International Journal of Informatics and Communication Technology (IJ-ICT)
Vol.2, No.2, July 2013, pp. 71~78
ISSN: 2252-8776

A Trust Management System Through Ambient Communication for VANET

Amel LTIFI*, Ahmed ZOUINKHI, Mohamed Salim BOUHLEL***
* Research Unit: Sciences and Technologies of Image
and Telecommunications
Higher Institute of Biotechnology of Sfax-Tunisia
** Research Unit: Modeling, Analysis
and Control Systems
National Engineering school of Gabes-Tunisia

Article Info

Article history:

Received Apr 10th, 2013
Revised June 18th, 2013
Accepted June 30th, 2013

Keyword:

Ambient communication
Security
Trust management system
UML state diagram
VANET

ABSTRACT

In a VANET, the network topology is constantly changing. In fact, it requires distributed self-organizing security systems. In this article, we propose a distributed self-organizing trust management system for vehicular ad-hoc networks (VANETs), given the disastrous consequences of acting on false information sent by the malicious peers in this context. Our application can verify the correctness of alert messages sent by other vehicles about road accident. We opted to apply ambient communication technology to provide a self-organized network. We introduce the concept of “ambient intelligent vehicle” that consists in integrating ambient intelligence features in VANET. Vehicles are considered as intelligent agents that communicate in an ambient environment. Such vehicles are able to control and to detect false warning based on trust management system depicted in this article. Vehicles are arranged into clusters in order to facilitate communication and to reduce overhead. We model how vehicle operate using UML state diagram.

Copyright @ 2013 Institute of Advanced Engineering and Science.
All rights reserved.

Corresponding Author:

Amel LTIFI,
Research Unit: Sciences and Technologies of Image and Telecommunications
Higher Institute of Biotechnology of Sfax-Tunisia
Email: altifi@gmail.com

1. INTRODUCTION

The potential of VANET applications is immense, considering the large amount of vehicles on the road. However, most of the VANET applications such as safety messages and hazard warning have stringent time requirements and malfunctioning systems and malicious attackers can cause loss of life and injury of due to accidents [1]. It is therefore, imperative to develop a strong security system for VANET.

To achieve this, the vehicles act as sensors and exchange warnings or information (like current speed or location) that enables the drivers to react early to abnormal and potentially dangerous situations like accidents, traffic jams or glaze.

Highly dynamic environments such as VANETs need an adapted form of trust establishment. Decisions regarding trust to other nodes must be made autonomously because no online connection to a security infrastructure is possible and must be based on partial information that is collected from unknown nodes during only a short period of time.

Therefore self organizing trust establishment [2] is needed. Each vehicle will play the certification authority in order to decide about neighbor’s confidence levels. However, as this information is not relevant for all vehicles, ambient communication is considered to be vital for more intelligent inter-vehicular communication.

The problem of road traffic safety is addressed in [3] by integrating the vehicles and road infrastructure with the inexpensive wireless sensor networks (WSNs).

Spurious exchange of alerts in VANET is discussed in [4]. In this paper, an algorithm of detecting false alert messages is depected. This algorithm is based on series of parameters to make a decision about the validity of alert messages.

Reference [8] used Context-aware communication that is considered to be vital for more intelligent inter-vehicular communication.

A multi-faceted trust model of use is anticipated in [5] for the application of ad-hoc vehicular networks (VANETs).

Our proposal integrated artificial intelligence and ambient intelligence concepts in vehicular communication in order to design a decentralized trust management system that responds to road security requirements. Vehicles are considered more intelligent to detect dangerous cases through ambient communication and to decide false/true warning messages received from others vehicles by setup security rules-based system.

For engineers and researchers, it is greatly necessary and important to modeling ambient communication before they start designing them for such applications [6]. For this purpose we used the UML state diagram to model different steps of ambient intelligent vehicle life cycle in a vehicular network taking into account our trust management model described in this article.

Our paper is organized as follows: after an introduction and scientific survey of the research domain, the second part introduces the Ambient Intelligence technology and discusses the possibility of its integration in VANET. The third part explains the proposed ambient intelligent vehicle model. The fourth and the fifth describe the two main components of our proposal: the trust management model and the knowledge base. The sixth part deals with modeling the behavior of the ambient intelligent vehicle with UML state diagram. Future research developments are discussed in a conclusion.

2. AMBIENT INTELLIGENT VEHICLE

Ambient Intelligence (AmI) [7][8][9] is growing fast as a multidisciplinary approach which can allow many areas of research to have a significant beneficial influence into our society. An ambient system is a ubiquitous environment that establishes a mechanism to provide the users with all the functionality of the devices and local/distributed software applications in a flexible, integrated and almost transparent way for the end-user [10].

The concept of ambient intelligent vehicle consists in empowering a vehicle with the capacities of communicating, informing, acquiring, deciding and reacting to the disturbances of its environment. These capabilities permit to the vehicle to affect, to cooperate, to transform the behavior of its environment. Therefore, the vehicle is an intelligent actor and proactive in its ambient environment with which it interacts by means of wireless communication and its embarked sensors which allow the data entry of its environment.

2.1. States of an ambient intelligent vehicle

To switch to the communication state the vehicle must undergo a strategy to properly enter in the network in order to manage its own active security on the road. From its departure to its arrival, the vehicle passes from a group to another. In each group, it passes through precised states as shown in Figure 1. These states are: Announcement, Communication, Partial revocation, Broken down and finally the Total revocation.

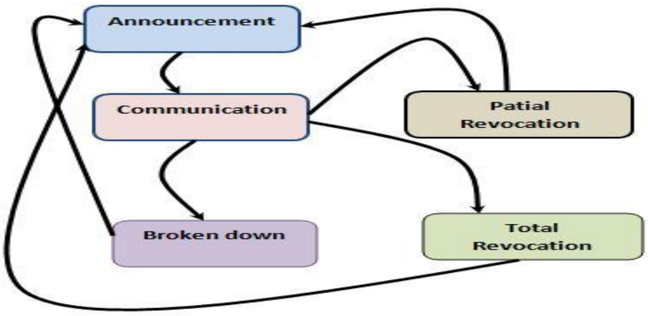

Figure 1. Possible states of ambient intelligent vehicle

2.1.1 Announcement

On the road, the vehicle passes from a group to another through its trajectory. When it comes into a group, the first action that should be done is to announce its presence to other vehicles in the group (its neighbors). The group leader replies this vehicle by an acknowledgement. After, the vehicle will be a member of the group. Others vehicles, receiving this request, should verify the existence of coming vehicle in its trust model. If it doesn't contain the coming vehicle, it should add it.

2.1.2 Communication:

Once the vehicle receives an acknowledgement from the group leader, it begins to communicate with other group members. In our case, the principal aim of this step is to cooperate with others to broadcast ALARM messages with the maximum of confidence. Commonly, there are no data in common between nodes in VANET. In our proposed system, vehicles in the same group share a reference trust model. With this model, each vehicle can verify the confidence level of a message sender. We clarify how to calculate this model later.

2.1.3 Partial revocation:

The vehicle should announce its exit from the group to other members. Each vehicle that detects this event verifies the existence of the leaving vehicle in its trust model. If it exists, the current time is saved into a timestamp. This timestamp is used in the total revocation step. This state is proposed to handle the fact that vehicle can enter many time successively to the same group in the same tour. So, we are not obliged each time to delete the correspondent trust value and to recalculate another time when it returns back. The vehicle should repeat the announcement step once it will reenter to the group.

2.1.4 Total revocation:

A vehicle launches the total revocation procedure periodically for all entries in the trust model. Each vehicle in the model that leaves the group for a long period of time without return must be deleted definitely (we use timestamps for this purpose).

2.1.5 Broken down

We put in consideration the case when a vehicle brakes down. The vehicle should repeat the announcement step once it's repaired.

2.2. Functional model

Our model is depicted in figure 3. It can handle the security of its environment by cooperating with the enclosures (vehicles in the same group, the group leader, RSU).

Each vehicle communicates with others vehicles and 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.

A knowledge base is an artificial intelligent tool. We use this tool to attach to the vehicle the ability to make decision. It processes general information of the vehicle (rate, constructor, position, direction, identifier …) and information concerning trust model (referential/local trust model). It's based on rules that reflect the expected vehicle behavior. The trust management model accesses the knowledge base in order to update trust model and to obtain the effective decision about received message correctness. When a vehicle detects a threat from the sensor information, it sends an ALARM message on broadcast. The receiver vehicle accesses its knowledge base to verify the trust value of the message sender to make the appropriate decision.

In the following, we detail some parts of the functional model such as the trust management system and the knowledge base. Others parts will be described in future papers.

3. TRUST MANAGEMENT MODEL

We distinguished two ways of trust establishment for VANET: one based on a security infrastructure (e.g. a central CA) or be built up dynamically in a self-organizing manner. The former process relies on common, global, trusted and well-known system parameters (e.g. a central CA), which can be used for message authentication. The latter process lacks of this global knowledge and point of control and needs to take advantage of other trust supporting mechanisms.

In our case, we focused to find solutions that are independent from certificated authorities. Vehicles are able to manage security issues by themselves through a set of control messages. We used a cluster-based approach to simplify communications between vehicles. We partition VANET into a number of clusters. In each cluster, exactly one distinguished node the Group Leader (GL) - is responsible for establishing and organizing the cluster. Certificated authority is not centralized but its role is distributed between all the group leaders. Each vehicle in a group A, has only the trust model of A. it's not concerned with vehicles in other

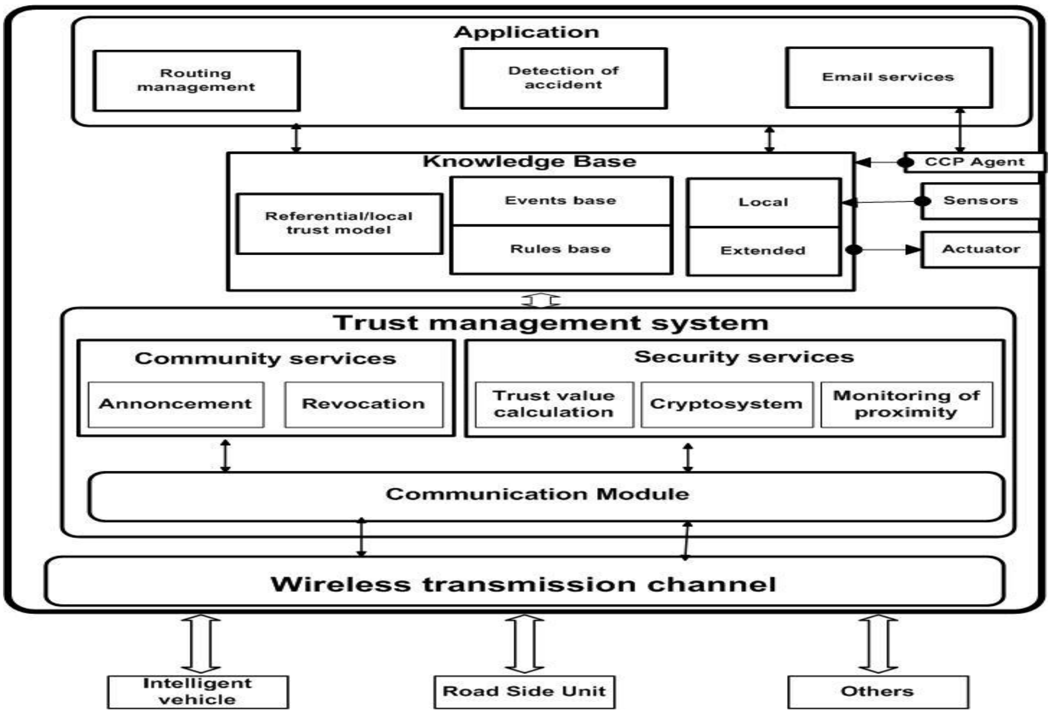

Figure 2. Functional model of the ambient intelligent vehicle

groups in each cluster, trust model is updated periodically and sent to RSU (Road Side Unit). The group leader is the responsible of fixing the value of this period that depends only on the average speed of the group.

We mentioned previously that each vehicle in the group creates a local trust model that contains, for each vehicle in its group, its identifier and a correspondent trust value. This value is initialized for the first time by the confidence control process (CCP). The value is written after in the local trust model. The local trust model is updated periodically by the reference trust model sent by the GL to vehicles in the same cluster. In this article, we are not interested in explaining the CCP operation. This work will be done in the future.

We describe more our trust management model in the sixth section by using UML stat chart model.

3.1. Knowledge Database

As opposite to nodes in others Mobile ad-hoc networks such as WSN, vehicles in VANET are qualified by an important capacity of memorizing. It’s possible to create a knowledge database updated periodically. It’s divided into two parts: Events database and rules database:

3.1.1 Events database:

We find in this database all knowledge necessary for vehicle to decide and to react in possible situations (accident, traffic …). It consists of:

- Vehicle properties:

These properties can be static (ex: idVehicle, constructor …) or dynamic (ex: position, acceleration, direction …). For the first type, it can be obtain from the constructor. And the second type of properties is collected from vehicle sensors.

- Local trust model

In a self organized architecture, vehicle should have some information about trust level of its neighbors in order to create trusted relationship. In [3], authors propose to collect and propagate the views of other nodes in an efficient, secure and scalable dynamically controlled by a diffusion of information to allow evaluation of information in a distributed and collaborative way. Despite the effectiveness of this solution, it has drawback that it depends on the existence of opinions on the confidence generated by the "Analysis Module". Design of this type of module would require much consideration in terms of hardware design [11].

Each vehicle backups a list formed by some couples (Id vehicle, trust value) for all vehicles in the same cluster.

The model of confidence in the vehicle Vi: Mi is shown in table 1.

Table 1. trust model structure within vehicle Vi

Vehicle	Id1	Id2	…	Idi	…	Idn
Confidence value	C1	C2	…	Ci	…	Cn

The establishment of this model is based on the approach of [12].

- Events

All events occurred on the road are recorded in this database. Each recorded event has a number of information as occurred time and position. When a vehicle detects an abnormal event on the road, it should record it and send an ALARM message, containing useful data about the detected event, in broadcast.

3.1.2 Rules database

There are a number of rules that should be known by each vehicle in the network:

R1: if a vehicle A receives from a vehicle B a BYE message, the vehicle A sets the “isConnected” flag of B in the A trust model to false.

R2: if a vehicle A receives from a vehicle B a HELLO message, the vehicle A verifies the existence of a B entry in the A trust model.

R3: if a vehicle A receives from B a HELLO message and if an entry for B exists in the A model, the vehicle A sets the “isConnected” flag of B in the A trust model to true, and it updates the timestamp.

R4: if a vehicle A receives from B a HELLO message and if an entry for B doesn’t exist in the A model, the vehicle A adds an entry for B (IdVehicle, Trust value) to its trust model.

R5: for each entry B in the trust model of a vehicle A, if ((Current Time (CT) – Timestamp of B) >= max delay (Dmax)), A deletes B entry from its model.

R6: if a vehicle A receives from a vehicle B an ALARM message, the vehicle A verifies the B trust value (TV)

R7: if a vehicle A receives from a vehicle B an ALARM message and (TV of B >= threshold), B is trusted and the ALARM message is true.

R8: if a vehicle A receives from a vehicle B an ALARM message and (TV of B < threshold), B is not trusted and the ALARM is false.

4. MODELING BY UML STATE DIAGRAM

As a powerful and object-oriented graphical modeling language, UML has been introduced into the design and development of safety-critical computer systems [13].

UML state chart is an action diagram. State diagrams are used to describe the behavior of a system. It exposes the object life in its communication with others as a sequence of states. Its display the possible states of an object as events occur [14].

In this article, we opted to use UML state chart in the fact that it can describe the dynamic model of our trust management system and interaction between different component objects.

4.1 Announcement state diagram

The presence of the vehicle on the road, in the vicinity of a group, leads the vehicle entering in the network. It announces to other vehicles by sending a HELLO message on broadcast as shown in Figure 3. This message is detected by the Group Leader (GL). After this, a state of waiting for an ACK message from the GL begins, and it passes to a Timeout state. If the ACK is not received within the timeout interval, the HELLO message is retransmitted and the same process will repeat. If it passes many times (N) through the Timeout state (> Nmax), it should be supposed out of the group. The reception of an ACK message means that it’s announced to the group and it can begin to communicate with all vehicles from which it’s received an ACK message.

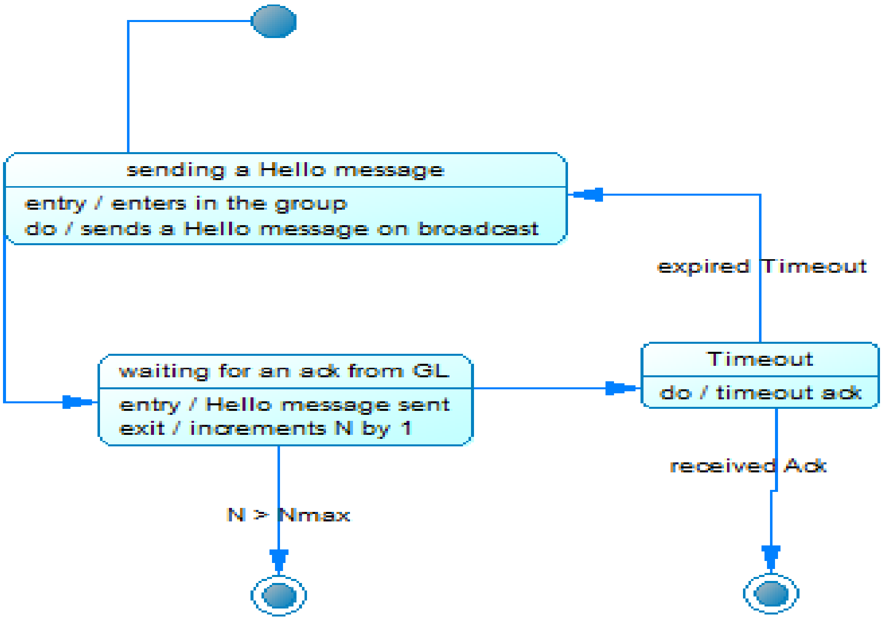
sending a Hello message
entry / enters in the group
do / sends a Hello message on broadcast
expired Timeout
waiting for an ack from GL
entry / Hello message sent
exit / increments N by 1
Timeout
do / timeout ack
received Ack
N > Nmax

Figure 3. Announcement state machine diagram

4.2 Communication state machine diagram

The state machine diagram of communication acts according to different types of messages indicated by the Figure 4; there are three types of messages that can be received in communication phase:

- HELLO message: this message is sent by a new entering vehicle. At the reception, the vehicle Id will be extracted from the message packet. So, it passes to "Id veh searching in the model" state. If the result is "true", the "isConnected" flag is set to 1, and the timestamp (T), attached to the vehicle that sent the HELLO message, is updated; else it starts the CCP agent to calculate trust value and it passes to the "adding (Id, trust value) entry". Finally, it returns to the "communication" state,
- BYE message: this message is sent by a leaving vehicle. As the case of HELLO message, it extracts the vehicle Id from the message packet and it passes to "Id veh searching in the model" state. If true, it positioned in the "Setting isConnected" flag in order to set the flag to 0. Furthermore, it updates a timestamps T attached to the vehicle that sent the BYE message.
- ALARM message: where an unexpected event occurs on the road, the vehicle, observing it, should broadcast an ALARM message. For security purposes, each vehicle, receiving it, should verifying the source trust value in its local trust model if it exists. It enters to "Alarm message treatment" if the trust value exceeds a minimal threshold (TVmin). So, it adds the unexpected event in its knowledge base, and it forwards the message.
- RefTM message: the reference trust model (RefTM) message is sent periodically by the GL to other vehicles in the group. It contains the trust model calculated by the GL based on the average of different trust models calculated by other vehicles and sent to GL that accumulates them in one referential. After receiving this message, vehicle updates its local trust model. When the "updating local trust model" state finishes, it returns to the "Communication" state.

A vehicle, in the "communication" state, should send periodically its local trust model; this task is presented by the "sending local trust model" state.

The state "verifying vehicles thresholds" is presented in the "Communication" diagram in order to manage vehicle automatic revocation from the local trust model. When the delay between current time and T, exceeds a threshold Tmax, it passes to the "deleting (Id, trust value) entry" state. And after, it returns to the "communication" state.

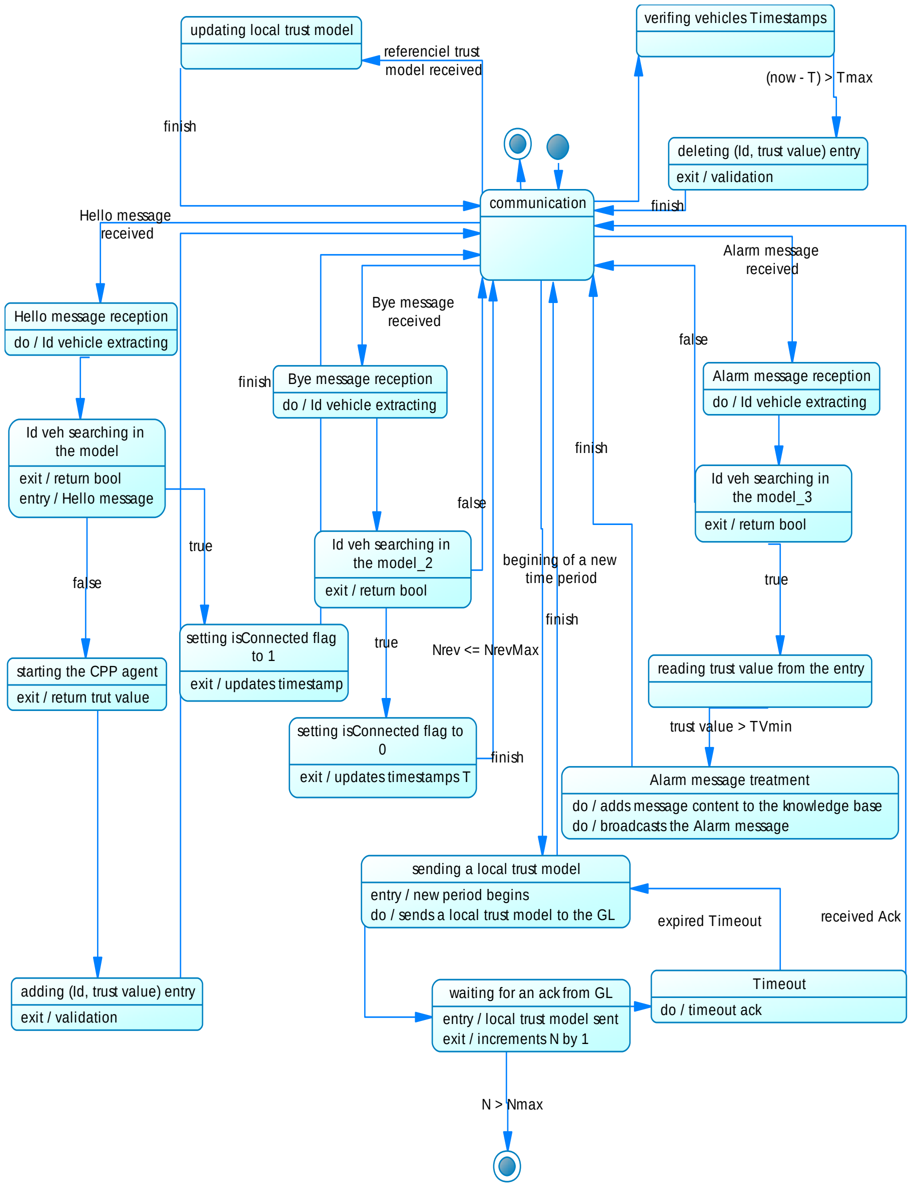
updating local trust model
referenciel trust model received
verifing vehicles Timestamps
(now - T) > Tmax
deleting (Id, trust value) entry
exit / validation
finish
finish
communication
Hello message received
Alarm message received
Hello message reception
do / Id vehicle extracting
Bye message received
false
finish
Bye message reception
do / Id vehicle extracting
Alarm message reception
do / Id vehicle extracting
finish
Id veh searching in the model
exit / return bool
entry / Hello message
Id veh searching in the model_3
exit / return bool
false
true
Id veh searching in the model_2
exit / return bool
begining of a new time period
true
false
finish
setting isConnected flag to 1
exit / updates timestamp
true
Nrev <= NrevMax
reading trust value from the entry
starting the CPP agent
exit / return trut value
setting isConnected flag to 0
exit / updates timestamps T
trust value > TVmin
finish
Alarm message treatment
do / adds message content to the knowledge base
do / broadcasts the Alarm message
sending a local trust model
entry / new period begins
do / sends a local trust model to the GL
expired Timeout
received Ack
adding (Id, trust value) entry
exit / validation
waiting for an ack from GL
entry / local trust model sent
exit / increments N by 1
Timeout
do / timeout ack
N > Nmax

Figure. 4. Communication state diagram

4.3 Revocation state diagram

When a vehicle decides to leave the group, it sends a BYE message on broadcast. After this, it follows the same mechanism described in the announcement diagram in order to be sure that the message is received by at least the GL. The Figure 5 presents the revocation steps.

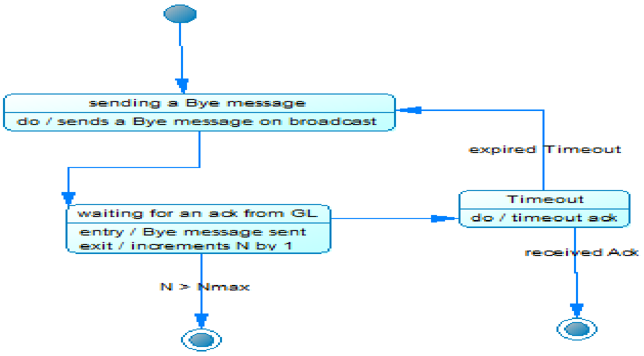

Figure 5. Revocation state diagram

5. CONCLUSION AND FUTURE WORK

To make vehicular networks viable and acceptable to consumers, we need to establish secure protocols that satisfy the stringent requirements of this application space. We integrate the ambient communication technology to VANET, aiming at a solution that is both comprehensive and practical. We identified the necessary elements and functions in the process of trust evaluation. We proposed a complete procedure of establishing trust model that begins by vehicle announcement to the group in order to communicate its identifier with neighbors, and after, begins communication with them, and finishes by vehicle leaving the cluster. We proposed a new way of trust management based on adding new skils to the vehicle to be an ambient intelligent object. This vehicle has a knowledge base used to make appropriate decisions about ALARM messages received. We used the UML state machine diagram for process modeling and validation.

Our goal is to pave the way for future work in implementing and simulating our trust management model to more evaluate the impact of the added value of our approach on the treatment of broadcast ALARM messages between vehicles.

REFERENCES

[1] S. Biswas and J. Misic, “Establishing Trust on VANET Safety Messages”, *In Proceedings of Second International Conference on Ad Hoc Networks (ADHOCNETS 2010)*, August 18-20, Victoria, British Columbia, Canada, 2010.

[2] P. Wex et al., “Trust Issues for Vehicular Ad Hoc Networks”, *67th IEEE Vehicular Technology Conference (VTC2008-Spring),* Marina Bay, Singapore, May 11–14, pp.2800-2804, 2008

[3] H. Qin et al., ”An integrated network of roadside sensors and vehicles for driving safety: Concept, design and experiments”, *in IEEE International Conference on Pervasive Computing and Communications (PerCom),* Mannheim, Germany, March 29 - April 2, pp. 79 –87, 2010.

[4] M. Aamir and S. Mukhi, “Algorithm to Detect Spuriou Communications in Vehicular Ad hoc Networks”, *International Journal of Information & Network Security (IJINS), June, Vol.2, No.3,pp. 239~244, 2013.*

[5] K. Paridel et al., “Teamwork on the road: Efficient collaboration in VANETs with context-based grouping”, *Procedia Computer Science*, Niagara Falls, Canada, September 19-21, vol. 5, pp. 48-57, 2011.

[6] U. Minhas et al., “Intelligent Agents in Mobile Vehicular Ad-Hoc Networks: Leveraging Trust Modeling Based on Direct Experience with Incentives for Honesty,” In Proceedings of the IEEE/WIC/ACM International Conference on Intelligent Agent Technology (IAT’ 2010), Toronto, Canada, September 2010. pp. 243-247, 2010.

[7] A. Nijholt, “Where computers disappear, virtual humans appear”, *Computers & Graphics*, n° 28, pp. 467-476, 2004.

[8] D. I. Tapia and J. M. Corchado, “An Ambient Intelligence Based Multi-Agent System for Alzheimer Health Care”, *International Journal of Architectural Computing (IJAC)*, pp. 15-26, 2009.

[9] J.C. Augusto and D. Cook. “Ambient Intelligence: applications in society and opportunities for AI”, *Proc. of the 20th International Joint Conference on Artificial Intelligence*, Hy-derabad, 6-12 January 2007.

[10] J. C. Augusto, “Ambient Intelligence: The Confluence of Pervasive Computing and Artificial Intelligence”, *in: A. Schuster (Ed.), Intelligent Computing Everywhere*, Springer, pp. 213-234, 2007.

[11] C. Chen et al., “A Trust-based Message Propagation and Evaluation Framework in VANETs”, *In Proc. of the The 4th IFIP International Conference on Trust Management (IFIPTM2010)*, pp.103-110, 2010.

[12] M. M. E. A. Mahmoud and S. Shen, “Secure Cooperation Incentive Scheme with Limited Use of Public Key Cryptography for Multi-hop Wireless Network”, *Proceedings of Global Communications (GLOBECOM'2010),* pp. 1-5, 2010.

[13] X. Hei et al., “Automatic Transformation from UML Statechart to Petri Nets for Safety Analysis and Verification”, *ICQR2MSE-2011*,pp.948- 951, 2011.

[14] K. Ranjini et al., “Design of AdaptiveRoad Traffic Control System through Unified Modeling Language”, *International Journal of Computer Applications (0975 –8887)*, February, Vol. 14, No.7, 2011.

BIOGRAPHY OF AUTHORS

Amel Ltifi is a PhD student at the National Engineering School of Sfax (Tunisia) and a member of Sciences and Technologies of Image and Telecommunications (SETIT) laboratory. She received the National engineering Degree from the National School of Informatic sciences (ENSI), Tunisia in 2003 in computer sciences. She received the Master degree from the Higher School of Informatics and Multimedia of Gabes (ISIMG), Tunisia, in 2010. Her research activities are focused on Distributed Systems, Ambient Intelligence systems and architectures, VANET and Wireless Sensors Network Concepts.

Ahmed Zouinkhi is Associate Professor at the National Engineering School of Gabes (Tunisia) and a member of Modeling, Analysis and Control Systems (MACS) laboratory. He received the Notional engineering Degree from the National Engineering School of Monastir (ENIM), Tunisia in 1997 in industrial computing. He received the DEA degrees and the CESS (certificate high specialized electrical study) from the Higher School of Sciences and Techniques of Tunis (ESSTT), Tunisia, in 2001 and 2003, respectively. He received his PhD degree in 2011 in Automatic Control from the National Engineering School of Gabes (Tunisia) and a PhD degree in Computer Engineering from the Nancy University (France). His research activities are focused on Distributed Systems, Smart Objects theory and applications, Ambient Intelligence systems and architectures, RFID, VANET and Wireless Sensors Network Concepts and Applications in manufacturing and supply chain.

Mohamed-Salim BOUHLEL was born in Sfax (Tunisia) in December 1955. He received the engineering Diploma from the National Engineering School of Sfax (ENIS) in 1981, the DEA in Automatic and Informatic from the National Institute of Applied Sciences of Lyon in 1981, the degree of Doctor Engineer from the National Institute of Applied Sciences of Lyon in 1983. He has received in 1999 the golden medal with the special mention of jury in the first International Meeting of Invention, Innovation and Technology (Dubai). He was the Vice President of the Tunisian Association of the Specialists in Electronics. He is actually the Vice President of the Tunisian Association of the Experts in Imagery and President of the Tunisian Association of the Experts in Information technology and Telecommunication. He is the Editor in Chief of the International Journal of Electronic, Technology of Information and Telecommunication, Chairman of the international conference: Sciences of Electronic, Technologies of Information and Telecommunication: (SETIT 2003, SETIT 2004 ,SETIT 2005, SETIT 2007, SETIT 2009 and SETIT 2012) and member of the program committee of a lot of international conferences. In addition, he is an associate professor at the Department of Image and Information Technology in the Higher National School of Telecommunication ENST-Bretagne (France).