expected sequences of presence or absence of events or combinations of events such as event A and B occur in either order followed by event C or D.

We can benefit from the first mechanism (event stream analysis) through performing similarity analysis on the alerts generated from the clusters heads. By comparing the similarity computed at each time epoch to such threshold, aggregated alerts will be generated. For better understanding, we present the following EPL statement as an example:

```
EPLStatement Similarity_Statement =
cepAdm.createEPL("insert into AlertStreamCorrelated
select ALS1.ID, ALS2.ID, ALS1.Target, ALS2.Target, Alert-
Similarity(
GetSourceSimilarity(ALS1.source,ALS2. source),
GetAttackSimilarity(ALS1.source,ALS2. source),
GetTimeSimilarity(ALS1.TimeStamp,ALS2.TimeStamp)) as
Alert_Similarity      from AlertStream1.win:time(5 minutes)
as ALS1,
AlertStream2.win:time(5 minutes) as ALS2
where ALS1.ID != ALS2.ID");
```

The EPL statement describes process of computing the similarity between two alerts, where the final similarity "*AlertSimilarity*" is based on three similarity values "*SourceSimilarity*" describes the malicious node, the "*AttackSimilarity*" that describes the type of attack and "*TimeSimilarity*" that describes the detection time by each cluster head. This statement is valid for each 5 minutes of period time. Thus, alerts out of this interval will not be correlated. All of these similarities are already defined in ESPER as user defined functions UDFs and called within the EPL statement.

After computing the similarity between alerts, just the alerts that meet the threshold will be correlated. This task is performed using the following statement:

```
EPStatement OutputStream_Statement =
cepAdm.createEPL("select * from AlertStreamCorrelated
(Alert_Similarity > Similarity_Threshold)");
```

## 4 Basic algorithms :

### 4.1 Test the malicious nodes :

The main goal behind our work is to detect a malicious node. To detect a malicious node , the cluster head performs a real-time analysis to all nodes that join in the cluster and test them by the metrics forwarding packet or the link rate , if those metrics are not in the usual values, then, they will be considered as malicious nodes . The figure 4.4 presents the algorithm of test of malicious node



---

**Algorithm : Test a Malicious Node**


---

Input: Set of nodes  
 Output: Malicious nodes  
 Begin : the cluster head analyze his neighbors  $V_i$   
 if  $V_i \rightarrow \text{ForwardingPacket} < 0.2$  or  $V_i \rightarrow \text{LinkRate} < 0.2$   
     then  
          $V_i$  remain as Malicious Node  
 end

---

**Figure 4.3 :** present the algorithm of test of malicious node

#### 4.2 Calculate the trust values :

The trust values base on 3 main function are : the Direct trust values ,the Indirect Trust values and the Total Trust values , those functions as we talked in the approach calculate the Trust value for each node  $V_i$  of the network

---

**Algorithm : Trust Values**


---

Input: Set of nodes  $v_i$  , Set of neighbors  $v_j$  of  $v_i$   
 Output: trust values ToTv  
 Begin : Nodes calculate the metrics  
 for  $i=0$  to  $n$  do  
     ToTv=0  
     for  $j=0$  to  $n$  do  
          $A = \text{DT}(\text{metrics})$   
          $B = \text{IDT}(\text{DT}, M)$   
          $Tv = \text{TrustV}(\text{DT}, \text{IDT})$   
          $\text{ToTv} = \text{ToTv} + Tv$   
     end for  
 end for

---

**Figure 4.4 :** present the algorithm of trust values calculation

**Choose Cluster Head :**

The election of cluster head base on the comparation the trust values of the neighbors , the node that has the highest trust values it become a cluster head , if we got an equality between two nodes we choose the who have the highest ID .

---

**Algorithm :**

---

**Input: Set of nodes****Output: Cluster head****Begin : every nodes exchange their trust values Tv to their neighbors****if  $Tv_i > Tv$  neighbors****then** **$V_i$  remain as a Cluster head****end if****if  $Tv_i = Tv$  neighbors****then****remain as a Cluster head who have the highest ID****end if**

---

**Figure 4.5 :** present the algorithm of election of the Cluster heads

**5 Simulation :**

Our approach needs to exchange message between node to create our topology of clusters , so we used a C++ language to create our algorithm and represent it by package graphic.h .

**What is C++ Why we choose it :**

C++ is based on the C language and it was developed in early 1980's by Bjarne Stroustrup at AT&T Bell Laboratories, Here “++” use for the extension because “++” is a syntactic construct used in C to increment a variable. Most of C++ content is the super-set of “C” ,Due to this extension most C programs can be compiled using a C++ compiler.

A C++ program is a collection of commands, which tell the computer to do “something”. This collection of commands is usually called C++ source code

C++ is the Mid-Level programming language because it acquire the feature of Low level as well as high level programming language.[40]

We choose C++ because :

- Object oriented
- Portable language (writing a program irrespective of operating system as well as Hardware)
- C++ use multi-paradigm programming. The Paradigm means style of programming .paradigm concerned about logics , structure and procedure of the program. C++ is multi-paradigm means it follow three paradigm Generic, Imperative, Object Oriented.
- It is useful for low level programming language and very efficient for general purpose.
- C++ provide performance and memory efficiency.
- It provide a high level abstraction.
- in the language of the problem domain.
- C++ is compatible with C.
- C++ used reusability of code.
- C++ used inheritance, polymorphism.
- Most of Simulate programs use C++ [40]

### **Discription of the simulation :**

The approach can be divided into 2 main parts :

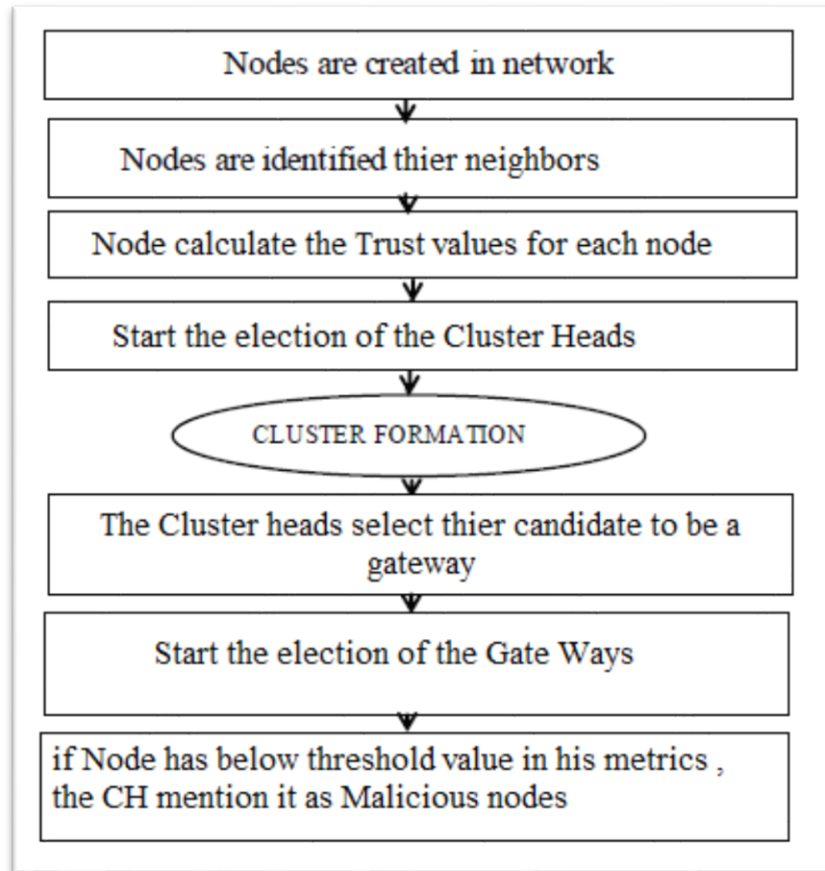
- Inisialized network : in this part , nodes create table nieghbors , calculate trust values for each node , elect the cluster head nodes , create the clusters and choose the gateways nodes .
- Analysed the malicious nodes : in this part , the cluster heads detect the malicious nodes , and choose other gateways if they are malicious .

The simulation experiments are carried out in visual studio 2010 in windows 8.1 , We assume all nodes can be nieghbors if they are close to each other at most a 250 meters . Nodes must get update of the trust values of their neighbors periodically.

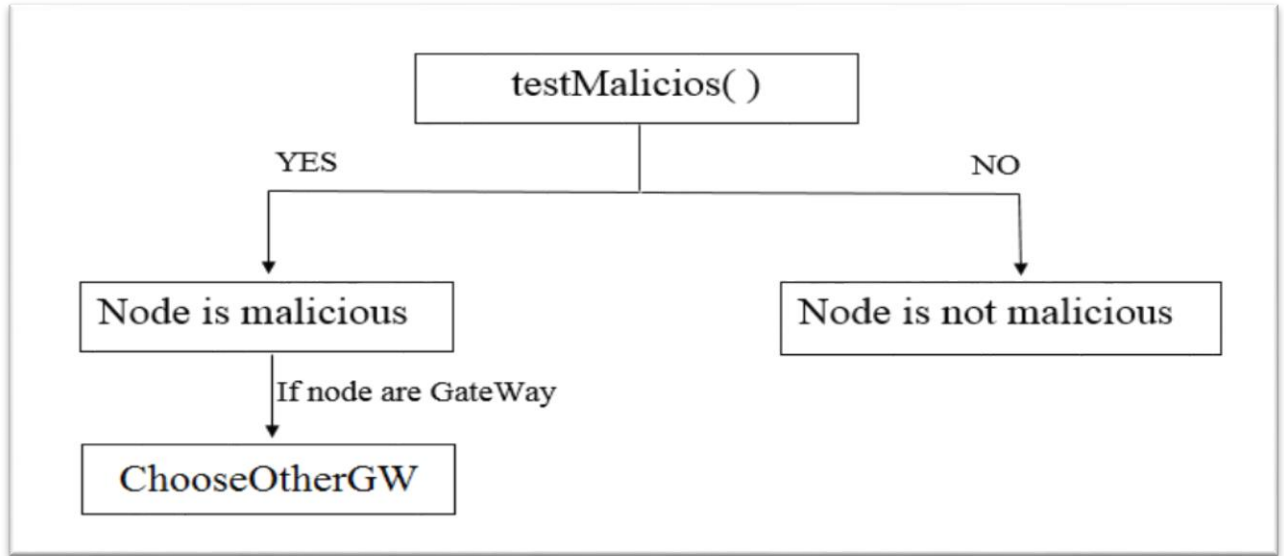
In the simulation, 80-20 mobile nodes move in a 1000 meter X 1000 meter rectangular region.

Compared with a square region, the rectangular region can enlarge the average route length, so that we can easily observe the performance difference in different scenarios. The mobility model is the random waypoint model, which is commonly used by other researchers. In our simulation, the QoS ( Quality of Service ) is in the high level, the metrics that we choose it to present the direct trust are : forwarding packet, link rate, and the energy of each node, we choose them randomly. The malicious node can detect if the values of forwarding packet or the link rate are less than 20%.

At each change position of nodes, the table of neighbors must be updated, and if node out/ in from the table neighbors, it should recalculate his trust values .



**Figure 4.6 :** present our Architecture



**Figure 4.7 :** present the analysed the malicious nodes

## 6 Result and Analyze :

We present the results of the simulation on two main parts witch are represented as follows : the coverture of cluster head and number malicious node detect by cluster head

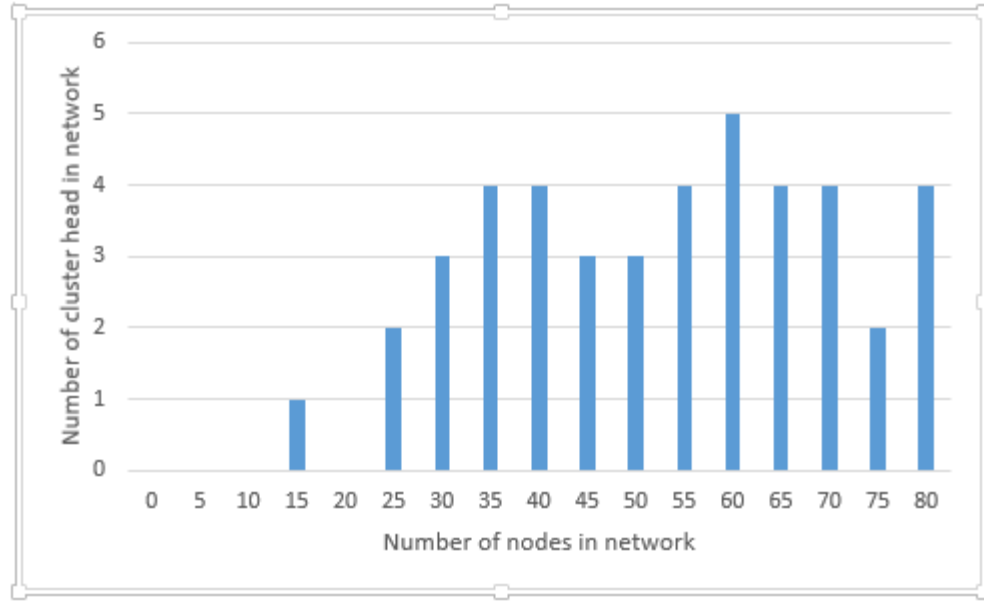
### 6.1. the coverture of cluster head :

The result are resumed in table 4.1 and we will present it in the next graph, the table present the number of Cluster heads on the number of nodes .

Number of nodes	0	5	10	15	20	25	30	35	40	45	50
Number of Cluster heads	0	0	0	1	0	2	3	4	4	3	3

Number of nodes	55	60	65	70	75	80
Number of Cluster heads	4	5	4	4	2	4

**Table 4.1:** number of CH by number of nodes



**Figure 4.8:** the increase of number of CH by number of nodes

In this result we observe that whenever the number of nodes increases in network, the number of cluster heads varies according to the number node elector and the position of nodes in network the cover surface of the network. So it will let more control on the movement of data in the cluster and cover the maximum surface.

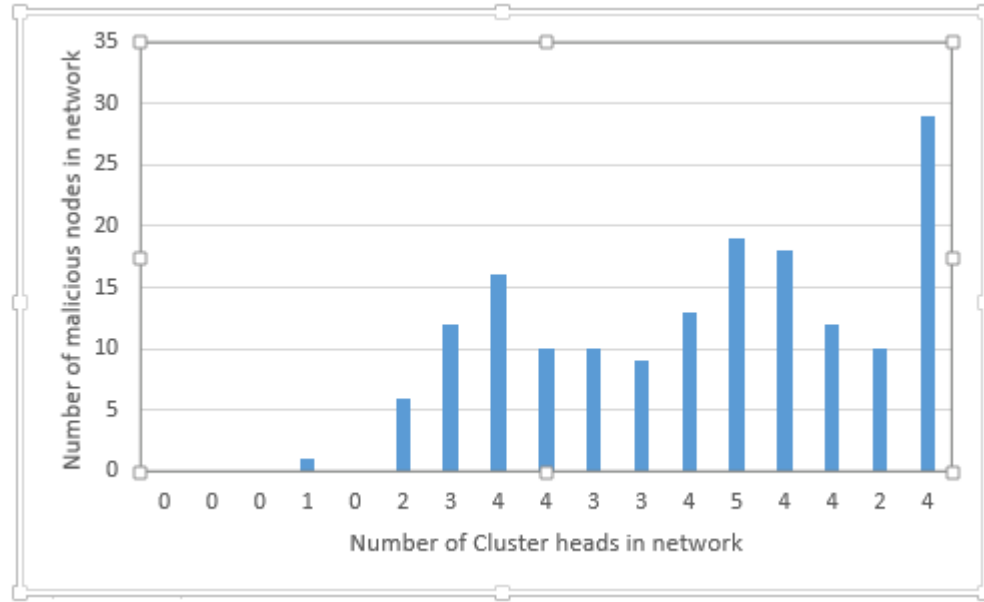
## 6.2. number malicious node detect by cluster head :

The results are resumed in table 4.2 and we will present it in the next graph, the table present the number of malicious nodes detect by the number of Cluster heads.

Number of cluster head	1	0	2	3	4	4	3	3
Number of malicious node	1	0	6	12	16	10	10	9

Number of cluster head	4	5	4	4	2	4
Number of malicious node	13	19	18	12	10	29

**Table 4.2:** Number of malicious nodes detected by the CH



**Figure 4.8:** Number of malicious nodes detected by the CH

In this result we observe that when the number of the cluster heads are vary , the number of detection the malicious node are vary too according to the number of the nodes join in the clusters and them position in networks .

## 7 Conclusion

This chapter was divided into two main parts, the approach and the simulation results. In the first part we set some definitions about our network then we give a description about our architecture and we mentioned some interesting Algorithms.

In the second part, we present our environment of our simulation, we talked about the tools of programming and we present our results at the end of the chapter.

## **CONCLUSION**



# Conclusion

Nowadays, mobile adhoc network (MANETs) are used in many areas. Security was and still one of the most addressed problems in MANETs. One of the most techniques that have a great attend in the last years is the intrusion detection systems.

In the course of this dissertation, we proposed an intrusion detection mechanism based on the cluster by considering the Trust metric in the cluster formation phase in order to improve detection accuracy. The main purpose of this mechanism is to detect the huge number of malicious nodes in the networks.

The experimental results clearly showed that the proposed mechanism has a high level to cover the network area according to the number of nodes, which means that the detection of malicious nodes could be more accurate.

As a prospect for this work, we aim to improve our approach to adding new metrics such as social trust metrics. In addition, we should test and evaluate our approach using NS-2 simulator with ESPER engine and comparing it with existing cluster based intrusion detection approaches.

## References

- [1] C.Cordeiro & D.Agrawal, “Mobile Ad hoc Networking “,OBR Research Center for Distributed and Mobile Computing, ECECS University of Cincinnati ,Cincinnati, OH 45221-0030-USA.
- [2] M.Dipobagio, "An overview on Ad hoc Networks", Institute of Computer Science (ICS),Freie Universitat Berlin,2009.
- [3] M.Yadav, N.Uparosiya ,” Routing Protocols, Advantages, Problems and Security” , International Journal of Innovative Computer Science & Engineering, Volume 1 Issue 2, 20 Nov 2014, Page No. 12-17, Jaipur, India.
- [4] Mr. Ankur Khetrapal , “Routing techniques for Mobile Ad Hoc Networks” , International Conference on Wireless Networks, ICWN 2006, Las Vegas, Nevada, USA, June 26-29, 2006
- [5] Guoyou He. “Destination-sequenced distance vector (DSDV) protocol.” Technical report, Helsinki University of Technology, Finland. 2 Dec 2003
- [6] Niththiyanathan Jeyaratnarajah, “Cluster-Based Networks”, Helsinki University of Technology,Espoo, Finland. Nov 2001
- [7]Nicolas DAUJEARD,Julien CARSIQUE,Rachid LADJADJ;Akim LALLEMAND,le routage dans les réseaux mobiles Ad hoc,igm.univmlv.fr/~duris/NTREZO/20022003/**AdHoc**.doc accessed on: 16/02/2017
- [8]<http://file.scirp.org/Html/3-9701112%E3%80%81/29c09322-280e-4a35-8ec1-7f23cf7334a9.jpg> accessed on: 16/02/2017
- [9] Nicklas Beijar,”Zone Routing Protocol (ZRP)”, Networking Laboratory, Helsinki University of Technology P.O. Box 3000, FIN-02015 HUT, Finland 1999
- [10] D. Helen , D. Arivazhagan ,”Applications, Advantages and Challenges of Ad Hoc Networks” ,Journal of Academia and Industrial Research (JAIR),(2014)

- [11] Razanfindralambo, T., Guerin-Lassous, I. “Increasing fairness and efficiency using the MadMac protocol in ad hoc networks”, Ad hoc Networks Journal, Elsevier ED.6(3), 408-423 (2008)
- [12] [https://en.wikipedia.org/wiki/Intrusion\\_detection\\_system](https://en.wikipedia.org/wiki/Intrusion_detection_system) accessed on: 25/02/2017
- [13] Sevil Şen, John A. Clark, ”INTRUSION DETECTION IN MOBILE AD HOC NETWORKS”, Guide to Wireless Ad Hoc Networks , pp 427-454 , UK 2009
- [11]<http://krazytech.com/technical-papers/intrusion-detection-and-avoidance-system> accessed on: 25/02/2017
- [15]<https://www.sans.org/reading-room/whitepapers/detection/intrusion-detection-systems-definition-challenges-343> accessed on: 25/02/2017
- [16]<https://www.hackthis.co.uk/articles/basics-of-intrusion-detection-systems> accessed on: 25/02/2017
- [17] Seyed Ali Mirheidari, Sajjad Arshad, Rasool Jalili , “Alert Correlation Algorithms: A Survey and Taxonomy”, Springer International Publishing Switzerland 2013
- [18]<http://dictionary.reference.com/browse/correlation> accessed on: 25/02/2017
- [19] Herve Debar, Marc Dacier, Andreas Wespi, “Towards a taxonomy of intrusion-detection systems”, IBM Research Division, Zurich Research Laboratory, Saumerstrasse 4, CH-8803 Ruschlikon, Switzerland 1999.
- [20] <http://slideplayer.com/slide/7807296/> accessed on: 16/02/2017
- [21] Tony Howlett, Open Source ,Security Tools ,Practical Applications for Security, Prentice Hall,Professional Technical Reference,Upper Saddle River, NJ 07458 “livre”.
- [22] Asieh Mokarian, Ahmad Faraahi, Arash Ghorbannia Delavar, False Positives Reduction Techniques in Intrusion Detection, Systems-A Review, Payame Noor University, Tehran, IRAN (2013)
- [23] Fabien Pouget, Marc Dacier, Alert Correlation: Review of the state of the art,

Corporate Communications Department, Institut Eurecom, France.(2001)

[24] SAFAA O. AL-MAMORY, HONG LI ZHANG, A Survey on IDS Alerts Processing Techniques, School of Computer Science, Harbin Institute of technology, CHINA (2007)

[25] P. Brutch and C. Ko, "Challenges in Intrusion Detection for Wireless Ad-hoc Networks," Proceedings of 2003 Symposium on Applications and the Internet Workshop, pp. 368-373, January 2003.

[26] S. Sen and J. A. Clark, Intrusion detection in mobile ad hoc networks, In: Guide to Wireless Ad Hoc Networks, S. Misra, I. Woungang and S.C. Misra (Eds.), Springer, 2009.

[27] Z. ZARRINGHALAMI AND M. KUCHAKI RAFSANJANI, "A SURVEY ON INTRUSION DETECTION SYSTEMS IN COMPUTER NETWORKS " , J. Appl. Math. & Informatics Vol. 30(2012), No. 5 - 6, pp. 847 – 864

[28] Y. Zhang, W. Lee, and Y. Huang, "Intrusion Detection Techniques for Mobile Wireless Networks," *ACM/Kluwer Wireless Networks Journal (ACM WINET)*, Vol. 9, No. 5, September 2003.

[29] GA .Jacoby, NJ.Davis, Mobile host-based intrusion detection and attack identification, IEEE Wireless Communications August 2007.

[30] A. Lauf, R. A. Peters, W. H. Robinson, "A Distributed Intrusion Detection System for Resource-Constrained Devices in Ad Hoc Networks". Elsevier Journal of Ad Hoc Networks, vol. 8, issue 3, pp. 253-266, May 2010.

[31] K. Nadkarni, A. Mishra, "A Novel Intrusion Detection Approach for Wireless Ad Hoc Networks," IEEE Wireless Communications and Networking Conference (WCNC. 2004), Vol.2, pp. 831 – 836, March 2004.

[32] W.Wang, H.Man, Y. Liu. A framework for intrusion detection systems by social network analysis methods in ad hoc networks. Wiley Security and Communication Networks April, 2009.

[33] J. Zhou, J. Chen, W. Xie, J. Li, Improved Weight Clustering Algorithm for IDS in Mobile Ad hoc Network. In International Conference Wireless Communications, Networking and Mobile Computing, Pp. 1565-1568, WiCom (2007).

- [34] S.Bose, S.Bharathimurugan, A.Kannan. Multi-layer integrated anomaly intrusion detection system for mobile ad hoc networks. IEEE ICSCN 2007. Chennai, India: MIT Campus, Anna University; February 2007.
- [25] M.Chuan-xiang, F.Ze-ming. A novel intrusion detection architecture based on adaptive selection event triggering for mobile ad-hoc networks. In: IEEE second international symposium on intelligent information technology and security informatics; January 2009.
- [36] E.Darra, C.Ntantogian, C.Xenakis and S.Katsikas , A Mobility and Energy-Aware Hierarchical Intrusion Detection System for Mobile Ad Hoc Networks , International Conference on Trust, Privacy and Security in Digital Business , 8th International Conference, TrustBus 2011, Toulouse, France, August 29 - September 2, 2011.
- [37] A. Bentaleb and H. Debbi, “A New Cluster Based Intrusion Detection for Mobile Ad hoc Networks”, unpublished paper.
- [38] P. Dewan and P. Dasgupta. Trusting Routers and Relays in Ad hoc Networks. In Proceed-ings of First International Workshop on Wireless Security and Privacy WiSr (2003).
- [39] J. S. Baras and T. Jiang, Managing Trust in Self-Organized Mobile Ad Hoc Networks, Proc. 12th Annual Network and Distributed System Security Symposium Workshop, San Diego, CA, (2005).
- [40] <https://www.go4expert.com/articles/choose-cpp-t3398/> accessed on: 12/05/2017