International Journal of Electrical, Electronic and Communication Sciences
ISSN: 2517-9438
Vol:10, No:8, 2016

Smart Trust Management for Vehicular Networks

Amel Ltifi, Ahmed Zouinkhi, Med Salim Bouhlel

***Abstract*—**Spontaneous networks such as VANET are in general deployed in an open and thus easily accessible environment. Therefore, they are vulnerable to attacks. Trust management is one of a set of security solutions dedicated to this type of networks. Moreover, the strong mobility of the nodes (in the case of VANET) makes the establishment of a trust management system complex. In this paper, we present a concept of 'Active Vehicle' which means an autonomous vehicle that is able to make decision about trustworthiness of alert messages transmitted about road accidents. The behavior of an "Active Vehicle" is modeled using Petri Nets.

***Keywords*—**Component, active vehicle, cooperation, petri nets, trust management, VANET.

I. Introduction

DUE to their simplicity of deployment and their low costs, the spontaneous networks are more and more used in various fields, such as the driving assistance and military monitoring. These networks are governed by strong constraints on storage capacity, computing power, and energy consumption. Moreover, these networks are vulnerable to attacks, because they are in general deployed in an open and thus easily accessible environment. An intruder can gain control over one or more nodes and deteriorate the operation of the network in various manners such as measurements falsification and denials of service. A second weakness of the spontaneous networks is the unreliability. This is related to nodes' characters and the instability of connections which can generate a denial of services and a waste of network power. With that, the strong mobility of the nodes (in the case of a network of vehicles) is added which makes the maintenance of effective routes in the network complex. In such a vulnerable unreliable environment, it is imperative to deploy a trust management system with an effective cooperation model which will be the basis for a reliable and secure routing. Given that, data about vehicles cannot be stored directly, traditional solutions as proposed in [1]-[3] could not be useful for VANET. Moreover, we could not use digital signature mechanism to verify packet integrity because these methods rely on a centralized authority to manage digital certificates. In addition, key revocation and key updating tasks would take much overhead which is not acceptable in an environment such as VANET.

New trust management solutions should be evolved to support the dynamics of VANET. All the methods mentioned in [1] fail to adjust with changes in the VANET environment. Self-organized trust establishment is required because of non-availability of infrastructure and shared global knowledge among the participating nodes. Furthermore, we can rely only on spontaneous communication in trust establishment.

The objective of this paper is to suggest a trust management system and effective cooperation model for vehicular networks. The idea presented is to create a smart daily space between vehicles. The behavior of the smart vehicle in cooperation with other members of VANET architecture was simulated by CPN Tools [4].

After the Introduction, the second part is declined to a brief study of trust management for VANET. Our smart trust management model is explained in the third part. Finally, a last part exposes the Petri Nets modeling of a smart vehicle behavior.

II. Trust Management in VANET

In mobile and heterogeneous network as VANET, trust evaluation of transmitted messages is a hard task. Fig. 1 illustrates challenges encountered by this type of networks including the high mobility and the existence of malicious neighbors.

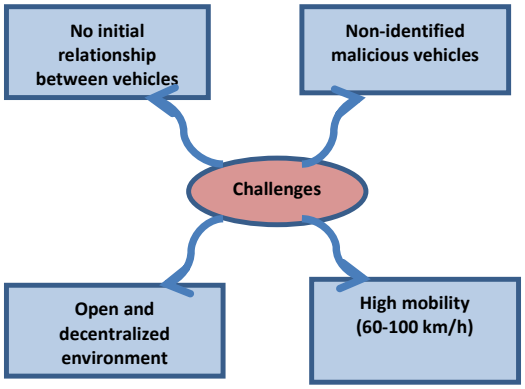

Fig. 1 VANET challenges

Trust management systems can be divided into two classes: Centralized and decentralized systems according to their dependency on trusted authorities. As well, we can divide these systems in trust management system dedicated to MANET network in general and systems specific for VANET as depicted in Fig. 2. A set of trust models for VANET are exploiting a method called "opinion piggybacking" where each vehicle, receiving a message M, attaches its opinion about the trustworthiness of M [5]. This approach is based on frequent gathering of vehicles' opinions which is its major drawback. Other approaches in [6]-[8] have recourse to request a certificate from trusted authorities to decide about data trustworthiness. This approach is not useful due to the absence of central certification authorities in mobile ad-hoc

Amel Ltifi is with the University of Sfax, Tunisia (e-mail: altifi@gmail.com).

networks such as VANET. At last, it is not feasible to adopt a huge number of existent trust models which require a centralized system or which are based on social networks or neighbors' opinions.

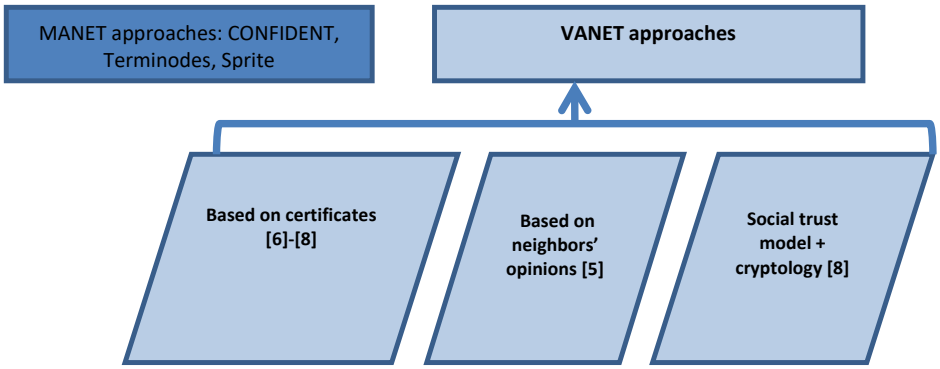

Fig. 2 Trust management approaches

The situation illustrated in this paper is when there is an accident or any obstacle in the road. The first vehicle detecting this event will send a warning message to other vehicles in its transmission range. So, each vehicle receiving the warning is in front of two possibilities as depicted in Fig. 3:

- believe on data received and transmit it
- or ignore it.

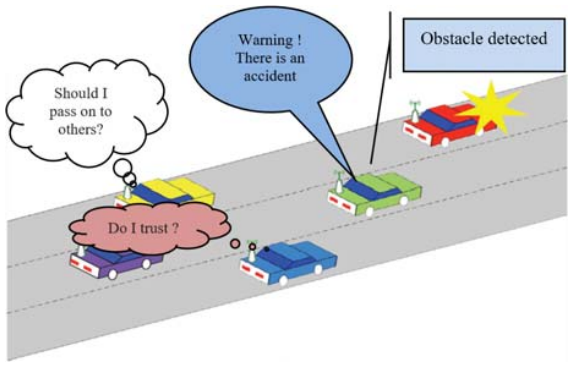

Fig. 3 General scenario

III. Our Cluster Based Approach

A vehicular Ad-hoc network consists of a set of cars which communicate with each other and with other road equipments via short range wireless communication.

Cluster-based approaches could be a practical solution for efficient multi-hop message propagation between vehicles [9]. In order to proactively create groups, nodes should follow a distributed protocol. Therefore, a distributed cluster infrastructure is established.

The cluster based infrastructure is applied in many approaches. In [10], a dynamic Public Key Infrastructure (PKI) is suggested for VANET. Authors propose to distribute central Certification Authority (CA) tasks between a set of dynamic CAs. Dynamic CAs are chosen according to a clustering algorithm where the group leaders (GL) perform the role of CAs. Authors [11] suggested a cluster-based solution which uses symmetric cryptography method for securing vehicles communication.

A. Model Layout

In our approach, vehicles are equipped with intelligent software that manages their security states. And they are organized as a set of clusters. Each cluster has one GL hat is the vehicle having the highest trust level. It is the responsible of creating/updating the trust model containing information about group members like their identifiers, trust value and cooperation's counters values. Moreover, in order to simplify communications between vehicles, vehicles are arranged into groups. In each cluster, the GL is responsible for establishing and arranging the cluster. The communication infrastructure is illustrated in Fig. 4.

The role of the GL is similar to a trusted authority as it is the responsible for managing alert message trustworthiness. The GL is differentiated from other vehicles by having a token.

The GL manages a list M (the reference model) which contains information about vehicles members (identities, their counters cooperation and their trust values).

To construct the reference model M, the GL is responsible for:

- Applying the inscription method on arrival of a vehicle to the group:

Inscription-Method:

1. **if (Idv not exists in M)**
2. **/*creates a new entry */**
3. **CC_v= 0;**
4. **TV_v= 0.5;**
5. **Insert (Id_v, CC_v, TV_v) in M**

- Updating counters cooperation (CC) and trust values (TV) for vehicles members according to their behaviors.
- Periodically, selecting the vehicle with the highest trust value to be the new GL and sending it the reference model **M**.

In order to improve active security and road safety, we presented the integration of intelligent features and autonomous functionalities on vehicles. We will explain by detail in the next section some characteristics of vehicles those

can be employed in our solution.

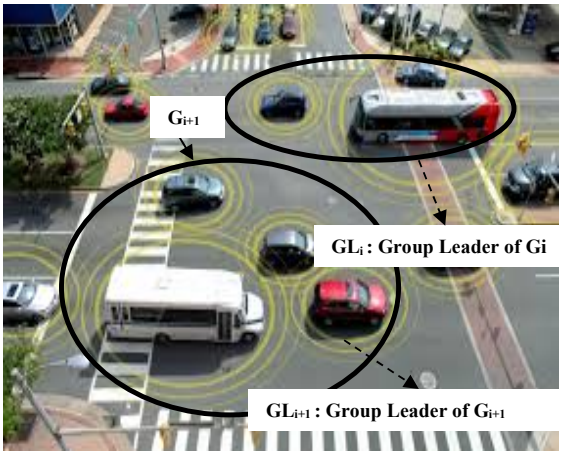

Fig. 4 Model layout of the vehicular network

B. Concept of Active Vehicle

A physical product can be qualified as active communicating while having the following capacities [12], [13]:

- **Memorization**: Storage of necessary information
- **Perception** : Monitoring of its physical environment
- **Communication**: Exchange of information with other object.
- **Action**: Treatment and execution of the mechanisms towards a task
- **Decision**: To make decisions relative to typical situations.

Therefore, the concept of "Active vehicle" is possible due to the appearance of a new generation of smarter-car technology. In addition, a new functional model of each vehicle is suggested to be integrated in vehicles designs in order to apply our trust management system.

C. Functional Model

The smart vehicles are vehicles equipped with a unit named OBU (On Board Unit). This unit can record, calculate, locate and send messages. We employed this unit to handle vehicle and road security through a set of components depicted in Fig. 5.

Each vehicle communicates with other vehicles and Road Side Units (RSUs) through wireless transmission channel. There are two main components that should be integrated in the vehicle: the trust management system and the knowledge base.

The knowledge base is used to make vehicle able to decide about trustworthiness of received warning messages. It processes general information of the vehicle (identifier, constructor, rate, position, direction …) and information concerning the reference trust model (M). In our model, some activities of the GL are achieved by accessing the knowledge base such as updating trust model and verifying alert message trustworthiness. When a vehicle detects an accident in the road, it sends a WARNING message to the leader who verifies the trust level of the vehicle sender and after decides to treat the WARNING message or ignore it.

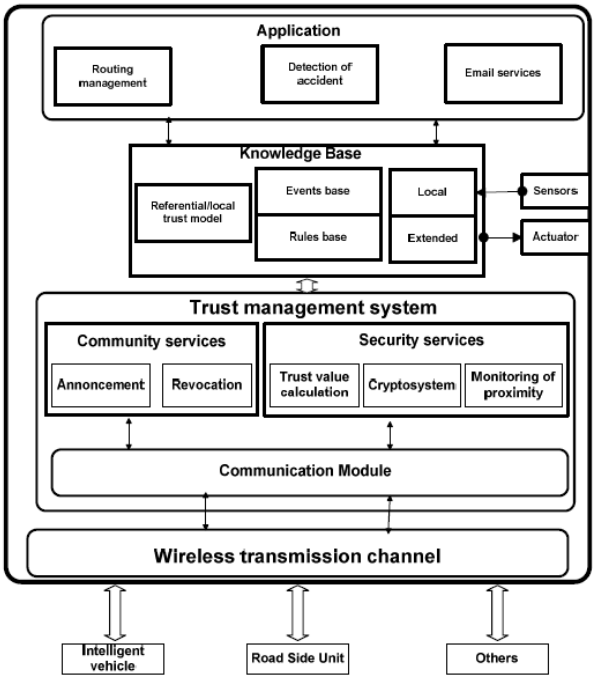

Fig. 5 Functional model of the application

Our trust management system offers many benefits to cars. With the most important is autonomous decision making via the knowledge database facilitating the creation of shared information. Smart cars are able to verify the trust level of received warning messages based on trust model offered by trust management system. The reference trust model is the main component of the knowledge base. This trust model contains the cooperation counter value (CC) and the trust value for each vehicle belonging to the same group. It's updated by the GL according to vehicles behaviors.

D. Transmitted Messages

The majority of VANET applications adopt the method of exchanging messages among cars in a periodic way [14]. So, it is mandatory to employ efficient schemes to exchange safety information and other security-related messages. Establishing a web of trust between vehicles is an appropriate approach to obtain secure communications. Hence, in our model, cars cooperate with each other to establish a trusted community which consists of behaved vehicles. Table I includes the list of messages defined in our communication protocol.

We include, in the suggested vehicle's model, autonomous features and "ambient intelligence" in order to support smart purposes such as decision making and alert messages treatment. We used Petri Net tool for modeling vehicle activities as illustrated in the next section.

TABLE I
TRANSMITTED MESSAGES

Message type	Description
HELLO	sent by a coming vehicle V to the group. After that, It will be sent periodically to detect any alteration of the topology (the leader or the vehicle's successor).
AckHELLO	sent by the leader to a vehicle V as a response to the « HELLO » packet. The vehicle V registers the address of the leader to be used in the communication
theSUCC	is the response to the "HELLO" packet sent by the successor of a sender V
GRE	sent periodically by each vehicle to the leader after receiving an « AckHELLO » from the leader to maintain a continuous connectivity between V and the GL
WARNING	contains some information on an alarm event, it is sent by the vehicle that detects the alarm state to the leader to be verified and registered
IsTRANSMITTED	sent to the leader by a vehicle after transmitting the alarm packet to another vehicle.
AckWARNING	sent by the leader to the vehicle that was detected the alert state when the leader accepts the warning message received after verifying the referential trust model.
ALARM	it contains a hashed and encrypted warning data exchanged between intermediated neighbors.
CONFIRM	sent to the leader by each vehicle after receiving an « ALARM » packet in order to verify its validity.
VALIDATION	sent by the leader as a response to the « CONFIRM » packet. It means that the leader confirms the validity of the « ALARM » packet
CorrVALIDATION	After receipt of the "CONFIRM" packet and when the leader discovers that the « ALARM » packet has been changed, then the leader would send the original alarm data that are stored in its buffer to prevent spread of erroneous messages**.**
ERROR	sent by the leader to a vehicle to stop the spread of the « ALARM » packet
BYE	Sent by a vehicle before departure to inform others vehicles in the group

IV. PETRI NETS MODELING

A. Introduction

Petri nets are essentially for parallel and distributed systems. Functional and dysfunctional modeling makes it possible 'to evaluate the performance of several architectures of complex systems in order to retain which solution would fit with requirements. Functional and dysfunctional modeling is treated thanks to the Petri nets that are well adapted to describe the processes of sequential dynamic control of a complex system. They make it possible to describe the behavior of the system under normal conditions and also in the case of failure of its components.

A net is PN = (P, T, F, W, M_0) where; P = {p_1, p_2, . . . , p_m} is a finite set of places, T = {t_1, t_2, . . . , t_m} is a finite set of transitions, F ⊆ (P × T) ∪ (T × P) is a set of arcs, W is a weight function of arcs, (default = 1), M0 : P → {0, 1, 2, . . . } is initial marking where P ∩ T = ∅ and P ∪ T , ∅. Also; k = P → {1, 2, 3, . . . } ∪ {∞} = partial capacity restriction (default = ∞).

Many researchers have used Colored Petri in many domains. In [15], authors used Colored Petri Nets (CPN) to model the dynamics of a railway system where stations are places, and trains are tokens. Authors, in [16] proposed a model of TCP/IP communication behavior. In [17] authors represent the behavior of the active product and the stream of messages through a wireless network.

The most important benefits that encourage the use of Petri Nets are not only the capability to design and to simulate system but also the capability to give specification at a time formal and graphic of system [15].

The reason why we choose Hierarchical Colored Petri Net is the fact that it is one among many mathematical modeling languages for distributed systems, trust management system in our case.

B. Models of the Trust Management System

Modeling of Active vehicle behavior in interaction with its environment is our main objective. Vehicles interact with each other through messages transmission through vehicular network; we used CPN-Tools software to simplify complex models and segregate it into other sub-models.

1. Model of "Active Vehicle"

The general model of an "Active vehicle" contains its different possible states which are: Announcement, communication and departure. When vehicle is in the road, it begins by sending a HELLO message to search the appropriate GL and its successor. When it receives a response from a GL, it will be a part of this group and it begins communication with the leader and members of this group. Therefore, its trust level will be evaluated and computed by the GL according to its behavior. Before its departure from the road, vehicle should send a BYE message to inform the GL and others vehicles members. The model of an "active vehicle" is illustrated in Fig. 6.

2. Announcement

In this model, the existence of the car on the road near the group is designed by the place "Arrival". This model illustrates the first step should be done by the vehicle to join a group which is the diffusion of a HELLO message. As marked in Fig. 7, after sending the HELLO message, a token HELLO will be put in the "net output msg V1" place in order to illustrate the broadcast of a HELLO message. The reception of an AckHELLO message is illustrated by a token in the "net input msg V1" place, this event validates the transition "Ack". The «Ackbar» transition is validated if there is no acknowledgement token. After, the same step will be repeated once more. This Petri Net guarantees vehicle inscription in the group.

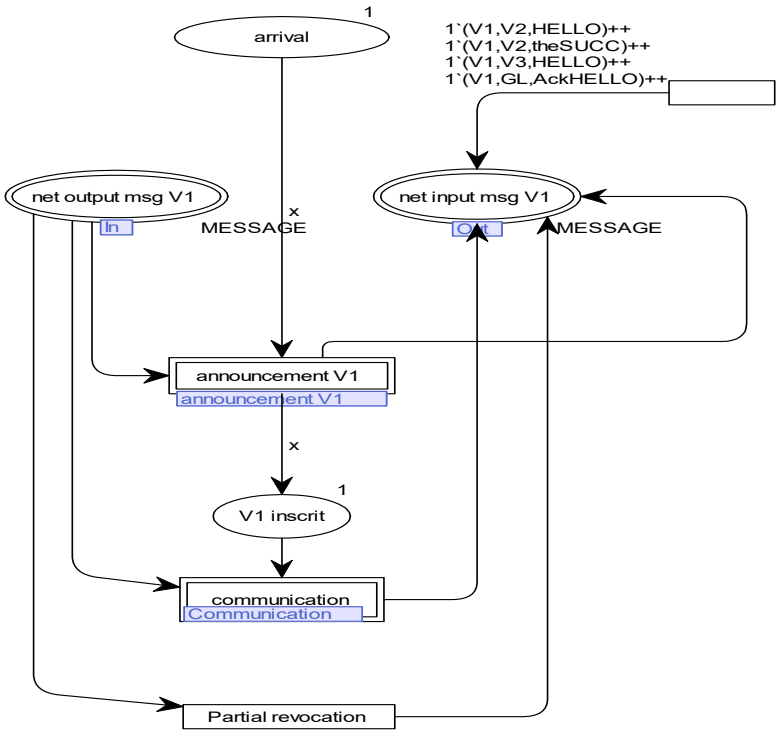

Fig. 6 Model of an Active vehicle

3. Communication

The Petri net of the communication step acts according to different types of messages indicated by Fig. 8; the transition "configuration complete" indicates that first the vehicle saved the leader address of its group and second it sent its owns private/public key to the leader. The transition "message handling" is a sub-model depicted by Fig. 9.

4. Model of "Message Handling"

This transition is depicted in Fig. 9 as a part of the communication model. The majority of messages (HELLO, ALARM, VALIDATION, corrVALIDATION, theSUCC, BYE and ERROR) are handled according to data registered in the knowledge base.

The received message category defines how the knowledge base is used. However, principally, this access is to update the referential trust model for the group.

5. Departure

The departure process is illustrated by Fig. 10. When the vehicle decides to leave, it should announce its departure by broadcasting a BYE message.

V. Conclusion

Our presented trust management system is provided as an application of Active Security in VANET. A new cluster-based protocol for VANET communication was defined. We explained in this protocol, how each vehicle communicates with its neighbors in order to be able to decide about: on the one hand the trust level of other vehicles, and thereafter to believe or not on their warning messages on the other.

We modeled and verified this protocol using a hierarchical colored Petri Nets. Sub-models inside this hierarchy are there displaying the evolution of every state of trust management system (announcement, communication, and departure).

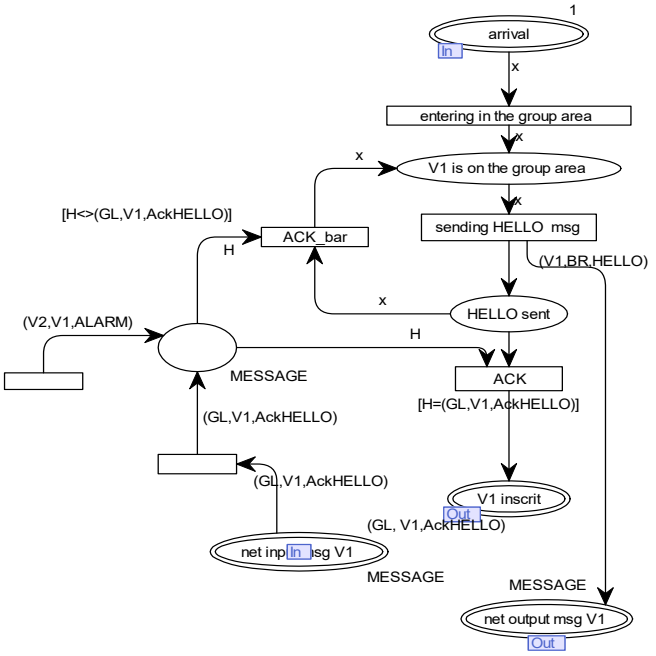

Fig. 7 Announcement Petri Net

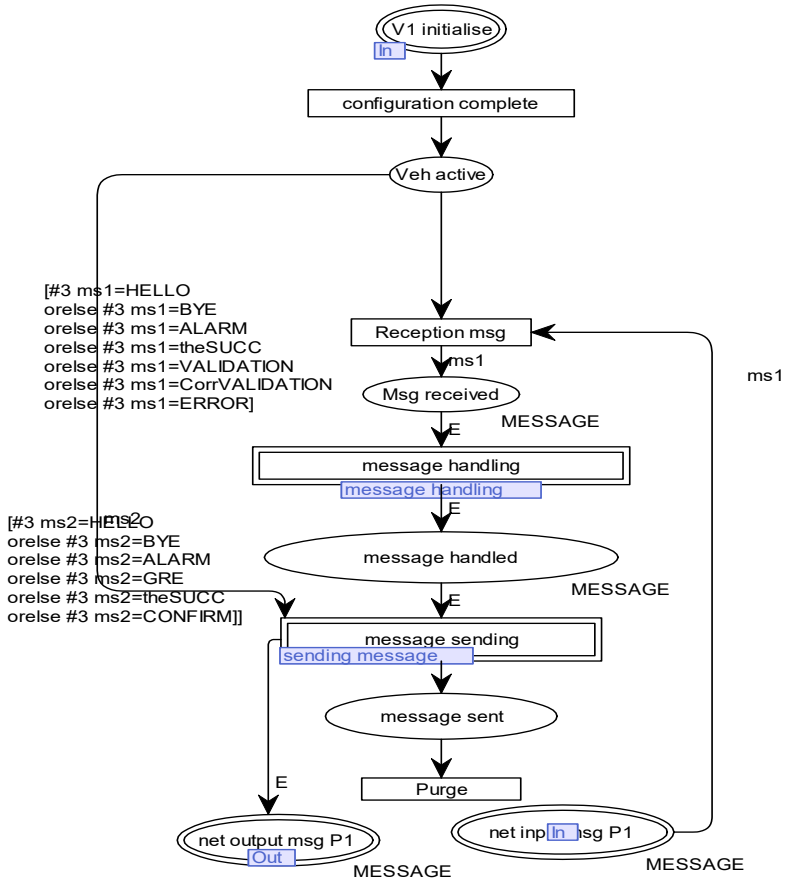

Fig. 8 Communication Petri Net

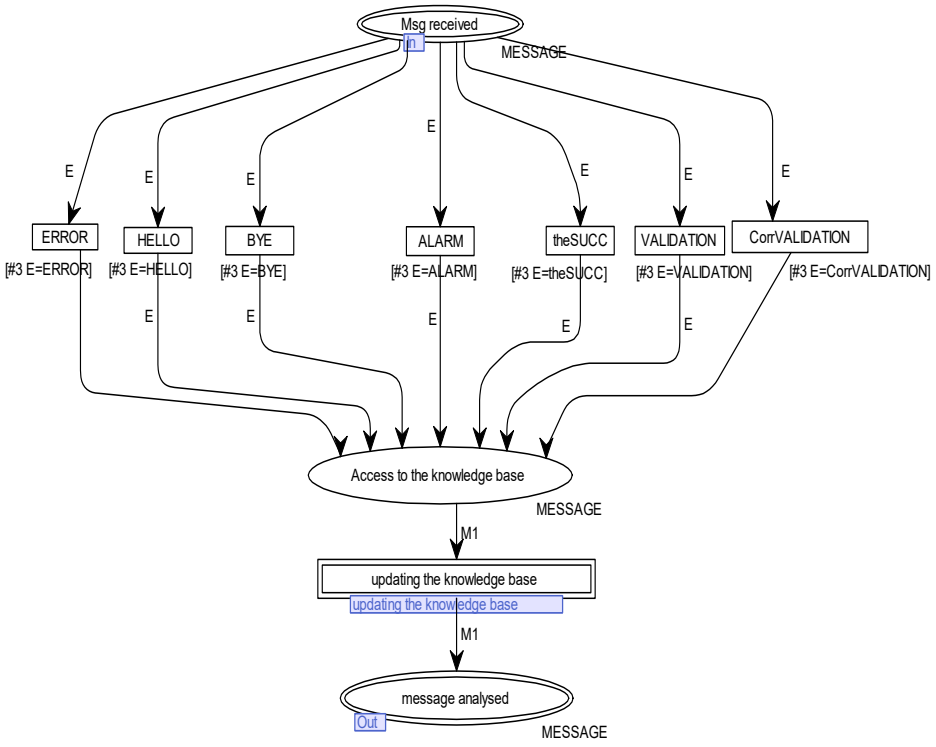

Fig. 9 Message handling Petri Net

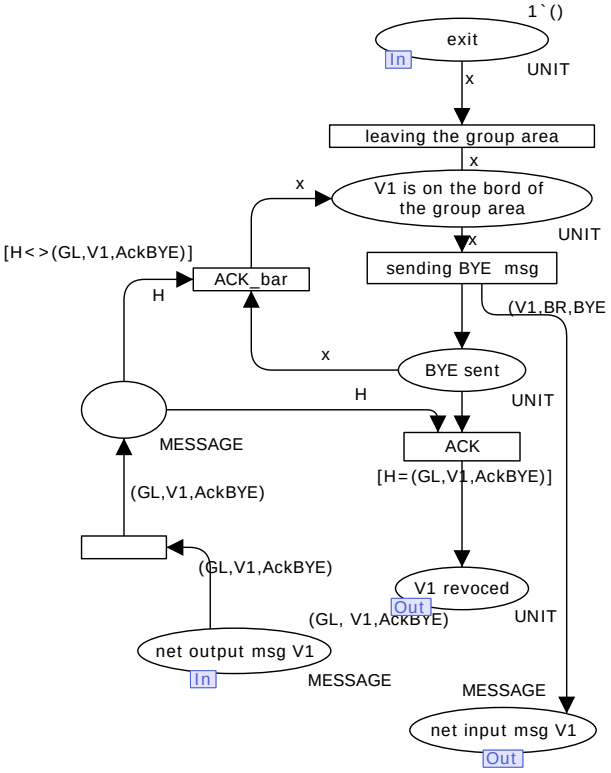

Fig. 10 Departure Petri Net

REFERENCES

[1] V. Manzoni, F. Codecà, S. Savaresi, P. Cravini, “The Implementation of the Safespot Architecture on a Powered Two-Wheeler Vehicle”, 12th IFAC Symposium on Control in Transportation Systems, CTS 2009.

[2] J.-H. Cho, A. Swami, and I.-R. Chen, “A survey on trust management for mobile ad hoc networks,” IEEE Communications Surveys and Tutorials 13(4): 562-583 (2011)

[3] V. Balakrishnan, V. Varadharajan, and U. Tupakula, “Trust management in mobile ad hoc networks,” in Handbook of Wireless Ad hoc and Sensor Networks, Springer, 2009, pp. 473–502.

[4] A.V. Ratzer, L. Wells, H.M. Larsen, M. Laursen, J.F. Qvortrup, M.S. Stissing, M. Westergaard, S. Christensen, and K. Jensen, “Cpn-tools for editing, simulating, and analysing coloured petri net”, LNC, 2679, pp. 450– 462, 2003.

[5] C. Chen, J. Zhang, R. Cohen, P. Ho, A Trust-based Message Propagation and Evaluation Framework in VANETs, In Proc. of the 4th IFIP International Conference on Trust Management (IFIPTM2010), pp.103-110, 2010.

[6] M. M. Elsalih Abdelsalam Mahmoud, S. Shen, Secure Cooperation Incentive Scheme with Limited Use of Public Key Cryptography for Multi-hop Wireless Network, Proceedings of GLOBECOM'2010, Miami Florida, USA, 6-10 Déc. 2010, pp.1-5

[7] Raya, M., Papadimitratos, P., Gligory, V.D., Hubaux, J.P.: On data-centric trust establishment in ephemeral ad hoc networks. In: Proceedings of the IEEE Conference on Computer Communications. (2008) pp. 1238–1246

[8] D. Huang, Z. Zhou, X. Hong et M. Gerla, Establishing Email-based Social Network Trust for Vehicular Networks, IEEE Consumer Communications and Networking Conference (CCNC 2010), Jan 9 – 12, Las Vegas, Nevada 2010

[9] I. A. Soomro, H.B. Hasbullah, and J.lb.Ab Manan,"User requirements model for vehicular ad hoc network applications," *International Symposium on Information Technology 2010 (ITSim 2010),* Malaysia.

[10] P. Caballero-Gil, J. Molina-Gil, and C. Caballero-Gil, "Data aggregation based on fuzzy logic for VANETs," in Proc. of International Conference on Complex, Intelligent, and Software Intensive (CISIS), pp.33-40, 2011.

[11] T. Gazdar, A. Belghith, and A. BenSlimane, "*A Cluster Based Secure Architecture for Vehicular Ad Hoc Networks*," *The 8th ACS/IEEE*

International Conference ACS/IEEE AICCSA'10, Hammamet, Tunisia, May 16-19, 2010 N.

[12] (Bajic, 2009) Eddy Bajic, "A Service-Based Methodology for RFID-Smart Objects Interactions in Supply Chain", International Journal of Multimedia and Ubiquitous Engineering, Vol. 4, No. 3, pp. 37-54, 2009.

[13] (McFarlane, 2003) D. McFarlane, "Product Identity and Its Impact on Discrete Event Observability", European Control Conference ECC 2003, Cambridge, Septembre 2003.

[14] J. Grover, N. K. Prajapati, V. Laxmi, M. S. Gaur, "Machine Learning Approach for Multiple Misbehavior Detection in VANET", First International Conference on Advances in Computing and Communications (ACC-2011), July. 22-24, Kochi Kerala, India, pp. 644-653, 2011.

[15] A. Giua, M.P. Fanti, and C. Seatzu, "Monitor design for colored Petri nets: an application to deadlock prevention in railway networks," Control Engineering Practice, Vol. 14, No. 10, pp. 1231-1247, October 2006.

[16] M. Bitam, "Modélisation et étude de comportement d'une ligne de communication TCP/IP, " 2005, Université Josef Fourier - Grenoble 1, juin, 2005.

[17] B. Brahimi, C. Aubrun, and E. Rondeau, "Modelling and simulation of scheduling policies implemented in Ethernet switch by using colored petri nets," 11th IEEE International Conference on Emerging Technologies and Factory Automation, Czech Republic, 2006.