# EVALUATING AND COMPARISON OF INTRUSION IN MOBILE AD HOC NETWORKS

Zougagh Hicham[1], Toumanari Ahmed[1], Latif Rachid [1] and Idboufker Noureddin[2]

[1]Laboratory Signaux system & Informatique, Ibn zohr University, ENSA Agadir
Hzm_1979@yahoo.fr
Atoumanri@yahoo.fr
Rachid@ensa-agadir.ac.ma
[2]Laboratory Reseaux & Telecom, University Caddi ayyad, ENSA Marrakech
N_idboufker@yahoo.fr

## ABSTRACT

*In recent years, the use of mobile ad hoc network (MANETs) has been widespread in many applications. Due to its deployment nature, MANETs are more vulnerable to malicious attack. The absolute security in the mobile ad hoc network is very hard to achieve because of its fundamental characteristics, such as dynamic topology, open medium, absence of infrastructure, limited power and limited bandwidth. The Prevention methods like authentication and cryptography techniques alone are not able to provide the security to these types of networks. However, these techniques have a limitation on the effects of prevention techniques in general and they are designed for a set of known attacks. They are unlikely to prevent newer attacks that are designed for circumventing the existing security measures. For this reason, there is a need of second mechanism to "detect and response" these newer attacks. Therefore, efficient intrusion detection must be deployed to facilitate the identification and isolation of attacks. In this article we classify the architecture for IDS that have so far been introduced for MANETs, and then existing intrusion detection techniques in MANETs presented and compared. We then provide some directions for future researches.*

## KEYWORDS

*Intrusion Detection System (IDS), MANET, Security, Mobile Agent*

## 1. INTRODUCTION

The mobile ad hoc network does not require expensive base station of wired infrastructure. Nodes within radio range of each other can communicate directly over wireless links, the cooperation of other nodes in network is needed; this is know as multi-hop communication. Therefore each node must act as both a host and a router at the same time. The network topology is constantly changing as a result of nodes joining in and moving out.

Initially, Manets was designed for military application, but in recent years, has found new usage. For example, search and rescue mission, data collection, virtual classes and conferences, PDA or other mobile devices are in wireless communication.

Providing security in mobile ad hoc network (Manet) has become a very importante issue. The first way of securing a mobile ad hoc network at the network layer is to secure the routing protocols because all of routing protocols does not define any measures of security and assumes that each node in the network is not a malicious node. The second way is to develop Intrusion Detection System (IDS) to detect intrusion, identify the malicious nodes, and isolate them from the rest of the network.

DOI : 10.5121/ijdps.2012.3221

Intrusin detection can be classified in two classes: Based on data collection mechanisms and Based on detection techniques:

Based on data collection mechanisms: In this case An IDS may be classified as either host-based or network-based, depending on the data collection mechanism. Host-based IDS (HIDS) systems are designed to monitor, detect and respond to user and system activity and attacks on a given host. While these systems are best suited to combat internal threats/file modifications and can collect and analyze data originating on a computer/processing system that hosts a certain service, they can get unwieldy. Network based IDS (NIDS) deals with information passing on the entire network between any pair of communicating hosts. While it is very good at detecting unauthorized outsider access, bandwidth theft, DOS, it is incapable of operating in encrypted networks and in high-speed networks. In addition, NIDS is effective when the network has certain chokepoints at which detection can be done. As is obvious the NID approach will not be effective in ad-hoc networks on account of absence of any choke points in such networks. As a result one might have to depend on having the intrusion detection mechanisms on all or some of the hosts in the system.

Based on detection techniques: There are three board categories: misuse detection, Anomaly detection, and specification-based detection; Misuse detection uses a priori knowledge on intrusions and tries to detect attacks based on specific patterns or signatures of known attacks. Although misuse detection systems are very accurate in revealing known attacks, their basic disadvantage is that attacking mechanisms are under a continuous evolution, which leads to the need for an up-to-date knowledge base [1]. On the other hand Anomaly detection has the advantage of being able to discover unknown attacks while it adopts the approach of knowing what is normal. As a result it attempts to track deviations from the normal behaviours that are considered to be anomalies or possible intrusion [2]. Finally specification-based detection in wich the system defines a set of constraints that describe the correct operation of a program or protocol. Then, it monitors the execution of the program with respect to the defined constraints [3].

The network infrastructures that be configured to are either flat or multilayer, depending on the applications. Therefore optimum network architecture for a MANET depends on its infrastructure [4]. In a flat network infrastructure, all nodes not considered equal. Thus, they are suitable for application such as virtual classes or conferences. In multilayer infrastructures, all nodes are considred different. Nodes my be partitioned into clusters with one clusterhead for each cluster.To communicate within the cluster, node can communicate directly. However, communication acrosse the clusters must be done through the clusterhead. This infrastructure is suitable for military application [4].

Stand-alone IDS : In this architecture, an IDS is run on each node independently to determine intrusion, and the decision taken for that node is based on a data collected, because there is no interaction among network nodes. Therefore, no data is exchanged. In addition each node has no information about the position of other nodes and no alert information crosses the network. This architecture is not effective because of its limitations. It also more suitable for flat network, but not selected at the IDS for MANETs.

Distributed and cooperative IDS: The nature of MANET is distributed and requires cooperation of other nodes; Zhang and Lee describe a distributed and Cooperative intrusion detection model where every node in the network participates in intrusion detection and reponse [5]. In this model. Each IDS agent is responsible for detection, data collection and local events in order to detect intrusions and generate an independent response. Even though neighboring IDS agents cooperate with each other when there is not any convincing evidence in global intrusion detection.

Hierarchical IDS: Hierarchical IDS architectures have been proposed for multi-layered network infrastructures where the network are divided into clusters. The clusterhead of each cluster has responsibilities compared the other members. For example routing packets across clusters. In this way, this clusterheads, behave just like control points. Each IDS agent is run on every member node and is responsible locally for its node, for example, monitoring and deciding on the locally detected intrusions. Each clusterhead is responsible locally for its node as well as globally for its cluster. For example, monitoring network packets and initiating a global reaction where an intrusion is detected [6].

Mobile Agent for IDS: Mobile agent have been deployed in many techniques for IDS in MANETs. Due to its ability of moving in network, the agent can interact with nodes, collecte information, and execute tasks assigned to them. There several advantages for using mobile agents [7]. Some functions are not assigned to every node; thus, it helps to reduce the energy consumption. Not need to move large amount of data throught the network via moving the analysis programs closer to the audit data. The mobile agents tend to be independent of platform architectures, and thus enable agent based IDS to run under different operating environnements[21].

## 2. Researches Achievement

In this section we presnt a state-of-the-art view of research in IDS for MANETs, including proposed architectures and development work that is going one.

Intrusion Detection Architecture Based on a Static Stationary Database hase been proposed by **SMITH [8].** The architecture is divided into two parts: the mobile IDS agent and the stationary secure database that contains signatures attacks (Fig 1).

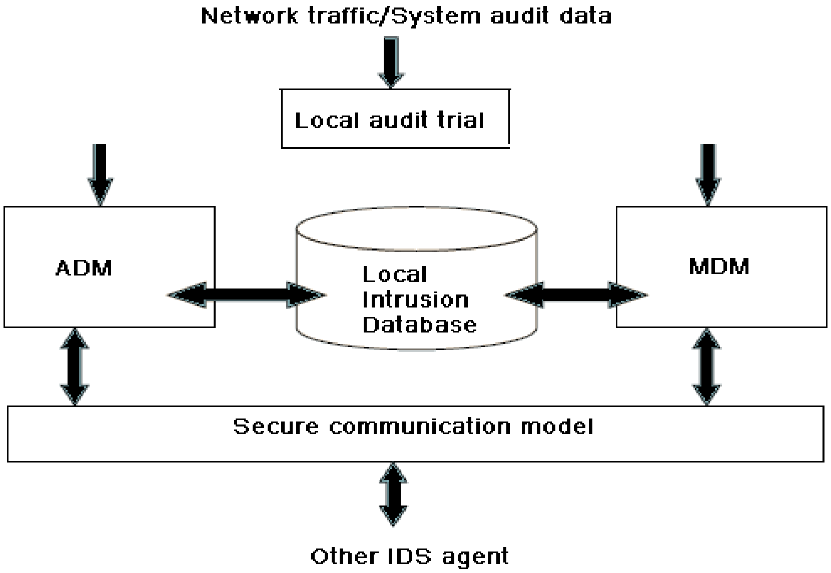

Fig 1: IDS based on stationary secure database.

**Mobile IDS Agent**: Each node in the network will have an IDS agent running on it all the time. This agent is responsible for detecting intrusions based on local audit data and participating in cooperative algorithms with other IDS agents to decide if the network is being attacked. Each agent has five parts:

- Local Intrusion Database (LID): that warehouses all information necessary for the IDS agent, such as the signature files of known attacks, the established patterns of users on the network, and the normal traffic flow of the network. The ADMs and MDMs communicate directly with the LID to determine if an intrusion is taking place.

- The secure communication module is necessary to enable an IDS agent to communicate with other IDS agents on other nodes. It will allow the MDMs and ADMs to use cooperative algorithms to detect intrusions. It may also be used to initiate a global response when an IDS agent or a group of IDS agents detects an intrusion.

- The ADMs (Anomaly detection modules) are responsible for detecting a different type of anomaly. There can be from one to many ADMs on each mobile IDS agent, each working separately or cooperatively with other ADMs.

- The MDMs (Misuse detection modules) identify known patterns of attacks that are specified in the LID. Like the ADMs, if the audit data available locally is sufficient to determine if an intrusion is taking place, the proper response can be initiated.

- Local audit trial: Notify an intrusion by cheking the audit data

**Stationary Secure Database** : The stationary secure database (SSD) acts as a secure trusted repository for mobile nodes to obtain information about the latest misuse signatures and find the latest patterns of normal user activity.

There are a few disadvantages in relying on a stationary database to provide vital IDS information. If an SSD is used, mobile nodes will have to be attached to the non mobile database periodically to stay up to date with the latest intrusion information. This may not be an option for some mobile ad hoc environments. Also, since the SSD must be a secure trusted source, it cannot be taken onsite without significant risk.

**Zhang** and **Lee** also proposed the model for a distributed and cooperative IDS as shown in (Fig 4) [5].

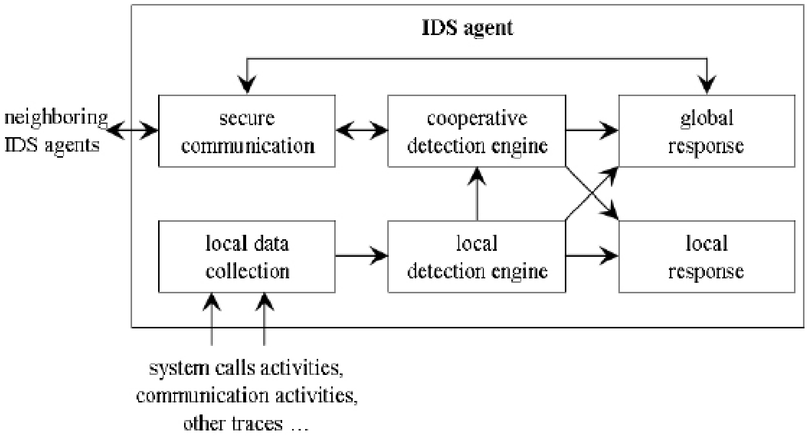

Fig 2: An Intrusion Detection System model.

In this model, an IDS agent runs at each mobile node, and performs local data collection and local detection. The authors consider two attack scenarios separately: abnormal update to routing tables and detecting abnormal activities in other layers than the routing layer.

The model for an IDS agent is structured into six modules. The local data collection module collects real-time audit data, which includes system and user activities within its radio range. This collected data will be analyzed by the local detection engine module for evidence of anomalies. If an anomaly is detected with strong evidence, the IDS agent can determine independently that the system is under attack and initiate a response through the local response module (i.e., alerting the local user) or the global response module (i.e., deciding on an action), depending on the type of intrusion, the type of network protocols and applications, and the certainty of the evidence. If an anomaly is detected with weak or inconclusive evidence, the IDS agent can request the cooperation of neighbouring IDS agents through a cooperative detection engine module, which communicates to other agents through a secure communication module [5].

**Albert et al** proposed a distributed and collaborative architecture of IDS by using mobile agents. This architecture takes advantage of the Simple Management Network Protocol (SNMP). The LIDS is distributed and utilizes mobile agents on each of the nodes of the ad hoc network [9]. In order to make a global concern for the community, the different LIDS coexiste within it and should collaborate. The different LIDS in a community will thus exchange two type of data: Security data to obtain complementary informations from collaborating hosts, and intrusion alerts to informe other of a locally detection intrusion. The LIDS architecture are shown in (Fig 3).

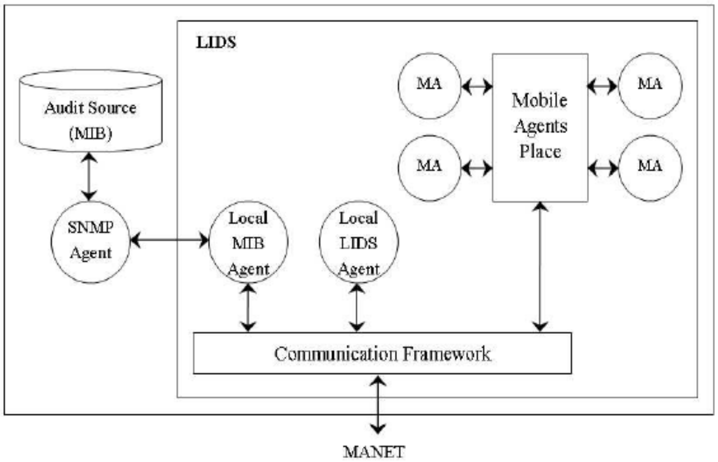

Fig 3: LIDS Architecture.

The key elements of the architecture are:

- ***A local LIDS agent:*** is in charge of local intrusion detection and response. It also reacts provided by other node in order to protect itself against this intrusion.

- ***Mobile Agent***: collect and process data on remots hosts with an ability to transfer the result of a computation back to their home LIDS or to migrate to other node far further investigation. The security control of these agent can be taken in charge by the mobile agent place. An agent should be able to protect itself from malicious mobile agent place.

- ***Local MIB agent*****:** provides a means of collecting MIB (Management Information Base variables for either mobiles agent or the local LIDS agent. If SNMP (Simple Network Management Protocol ) runs in the node, the local MIB agent will be the interface with the runing SNMP based agent should be developed specialy. To allow optimised updates and

  retrivial of the MIB variables used by intrusion detection. The interface between the LIDS and this tailor-made agent.

- ***Communication Framwork***: To facilite for both internal and external communication with a LIDS.

- ***Mobile Agent Place****:* To provide a security control to mobile agents.

In this design the local LIDS can use either anomaly or misuse detection . However, the combination of two mecanisms will offert the better model. Once the local intrusion is detected. The LIDS initiates the reponse and informs the other nodes in the network, upon receiving an alert, the LIDS can protect itself against the intrusion.

The novely in this sheme lies in its use of SNMP data located in MIBs as audit source and the use of mobile agent to process data at the source to reduce communication overheads. The use of a standart alerte format, Intrusion Detection Exchange Format (IDMEF), Intrusion Detection Exchange Protocol (IDXP).

**Karachirski and guha** have proposed a distributed intrusion detction system for ad hoc wireless network based on mobile agent technologie [10]. The system can be divided into three main modules, each of wich represents a mobile agent with certain functionlity: monitoring, decision making and initiating a response (Action). By separating functional tasks into categories and assignig each task to a different agent, the workload is distributed whiche is suitable for the caracteristics of MANETs. The proposed IDS is built on a mobile agent framwork as shown in (Fig 4).

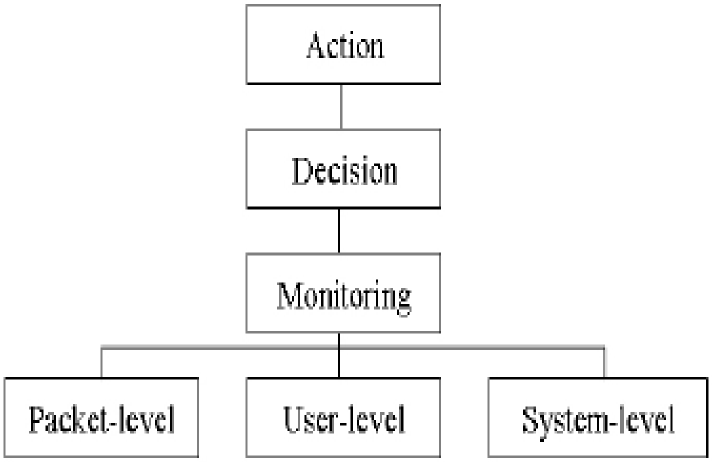

Fig 4: Layered Mobile agent Architectur.

- **Network monitoring:** Only certain nodes have sensor agents for network packet monitoring to preserve computation power and batterie power of mobile hosts.

- **Host monitoring:** every node on the Manet is monitored intrnally by a host monitoring agent. This includes monotoring system-level and application-level activities.

- **Decision Agent:** The decision agent is run only on certain nodes, mostly those nodes that run network monitoring agents. These nodes collect all packets within its radio range and analyze them to determine whether the network is under attack. If the local detection agent cannot make a decision on its own host due to insuficient evidence, its local detection agent reports to this decision agent in order to investigate further. This is done by using packet-monitoring results that comes from the network-monitoring sensor that is running locally. If the decision agent concludes that the node is malicious [6] .
- **Action**: every node has an action modules responsible for resolving intrusion situation on a host.

  The network is logically divided into clusters with a singl clusterhead for each cluster. This clusterhead will monitor the packets within the cluster. The select nodes host network monitoring sensors that collect all packets, and analyse the packets for know pattern of attacks.

**Sun et al [11]** has proposed an anomaly-based two-level nonoverlapping Zone-Based Intrusion Detection System (ZBIDS). By dividing the network into nonoverlapping zones (zone A to zone I). The nodes can be categorized into two types: the intrazone node and the inter-zone node (or a gateway node)(Fig 5). Each node has an IDS agent run on it. This agent is similar to the IDS agent proposed by Zhang and Lee (Fig 6 ). Others components on the system are data collection module and detection engine, local aggregation and correlation (LACE) and global aggregation and correlation (GACE). The data collection and the detection engine are responsible for collecting local audit data and analyzing collected data for any sign of intrusion respectively. The remainder, LACE module is responsible for combining the results of these local detection engines and generating alerts if any abnormal behavior is detected. These alerts are broadcasted to other nodes within the same zone. However, for the GACE, its functionality depends on the type of the node. If the node is an intra-zone node, it only sends the generated alerts to the inter-zone nodes. Thus, if the node is an inter-zone node, it receives alerts from other intra-zone nodes, aggregates and correlates those alerts with its own alerts, and then generates alarms. The intrusion response module is responsible for handling the alarms generated from the GACE.

Using the aggregation algorithm under the zone based famwork, ZBIDS can reduce the false alarm ratios to an acceptabl level, especially at high mobility levels. The gatway node can also present more diagnostic information about the attacks. Therefore, the local IDS agent and the agregation algorithm under the zone based framework complement each other to form a complete MANET IDS.

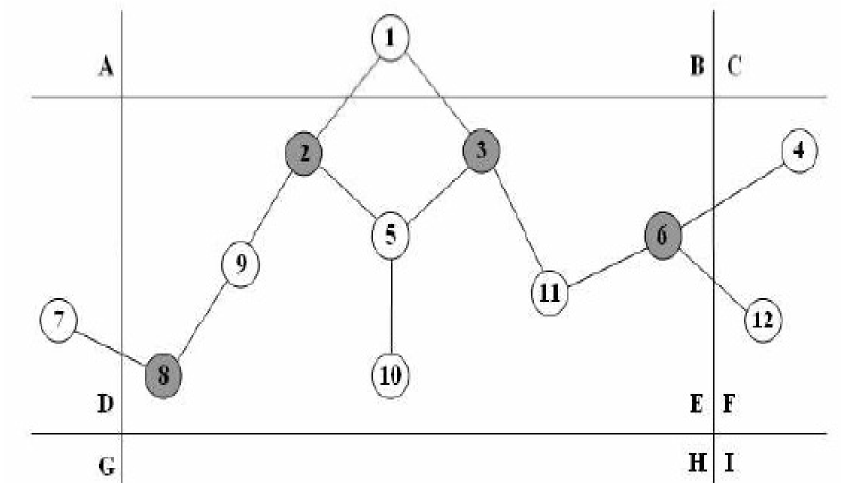

Fig 5: ZBIDS for MANETs

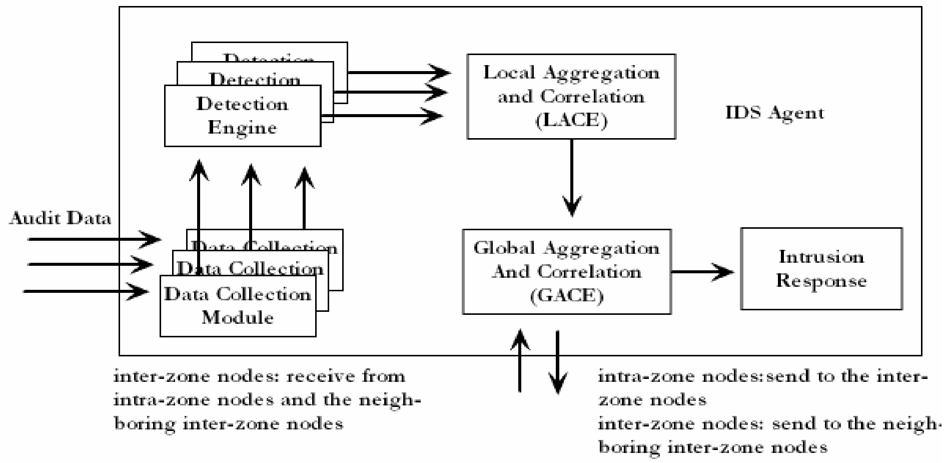
Detection
Detection
Detection Engine
Local Aggregation and Correlation (LACE)
IDS Agent
Audit Data
Data Collection
Data Collection
Data Collection Module
Global Aggregation And Correlation (GACE)
Intrusion Response
inter-zone nodes: receive from intra-zone nodes and the neighboring inter-zone nodes
intra-zone nodes:send to the inter-zone nodes
inter-zone nodes: send to the neighboring inter-zone nodes

Fig 6: Diagram of an IDS agent in ZBIDS

**Sterne et al. [12]** proposed a dynamic intrusion detection hierarchy that is potentially scalable to large networks use clustering. This methode can be structured in more than tow levels. Thus, nodes on first level are cluster heads, while nodes on the second level are leaf nodes. In this model, every node has the task to monitor, log, analyze, respond, and alert or report to cluster heads. The Cluster heads, in addition, must also perform: (1) Data fusion/integration and data filtering, (2) Computations of intrusion, and (3) Security Management. To form the hierarchical structure, every node uses clustering, which is typically used in MANETs to construct routes, to self-organize into local neighborhoods (first level clusters) and then select neighborhood representatives (clusterheads). These representatives then use clustering to organize themselves into the second level and select the representatives. This process continues until all nodes in the network are part of the hierarchy (Fig 7).

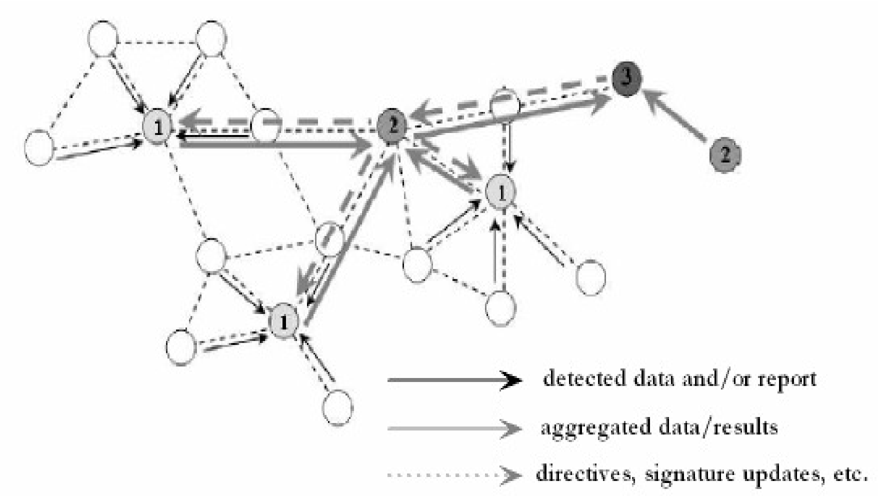
1
2
3
1
1
2
detected data and/or report
aggregated data/results
directives, signature updates, etc.

Fig 7: :Dynamic Intrusion Detection Hierarchy.

**A.Mitrokotsa et al**. in 2006 proposed a distributed model in [13], this approach is for detecting the packets dropping attack based on feature selected from the MAC layer. The proposed intrusion detection system is composed of multiple local IDSs agents. Each IDS agent (Fig 8 ) is responsible for detecting possible intrusions locally. The collection of all the independent IDS agents forms the IDS system for the mobile wireless ad hoc network. Each local IDS agent is composed of the following components:

***Data Collector***: is responsible for selecting local audit data and activity logs.

***Detection Engine***: is responsible for detecting local anomalies using local audit data. The local anomaly detection is performed using the eSOM classification algorithm.

The procedure that is followed in the local detection engine is the one described below:

- Select labeled audit data and perform the appropriate transformations.
- Compute the classifier using training data and the **eSOM** algorithm.
- Apply the classifier to test local audit data in order to classify it as Normal or Abnormal.

***Response Engine***: If an intrusion is detected by the Detection Engine then the Response Engine is activated. The Response Engine is responsible for sending a local and a global alarm in order to notify the nodes of the mobile ad hoc network about the incident of intrusion. Special attention should be paid on the function of the Response Engine in order to avoid possible flooding caused by the notification messages of intrusion. Thus, the broadcasted notification of intrusion is restricted to a few hops away from the node where the anomaly has been detected since the neighboring nodes run the greatest risk of possible intrusion. When the Response Engine is activated, the node fires a fake RTS (Ready to Send) message destined to the suspicious node. If the suspicious node replies to that packet then the node is classified as malicious. Otherwise, the node fires an AODV_ERROR message as the suspicious node is indicated as moved. After the discovery of the adversary the local IDS agent fires an ALERT message notifying its one hop neighbors. Alternatively, the local IDS agent could send ALERT messages to all potentially traffic generators that exist in its routing table, thus achieving a global response to all nodes that are directly influenced by the malicious node.

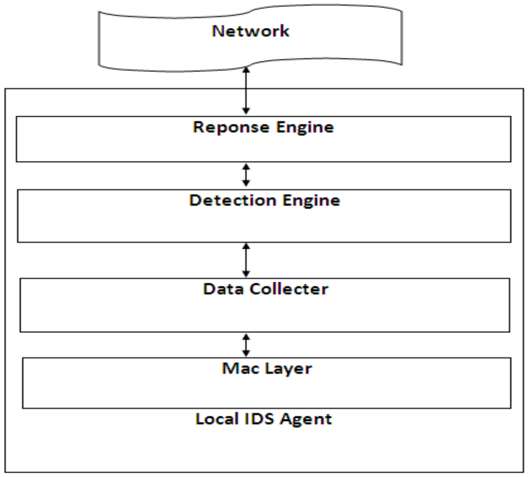

Fig 8: IDS with multipl local IDS

**R.Nakkeeran et al**. in 2010 proposed an Agent Based cooperative and distributive model in [14]. This model provides the three different techniques to provide sufficient security solution to current node, Neighboring Node and Global networks (Fig 9). It has been explained in the following section.

- ***Home Agent:***

Home agent is present in each system and it gathers information about its system from application layer to routing layer.

- Current node: If an attacker sends any packet to gather information or broadcast through this system,the Home-Agent calls the classifier construction to find out the attacks. If an attack has been made, it will filter the respective system from the global networks.

- Nighbouring node: Any system in the network transfer any information to some other system, it broadcast through intermediate system. Before it transfer the message, it send mobile agent to the neighboring node and gather all the information and it return back to the system and it calls classifier rule to find out the attacks. If there is no suspicious activity, then it will forward the message to neighboring node.

- Data collection: Data collection module is included for each anomaly detection subsystem to collect the values of features for corresponding layer in a system. Normal profile is created using the data collected during the normal scenario. Attack data is collected during the attack scenario.

- Data process: The audit data is collected in a file and it is smoothed so that it can be used for anomaly detection. Data preprocess is a technique to process the information with the test train data. In the entire layer anomaly detection systems, the above mentioned preprocessing technique is used.

- **Cross feature analysis for classifier sub model construction.**

- **Local integration**: Local integration module concentrate on self system and it find out the local anomaly attacks. Each and every system under hat wireless networks follows the same methodology to provide a secure global network.

- **Global integration:**

Global integration module is used to find the intrusion result for entire network. The aim of global integration is to consider the neighbor node(s) result for taking decision towards response module.

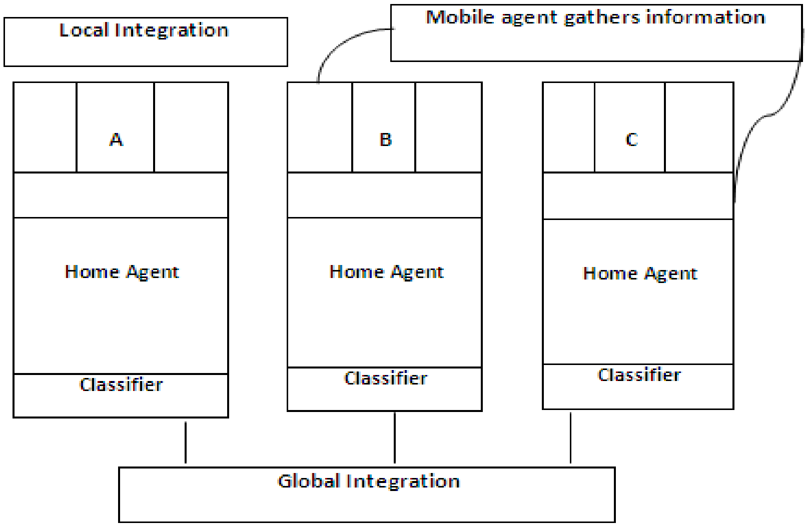

Fig 9: Proposed System Architecture

# 3. INTRUSION DETECTION TECHNIQUES MISBEHAVING NODE IN MANET

## 3.1 Watchdog and Pathrater Approche.

Tow techniques were proposed by Sergio Marti et al [15], Watchdog and pathrater, to be added on top of the standart routing protocol (DSR) [16].

A **watchdog** identifies the misebehaving nodes by eavesdroping on the transmission of the next hop. A pathrater helps routing protocols avoid these nodes.

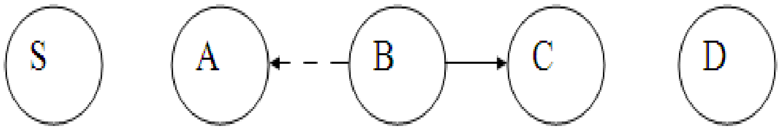

Fig 10: Although node B intends transmit a packet to node C, node A could overhear this transmission.

Fig 10 , shows how the watchdog works. Assume that node S wants to send a packet to node D, which there exists a path from S to D through nodes A, B, and C. Consider now that A has already received a packet from S destined to D. The packet contains a message and routing information. When A forwards this packet to B, A also keeps a copy of the packet in its buffer. Then, it promiscuously listens to the transmission of B to make sure that B forwards to C. If the packet overheard from B (represented by a dashed line) matches that stored in the buffer, it means that B really forwards to the next hop (represented as a solid line). It then removes the packet from the buffer. However, if there's no matched packet after a certain time, the watchdog increments the failures counter for node B. If this counter exceeds the threshold, A concludes that B is misbehaving and reports to the source node S.

DSR with the woatchdog has the advantages that it can detect misbehavior at the forwarding level and not just the link level. Watchdog weakneesses are that it might not detect amisbehaving node in the presence of : ambiguous collisions, receiver collisions, limitted transmission power, false misebehavior, collusion and partial dropping.

The **pathrater,** combines Knowledge of misbehaving nodes with link reliability data to pick the route most likely to be reliable. Each node maintains a rating for every other node it knows in the network. The pathrater can choose the path with the highest metric. Therfore, the path metrique is calculating by averaging the node rating in the path.

## 3.2 CONFIDANT

Bachrgger and Lebudec[17] proposed a CONFIDANT (Cooperation of nodes, Fairness In dynamic Ad hoc Networks) wich is in fact an expansion of DSR Protocol..This technique is similar to watchdog and pathrater. Each node can observe the behavior of all its neighboring nodes that are within its radio range and learn from them. This system also solves the problem of Watch and Pathrater, such that misebehavior are punished by not including them in routing and not helping them in forwarding packets, so they are punished. Additionally. When a node discovers à misbehaving node, it inform all other nodes and they too do not use this node.

CONFIDANT protocol consists of monotoring System, Reputation System, Trust Manager and Path manager. Their tasks are divided into two section: the process to handl its own observations and the process to handl reports from trusted nodes (Fig11).

For observations the monitor uses a “neighborhood watch” to detect any malicious behaviors with in its radio range. If a suspicious event is detected, the monitor then reports to the reputation system. At that time, the reputation system performs several cheks and updates the rating of the reported node in the reputation table. In the rating result is unacceptable, its passes the information to the path manager, wich is removes all paths containing the misbehavior node. Then the trust manager sends an alarm to warm other nodes that consider these nodes as ftiends.

When the monitoring receives an alarm message from trusted nodes, at first the trust manager evaluates the message to see if the source node is trustworthy. If so, the alarm message with the trust level will be stored in the alarm table. All alarm message of the reported node will then be combined to see if there is enough evidence to identify that it is malicious. In this case, the information will be sent to reputation system, which then performs the same functions in the previous paragraph.

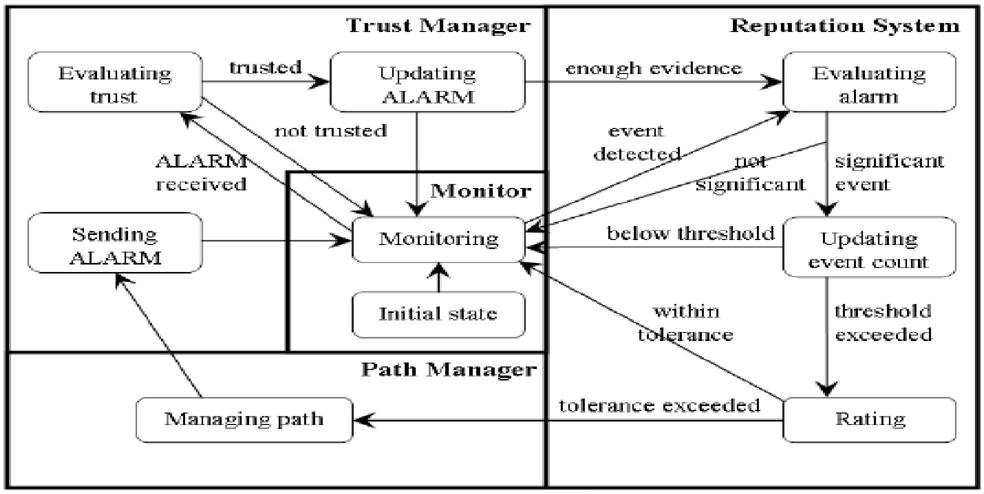

Fig 11 : Trust architecture and finite state machine within each node.

### 3.3. CORE

Michiardi and Molva [18] presented a technique to detect a specific type of misbehaving nodes, which are selfish nodes, and also force them to cooperate. This technique is based on a monitoring system and a reputation system, wich includes both direct and indirect reputation from the system. Sometimes nodes do not misebehave intentionally; for example whem their battery is low, they should not be considered misbehaving nodes and be fired from the network. To do so, the reputation should be rated based on past reputation. The participation in the network can be categorized into several functions such as routing discovery (in DSR) or forwarding pachets. The difference between CORE and CONFIDANT is that only allows positive reports to pass through but CONFIDANT allows the negative ones. This means that CORE prevents false reports, and thus it prevents a DOS attack which CONFIDANT cannot do when a node cannot cooperate, it is given a negative rating and its reputation decrease. In contrast a positive rating is given to a node from which a positive report is received and then its reputation increases.

### 3.4. OCEAN

Bansal and Baker [19] also proposed a protocol called OCEAN (Observation-based cooperation enforcement in Ad hoc Networks) which is an extension of DSR protocol. OCEAN uses a monitoring and a reputation system. However, contrary to previous approaches, OCEAN relies only on its own observation to avoid the new vulnirability of false accusation from second-hand reputation exchange.

OCEAN divides routing misbehavior into two groups: misleading and selfish. If a node takes part in routes finding but does not forward a packet, it is therfore a misleading node and misleads other nodes. But if a node participate in routes finding, it is considered as a selfish node.

In order to detect misleading routing behaviors, after a node forwards a packet to its neighbor, it saves a packet in a given time period, it is monitored. It then produces a positive or negative event as its monitoring results in order to update the rating of neighboring node. If the rating is lower than faulty threshold, neighboring node is added to the list of problematic nodes and also added to RREQ as an avoid-list. As a result, all traffic from the faulty neighbor node will be rejected. This node is given a specific time to return to the network because it is possible that this node is wrongly accused of misbehaving.

### 3.5. ExWatchdog

Nasser and Chen [20] proposed an IDS called ExWatchdog which is an extension of Watchdog. Its function is also detecting intrusion from malicious nodes and reports this information to the response system. Watchdog resides in each node and is based on overhearing. Thus a serious problem arises when the node that is overhearing and reporting itself is malicious, and then it can cause serious on network performance.

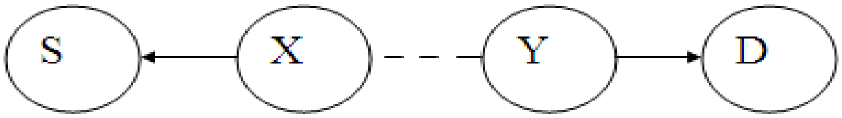

Fig 12: **X** falsefly report **Y** as misebehaving node.

In the (fig 12) , node X could report the node Y is not forwarding packet in fact it does. This will cause S to make B as misebehaving when A is the real culprit.

The main feature of the proposed system is its ability to discover malicious nodes which can partition the network by falsely reporting other nodes as misbehaving and then proceeds to protect the network. So, ExWatchdog solves a fatal problem of Watchdog.

## 4. SUMMARY

In this paper we survey several intrusion detection shemes and intrusion detection techniques for misbehaving nodes that have been proposed recently.

Firstly, the highlighted features of schemes of IDS are summarized in (Tab 2). Sever memory constraints on a mobile device imply that misuse detection systems that need to store attack signatures will be relatively to be less effecctive. Therfore, distributed anomaly detection is by far the methodology of choice for intrusion detection in MANETs. In addition there is a trend to use a mobile agent for intrusion detction and response in mobile ad hoc networks because this agents adress the search and analysis problems involving multiple distributed resources in an efficient manner.

Secondly, if we review all the intrusion detection techniques above , we can conclude that although of this techniques use the warchdog mechanism, they improve it and solve some of its problems ang there are common in detecting selfish nodes. (Tab 1) represents the final comparison between discussed intrusion detection techniques.

Tab 1: Intrusion detection technique comparison.

| **ID Techniques** | | **Watchdog/Pathrater** | **Confidant** | **Core** | **ExWatchdog** | **Ocean** |
|---|---|---|---|---|---|---|
| Observation | Self to neighbor | Yes | Yes | yes | Yes | yes |
| | Neighbor to neighbor | No | Yes | no | No | yes |
| Misbehavior Detection | Malicious-routing | No | Yes | no | Yes | no |
| | Malicious-packet forwarding | Yes | Yes | no | Yes | no |

| | | | | | | |
|---|---|---|---|---|---|---|
| | Selfish routing | No | Yes | yes | No | yes |
| | Selfish packet forwarding | Yes | Yes | yes | Yes | yes |
| Punishement | | No | Yes | yes | No | yes |
| Avoid misbehaving node in rout finding | | Yes | Yes | no | Yes | yes |
| Architecture | | Distributed and cooperative | | | | Stand alone |

## 5. Conclusion

Ad hoc networks are an increasingly promising area of research with lots of pratical applications. However, MANETs are extremely vulnerable to attacks, due to their dynamically changing topology, absence of conventional security infrastructures and open medium of communication, which, Unlike their wired countreparts, cannot be secure.

Intrusion detection can compliment intrusion prevention techniques (such as encryption, authentification, secure MAC, secure routing, etc.) to improve the network securing. However new techniques must be developed to make intrusion detection work better for the wireless ad hoc environment. The aim of an IDS is detecting attacks on mobile nodes or intrusion in to network. Intrusion detection systems, if well designed, effectively can identify misbehaving activities and help to offer adequate protection. Therefore, an IDS has become an indispensable component to provide defense-in-depth security mechanisms for MANETs. However, attackers may try to attack the IDS system itself [15]. Accordingly, the study of the defense to such attacks should be explored as well. In our futur works we intend to concept and implement an intrusion detection system on top of the optimized link state routing protocol (OLSR)

Tab 2: comparison of different IDS

| **PROPPOSED SYSTEM** | **ALGORITHM** | **ARCHITECTURE** | **HIGHLIGHTS** |
|---|---|---|---|
| • IDS based on a static<br>• stationary data base (SSD)<br>By Smith (2001) | •Mobile Agent Anomaly, Misuse & Hybride.<br>•Independently decision making. | • Mobile IDS agent.<br>• Stationary secure data | • The use of SSD limits communication with IDS agent<br>• SSD stored in hight physical security area<br>• Periodically up to date with non mobile database |
| Local IDS (LIDS)<br>By Albert & al (2002) | •. Mobile Agent based distributed anomaly detection<br>• Independently decision making. | • Several data collecting agent (LIDS, Mobile agent, MIB Agent).<br>• A common communication framework. | • Use SNMP data located in MIB to process data, transmit SNMP requests to remote hosts to overcome the unreliability of UDP by using Mobile Agent.<br>• Cost of local information collection is negligeable by runing SNMP agent on each node. |
| Distributed IDS using multiple agent<br>By Kachirski & guha (2002) | • Mobile agent based anomaly decision. | • Multiple sensor type for specific function :<br>• Network Monitoring.<br>• Host Monitoring.<br>• Decision Making.<br>• Action. | • Multiple sonsors used to implement a bandwidth conscious sheme.<br>• Distributed IDS make better network performance. |

| | | | |
|---|---|---|---|
| Distributed & cooperatif IDS By zhung & Lee (2002) | • Distributed<br>• Anomaly Detection | Distributed & cooperatif IDS | • Detection localy and independently.<br>• Detect globaly and cooperatively by voting |
| Zone Based IDS framework (ZBIDS) By sun & al (2003) | • Mobile agent<br>• Markove Chaine | • Special kind of clustering algorithm.<br>• Data collection Module.<br>• Detection Engine.<br>• LACE & GACE | • Using aggregation algorithm under ZBIDS can reduce the false alarm ratios to an acceptable level.<br>• Aggregation algorithm achive better detection ratio.<br>• Propagation of the local alerts of intrazone node =>extra communication overhead introduced |
| Intrusion detection of packetrs dropping attack in MANET By Mitrokosta & al (2006) | Neural network based distributed detection | • Data collector<br>• Detection engine<br>• Reponse engine | • Identify the source of the packet dropping attack.<br>• Able to identify new attack.<br>• The classes of the trained data have to be difined manually.<br>• Continuously updating trained eSOM |
| Agent Based Efficient anomaly Intrusion Detection System By Nakeran & al (2010) | Agent Based cooperative and distributed | • Local integration.<br>• Global Integration.<br>• Home Agent<br>• Calssifier | • No discription about security of Mobile Agent<br>• Performance is better compared to other algorithms<br>• Low false alarm rate |
| Dynamic Hierarchical Intrusion Detection Architecture By Stern & al (2005) | • Cluster Based signature<br>• Dynamic & cooperative<br>• Logical IDS | • Data fusion / integration /reduction<br>• Intrusion Detection Computation<br>• Security Management | • Not rely solely on promiscuous node monitoring like many proposed architectures<br>• This architecture supports direct periodic reporting where packet counts and statistics are sent to monotoring node periodically |

# REFERENCES

[1] Faroq Anjum,Dhanant Subhadrabandhu and Saswati Sarkar, “Signature Intrusion Detectio for Wireless Ad Hoc Networks: A Comparative study of various routing protocols”, in 2003.

[2] P C Kishore Raja, Dr.Suganthi.M, R.Sunder, “WIRELESS NODE BEHAVIOR BASED INTRUSION DETECTION USING GENETIC ALGORITHM”, Ubiquitous Computing and Communication Journal, 2006.

[3] Ping Yi, Yichuan, Yiping Zhong, Shiyong Zhag, “Distributed Intrusion Detection for Mobile Ad Hoc Networks ”, Processing of the 2005 IEEE Symposium on Application and the Internet Workshops AINT-W05.

[4] 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.

[5] Y. Zhang and W. Lee, “Intrusion Detection in Wireless Ad Hoc Networks,” 6th Int’l. Conf. Mobile Comp. and Net., Aug. 2000, pp. 275–283.

6 ] Tiramuch Anantvalee, Jie Wu, “ A survey on Intrusion Detection in Mobile Ad Hoc Networks” 2006 Springer.

[7] A. Mishra, K. Nadkarni, and A. Patcha, ,"Intrusion Detection in Wireless Ad Hoc Networks," IEEE Wireless Communications, Vol. 11, Issue 1, pp. 48-60, February 2004.

[8] A. B. Smith, “An Examination of an Intrusion Detection Architecture for Wireless Ad Hoc Networks,” 5th Nat’l. Colloq. for Info. Sys. Sec. Education, May 2001.

[9] P. Albers et al., “Security in Ad Hoc Networks: a General Intrusion Detection Architecture Enhancing Trust Based Approaches,” 1st Int’l. Wksp. Wireless Info. Sys., Ciudad Real, Spain, Apr. 3–6, 2002.

[10] O. Kachirski and R. Guha, “Intrusion Detection Using Mobile Agents in Wireless Ad Hoc Networks,” Knowledge Media Net., Proc. IEEE Wksp., July 10–12, 2002, pp. 153–58.

[11] B. Sun, K.Wu, and U. W. Pooch. Alert Aggregation in Mobile Ad Hoc Networks," Proceedings of the 2003 ACM Workshop on Wireless Security (WiSe'03) in conjuction with the 9th Annual International Conference on Mobile Computing and Networking (MobiCom'03), pp. 69-78, 2003.

[12] D. Sterne, P. Balasubramanyam, D. Carman, B. Wilson, R. Talpade, C. Ko, R. Balupari, C.-Y. Tseng, T. Bowen, K. Levitt, and J. Rowe, “A General Cooperative Intrusion Detection Architecture for MANETs," Proceedings of the 3rd IEEE International Workshop on Information Assurance (IWIA'05), pp. 57-70, March 2005.

[13] Aikaterini Mitrokotsa, Rosa Mavropodi, Christos Douligeris,”Intrusion Detection of Packet Dropping Attacks in Mobile Ad Hoc Network” TAyia Napa, Cyprus, July 6-7, 2006.

[14] R. Nakkeeran, T. Arul doss Albert and R.Ezumalai,”SAgent Based Efficient Anomaly Intrusion Detection System in Ad hoc networks”, IACSIT International Journal of Engineering and Technology Vol. 2, No.1, February, 2010.

[15] S. Marti et al., “Mitigating Routing Misbehavior in Mobile Ad Hoc Networks,” Proc. 6th Annual Int’l.Conf. Mobile Comp. and Net., Boston, MA, pp. 255–65

[16] D. B. Johnson, and D. A. Maltz, "The Dynamic Source Routing Protocol for Mobile Ad Hoc Networks (Internet-Draft)," Mobile Ad-hoc Network (MANET) Working Group, IETF, October 1999.

[17] S.Buchgger and J. Le Boudec, “ Performance analysis of the CONFIDANT protocol” in proc IEEE/ACM Workshop on Mobil Ad Hoc Ntworking and computing (MobiHoc’02), Lausannne, Switzeland, June 2002? PP.226-336.

[18] P. Michiardi and R. Molva, “ core a collaborative reputation mechanism to enforce node cooperation in Manet,” Communication and multimedia Security Conference (CMCS’02) Sepember 2002.

[19] S.Bansal and M. Baker, “”Observation-based cooperation enforcement in ad hoc networks,” Research report cs.NI/307012, Stanford University, 2003.

[20] Nidal Nasser and Yunfeng Chen, “Enhanced Intrusion Detection System for Discovering Malicious Nodes in Mobile Ad hoc Networks”, Proc. ICC 2007.

[21] D.B.Ray and R.Chaki “Mobile based detection of selfish node in Manet”, International Journal of Wireless & Mobile Networks (IJWMN) Vol. 3, No. 4, August 2011.