# A Survey on VANET Intrusion Detection Systems

Mohammed ERRITALI [*1], Bouabid El Ouahidi [*2]
[*] First- Second: Department of Computer Science
Mohamed V Agdal University – L.R.I ,Faculty of Sciences Rabat, Morocco
[1] mederritali@yahoo.fr
[2] ouahidi@fsr.ac.ma

***Abstract*— In recent years, the security issues on Vehicular ad hoc networks (VANETs) have become one of the primary concerns. The VANET is inherently very vulnerable to attacks than wired network because it is characterized by high mobility, shared wireless medium and the absence of centralized security services offered by dedicated equipment such as firewalls and authentication servers. Attack countermeasures such as digital signature and encryption, can be used as the first line of defense for reducing the possibilities of attacks. However, these techniques have limited prevention in general, and they are designed for a set of known attacks. They are unlikely to avoid most recent attacks that are designed to circumvent existing security measures. For this reason, there is a need of second technique to "detect and notify" these newer attacks, i.e. "intrusion detection". This article aims to present and classify current techniques of Intrusion Detection System (IDS) aware VANETs.**

**Keyword- Intrusion Detection System (IDS), VANET, Survey.**

## I. INTRODUCTION

A Vehicular ad hoc network called VANETs [1,2] is a mobile network allowing to vehicles to communicate with each other in the absence of fixed infrastructure, with the aim of improving road safety through the exchange of alerts between neighborhood vehicles or to offer new comfort services to road users. The characteristics of these networks such as: shared wireless medium, the highly dynamic network topology absence of conventional security infrastructures pose a number of nontrivial challenges to security design.

Vulnerabilities of ad-hoc networks are not limited unfortunately in the problem of shared wireless medium but also in routing mechanism and auto-configuration used.

These mechanisms are based on trust between the participating nodes. If a node has a malicious behavior, all services offered by the cooperative network will be paralyzed (routing table poisoning, congestion, packet alteration ...).

An effective way to identify when an attack occurs in a VANET is the deployment of an Intrusion Detection System (IDS).

An intrusion detection system (IDS) is a mechanism to identify abnormal or suspicious activities on the target analyzed (network or host). It allows having knowledge of successful or failed intrusions attempts. IDS solutions are proposed for detecting internal attacks. These are attacks that cryptographic solutions cannot detect. Indeed, internal attacks are attacks by compromised nodes. An IDS is often used as one second line of defense after the cryptographic systems.

In general, an intrusion detection system is composed of three phases: a phase of data collection followed by an analysis phase and finally a phase response to prevent or minimize the impact of the attack on the system. IDS is located at some special nodes called monitors or monitoring nodes. The deployment of these nodes differs depending on the protocol type and the architecture of the IDS.

IDS can be classified according to detection techniques used into three categories:

- Signature based system [3]: The system has a database behavior of certain attacks with which are compared the data collected. An attack is detected if the data coincide with malicious behavior already registered.

- Anomaly detection system [4]: the system detects any behavior which deviates the standard preestablished behavior and triggers a response (notification).

- Specifications based system [5]: the system defined a set of conditions that a program or protocol must satisfy. An attack is detected if the program or protocol does not meet the conditions set of proper operation.

We can also classify IDS according to the architecture into three basic categories: stand-alone, hierarchical or distributed [6].

The rest of this paper will be structured as follows. Section 2 describes IDS architecture. In section 3 and 4, we present a discussion regarding the IDS classification. Finally, the conclusions and future research are shown in section 5.

## II. IDS ARCHITECTURES

1. Stand-alone IDS: In this architecture, each node is based on its local resources to collect data on remote nodes of the networks and detects intrusion .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.

2. Cooperative and distributed IDS [7]: Cooperative IDS are characterized by cooperation between neighboring nodes to detect the intrusion, if detection is unaccomplished individually. This cooperation is realized by exchanging information or alerts. The major problem for the IDS is that they cause degradation of network performance by traffic exchanged between IDS agents. Cooperation between the IDS based on techniques different as mobile agents and neural networks...

3. Hierarchical IDS [8,9]: To remedy the lack of cooperation between different IDS proposed for ad hoc networks, an alternative method has been proposed for intrusion detection. This approach is based on the division of the network into a set of groups (clusters) each having one cluster Head determined by a cooperative algorithm between nodes. Hierarchical intrusion detection Systems try to reduce the cooperation between nodes by dividing the network into clusters. In this case the cooperation is carried out between the elected cluster Head and each of members of the same cluster, as is the case in ad hoc multilayer networks.

So an alert is reported to the cluster head if a member node of this cluster cannot detect an attack only or the certainty of detection is below a certain threshold. Cluster Head in this type of IDS acts as the administrator of the group and allows monitor what is happening in his cluster. On the other hand the detection agent is distributed in all network nodes, whereas the response to alerts is a hierarchical manner according to the level of certainty of detection. This approach minimizes the network load since the cooperation is reduced between cluster head and members. However, it does not have a global vision of network because of the lack of cooperation between different clusters and it is consequently ineffective against some distributed attacks.

## III. ANOMALY DETECTION SYSTEMS

### *3.1 Watchdog and Pathrater: IDS based on monitoring of router nodes*

Watchdog [10] consists to monitor the behavior of all nodes, and choose the safest route through the module Pathrater. Therefore, all nodes in the network monitor each other as mesh architecture. Figure 1 below shows the Watchdog mechanism.

Indeed, if the node S wants to send a packet to node D via intermediate nodes A, B and C, the packet is transmitted to the node A which in turn forwards it to the node B but retains a copy of the packet.

The next step in the process is to monitor whether B will retransmit the packet to node C by listening and comparing all the packets sent by node B. If node B retransmits the packet after a certain time, node A can conclude that B is malicious node and its decision is reported at node S.

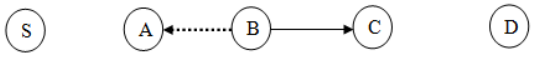


Figure 1. Watchdog Principle [10]

### *3.2 Confidant: a system based on reputation*

Buchegger and Le Boudec are proposed an extension to DSR routing protocol [11] called Confidant [12], using a mechanism similar to the Watchdog and Pathrater mechanism. Each node monitors the behavior of its neighbors. Once a malicious behavior is detected, the malicious node is excluded from all the services offered by the network (for example packet retransmission) and isolates it with a reputation system by alerting other nodes with a broadcasted warning message.

Figure 2 below shows the Confidant mechanism.

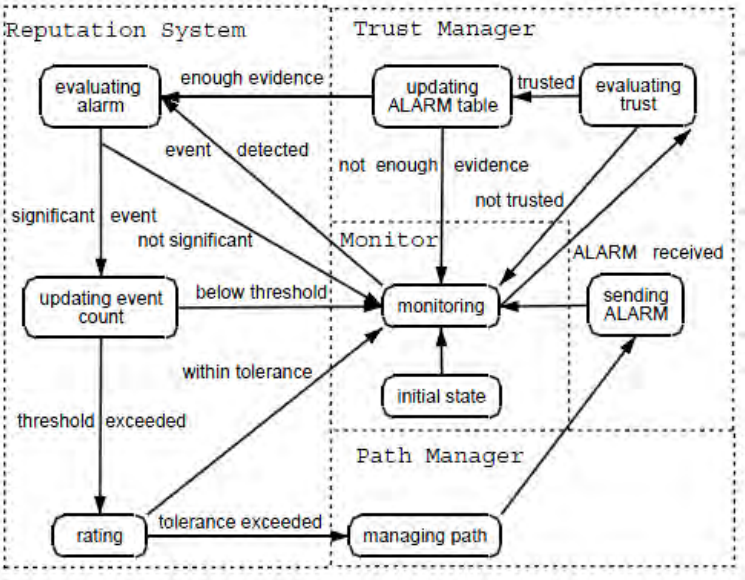


Figure 2. Confidant Principle [12]

The proposed mechanism uses the module monitoring to detect any malicious activity. If a suspected case is detected, the module Monitor sends a notification to the Module Reputation System, which in turn is an update of his reputation table based on the activity reports received.

If the reputation value exceeds a critical threshold, an alarm is sent to other nodes via the Trust Manager Module and the Path Manager, which removes all routes containing the malicious node.

Since this protocol allows sending alarms, the network can be subject to attacks by sending false accusations. Thus, the denial of service attack can be easily achieved.

*3.3 CORE: a system based on reputation*

The CORE [13] mechanism offers a solution to counter the selfish behavior of nodes. The solution is to offer incentives to any node wishing to participate in collaborative processes. The incentives are inspired by game theory. Each node has a reputation to establish reflecting his honesty. To transmit or receive a packet, the node must have sufficient reputation. In addition, each node detected malicious or selfish sees its reputation diminish what has the effect of completely isolating the node of network (unable to send or receive packets). This obliges nodes to adopt a honest behavior.

In CORE, each node assigns a reputation value to any other node involved in the collaborative process. Note that CORE unlike Confidant assigns only positive values to the reputation, if the node receives a positive decision of another node (indirect supervision). Negative values are reserved only for direct monitoring if the monitored node is not cooperating.

In doing so, the mechanism eliminates any false accusations and denial of service attacks which suffers confidante.

If a node A requests a service from node B (packet retransmission, route discovery), node B checks its reputation table and calculates the total value of reputation (monitoring direct and indirect) for node A. if it turns out that the node A has a negative global reputation then the request will be rejected and the node will be isolated.

*3.4. Zhang et Lee IDS*

Zhang and Lee [7] are proposed a cooperative distributed architecture as shown in figure 3 where each node is responsible for detecting signs of intrusion locally. Each node, called IDS agent is responsible for data collection and detection of malicious activities. However, neighbors IDS agents may cooperate with each other for global intrusion detection.

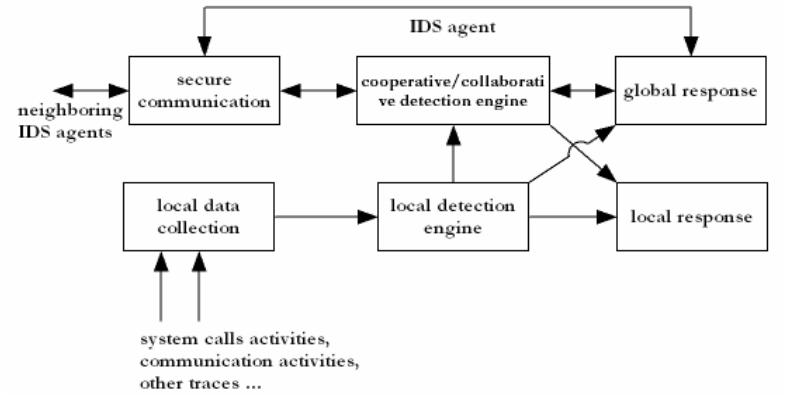


Figure 3. IDS agent model

The model of the IDS agent is divided into six modules: local data collection module that collects real-time data including system events and operations performed by the user. The local module detection engine decides from data collected if the system is attacked or not. The module can initiate a response if an attack is detected with specific evidence. The response is executed by the module local response (alert the local user) or module global response (global alert) depending on the type Attack of protocol or application.

The cooperative detection engine module is executed when an abnormality is detected with weak evidence and requests the cooperation of the other nodes of network via another secured communication module called secure communication.

*3. 5 Zone-Based Intrusion Detection System (ZBIDS)*

Sun [14] are proposed a system that split the network into into non-overlapping zones (zone A to zone I). Figure 4 below shows the ZBIDS mechanism.

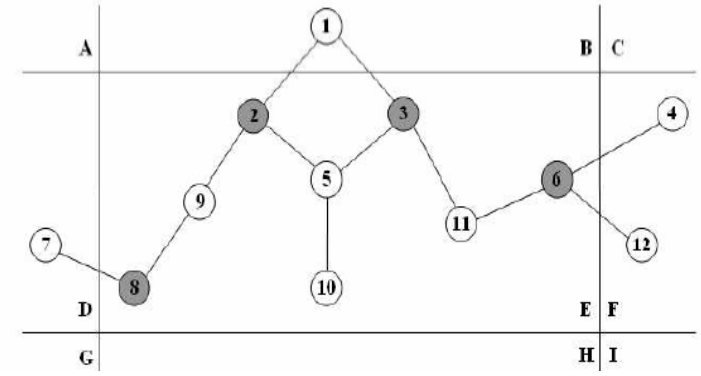


Figure 4. ZBIDS Principle

Referring to Figure 4, the nodes can be classified into 2 different groups:

• Intrazone would be independent nodes by a shown in figure 4 with nodes 9, 5, 10, and 11.

• Interzone node would be the nodes that have a physical connection to a different node in a different zone area. Example would be node 8, 2, 3 and 6.

ZBIDs use local and collaborative detection technique. The local detection module consists of a general intrusion detection agent model and a Markov chain-based anomaly detection algorithm. The collaborative detection module works on the ZBIDS agents and uses an aggregation algorithm on the gateway nodes.

## IV. SIGNATURE BASED SYSTEMS

*4.1 SNORT*

In [15] the authors propose a way to adapt the famous intrusion detection system (Snort) to a personal distributed network environment. The idea is that the IDS must first be distributed and be completely in tune with user settings such as profiles, keys, access rights....

SNORT [16] is used to analyze network traffic of type IP, it can be configured to operate in three modes:

- Sniffer: In this mode, Snort reads the packets on the network and displays in a continuous manner on the screen.

- Packet logger: in this mode SNORT logs network traffic in directories disk.

- NIDS: In this mode, Snort network traffic analysis, compares the traffic to rules already established user-defined actions to be executed.

### *4.2 Jaydip Sen clustered IDS*

Jaydip Sen [9] proposes a semi-Centralize clustered architecture that integrates a local intrusion detection.

In this architecture the network is divided into clusters which are managed by cluster head and inter-cluster communication takes place through gateway nodes by use of mobile agents and every node maintains a database of known attack for signature based detection.

## V. CONCLUSION AND PERSPECTIVES

The design of security solution in vehicular ad hoc networks attracts more and more attention from research groups. Indeed VANETs are extremely vulnerable to attacks, due their shared wireless medium and the absence of conventional security infrastructures.

However Intrusion detection systems can compliment intrusion prevention techniques (such as encryption, authentification) to improve the network securing. With the highly dynamic network topology, all of the proposed intrusion detection systems (IDSs) are distributed and have a cooperative architecture and use anomaly detection approach.

The aim of an IDS is detecting attacks on mobile nodes or intrusion in to network. However, attackers may try to attack the IDS system itself [10]. 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 greedy perimeter stateless routing protocol (GPSR).

## REFERENCES


[1] Sofiane Khalfallah, Moez Jerbi, Mohamed Oussama Cherif , Sidi-Mohammed Senouci , Bertrand Ducourthial, Expérimentations des communications inter-véhicules, Colloque Francophone sur l'Ingénierie des Protocoles (CFIP), Les Arcs : France (2008).

[2] Moez JERBI , Protocoles pour les communications dans les réseaux de véhicules en environnement urbain : Routage et GeoCast basés sur les intersections . Thèse , France (2008).

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

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

[5] 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.

[6] Mishra, A., K. Nadkarni and A. Patcha. 2004. « Intrusion detection in wireless ad hoc networks». IEEE Wireless Communications, vol. 11, no 1, p. 48-60.

[7] 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.

[8] Tiramuch Anantvalee, Jie Wu, "A survey on Intrusion Detection in Mobile Ad Hoc Networks" 2006 Springer.

[9] Jaydip Sen, "An Intrusion Detection Architecture for Clustered Wireless Ad Hoc Networks", Second International Conference on Computational Intelligence, Communication Systems and Networks, 2010.

[10] Marti, S., T.J. Giuli, K. Lai et M. Baker. 2000. « Mitigating routing misbehavior in mobile ad hoc networks ». In Proceedings of the Sixth Annual ACM/IEEE International Conference on Mobile Computing and Networking, p. 255-265.

[11] D. Johnson, B.D.A. Maltz, and Y.C.Hu, "The Dynamic Source Routing Protocol for Mobile Ad Hoc Networks (DSR)", draft-ietf-manet-dsr-10.txt, 2004.

[12] 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.

[13] P. Michiardi and R. Molva, " core a collaborative reputation mechanism to enforce node cooperation in Manet," Communication and multimedia Security Conference (CMCS'02) September 2002.

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

[15] K. Masmoudi and H. Afifi, 2007. An identity-based key management framework for personal networks. IEEE International Symposium on Security in Networks and Distributed Systems (SSNDS'07), 537–543.

[16] Klaus Müller, IDS - Système de Détection d'Intrusion, Partie II. http://www.linuxfocus.org/Francais/July2003/article294.shtml