Reconcile Security Considerations For Automated Vehicles

Rakshitha B T[1], Harshini S Babu[2]
[1]Professor, Dept of Computer Science and Engineering
[2]Dept of Computer Science and Engineering
[1, 2] Atria Institute of Technology, Bangalore,Karnataka, India

Abstract- *An Automated vehicle (Self-driving) is an emerging research area. Presently, many industries, research organizations and universities are working on intelligent vehicles. Some researchers are working on security issues of intelligent vehicles (IV). Most of the researchers focus on static security (static security cannot adapt to the changes in the environment). Since the environment of IV is dynamically changing, the approach of static security is not feasible to provide reconcile cyber-security in IV. Reconciling systems evolve in a very uncertain environment and try to fullfill a business objective by sensing the environment, analysing it and taking the best decision according to its requirements. In this paper, we discuss reconcile security requirements engineering to provide cyber-security in IV. To full fill our objective, we use the goal model approach of RE, the Knowledge Acquisition in Automated Specification (KAOS) Model approach, and designed it using Objective tool to find the reconciling requirements. Self-reconciliation in requirement engineering is acquired by five building blocks such as Monitor, Analyse, Plan, Execute and Knowledge i.e. [MAPE-K] loop architecture, which provides the reconciling capabilities to our proposed reconciling requirements for cyber-security in IV.*

Keywords- Cyber Security, Requirement Engineering, MAPE-K, Intelligent Vehicles

I. INTRODUCTION

Connected Vehicles (IV) is the term of the automobiles that have intelligence abilities, which includes computing, measuring, and networking. IV is evolving from simple technology to convergence technologies, where the connected vehicle can take its decision, according to the real-time situation. IV raises new business trends all over the world marketplace through uniting information communication technology (ICT), and automotive that leads the hardware, software and manufacturing industries. The large IT Companies like, Google, Microsoft, Apple, etc. released automotive operating system as-well-as automotive manufacturers constructed environment for making connected vehicles based on the advanced technologies like automatic parking system, lane-keeping system, conflict prevention system, etc. IV can improve traffic efficiency, reduce pollution, and can prohibit car accidents. Intelligent Vehicles (IVs) are capable to take their decisions in different situations such as lane change, distance measurement, communication with nearest vehicles, roadside units, receive and transmit the message and can take proper action on road, adhering to the traffic rules. The IV systems are internally connected through the steering, sensors, ECU's (Electronic Control Units), actuators and are externally connected to Road Side Units (RSU), and other nearby IVs. They rely on seamless data exchange and information flow. The larger the connectivity, the more is the possibility of cyber-attack in IVs [1]. An attacker might exploit vulnerabilities or tamper message, causing effect to multiple systems. The environment of IV is very vulnerable and dynamic in nature, so static security is unable to change the security mechanism and take the right decision at runtime, therefore, dynamic security or reconciling security is required [2]. To, understand and solve the security issues in IV's, this paper presents the reconciling requirements for connected vehicles for current and upcoming automotive technologies
(driverless).

This paper is organized into six sections. Section 2 discuss the reconcile system and security issues and their possible solutions for Intelligent Vehicles. Section 3, propose the reconcile security requirements for Intelligent Vehicles. Section 4 presents the security requirements goal model for the IVs and finally in section 5, we conclude the paper with some remarks on our proposed idea and possible future work for improvement.

II. RECONCILE SYSTEMS AND SECURITY REQUIREMENTS FOR IV

2.1 Reconcile Systems

The reconciling system evolves in a very uncertain environment, of which it is aware. It tries to full fill a business objective by sensing the environment, analysing it and taking the best decision according to its requirements. We can say

that a reconciling system should make well-enough decisions, thus involving a strong notion of a trade-off between the satisfactions of the different requirements. Self –reconcile software can be aware of their architecture and thus reconfigure autonomously at runtime to activate only the required modules for a certain environment state. In this paper, we use the KAOS methodology, and we focus on adoption of countermeasures facing security issues of connected vehicles. "Awareness Requirements for Reconciling Systems [2]" by Souza defines a new type of requirement called Awareness Requirement that can refer to other requirements and their success/failure. In this paper, adaptation is implemented through MAPE (Monitor, Analysis, Plan, and Execute) feedback loop. "Law and Reconciling in Requirements Engineering" [3], Ingolfo and Souza have presented and characterized the significant relationship between law and adaptation in requirements engineering. Here adaptation techniques have been tailored to accommodate legal compliance requirements. As our domain is an autonomous vehicle, the biggest concern is complying with the law. We referred this work to explore how the adaptation can be tuned using certain laws. "Toward goal-oriented development of Reconciling Systems" [4], Morandini et al. define how to model a Reconciling system with agents by modifying a late requirement TROPOS goal model. They define new modelling entities to represent symptoms, stated goals along with pre-and post-conditions to link the recovery actions to a runtime sensing of the internal and external environment. They also show how to directly map the final goal model into an agent implementation platform.

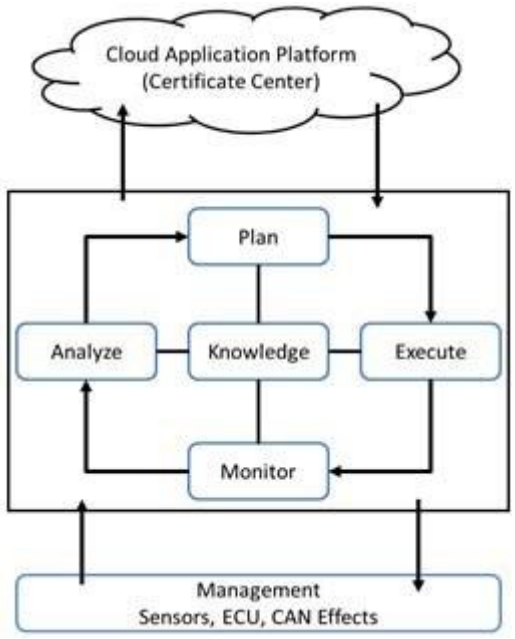

Fig. 1.MAPE-K Reconcile Process Elements

Monitoring, Analysis, Planning, Executing, and Knowledge (MAPE-K) [5] is an activity loop that a Reconciling System should follow to reach adaptation. It consists of four processes and one knowledge base.

We refer to the fig. 1 above and explain each phase briefly in table 1.

Table 1. MAPE-K Description

Activity of MAPE-K	Description
Monitoring (M)	Monitoring self and control the environment: in this phase, the system uses sensors to gather raw information.
Analysing (A)	In the analysing phase, the raw data is understood and it is given semantics.
Plan (P)	Now that the environment is understood, the system reasons over the available knowledge, and selects a best suitable series of actions to be conducted i.e. it creates a plan.
Execute (E)	In this phase, the plan is executed via the actuators (effectors) of the system and the environment is modified. The monitoring activity will detect potential changes, and the system will keep performing the four activities.
Knowledge (K)	Knowledge is the knowledge base of the system. Every planning activity has founded on the awareness of the environment. We could better use term "belief" as the system understands something from the environment and considers it faithful to perform reasoning tasks (it believes it is true, but maybe it is not "really" true)
Remark: We have used MAPE-K activity loop with the KAOS model.	

2.2. Security Challenges and possible Solutions for Intelligent Vehicles

The reconciling requirements for changing security mechanism at run-time is not an easy problem in seamless communication in a network. The intelligent vehicles have so many security challenges. In fig. 3 we illustrate some important and basic security drawbacks of intelligent vehicles during their communication [6].

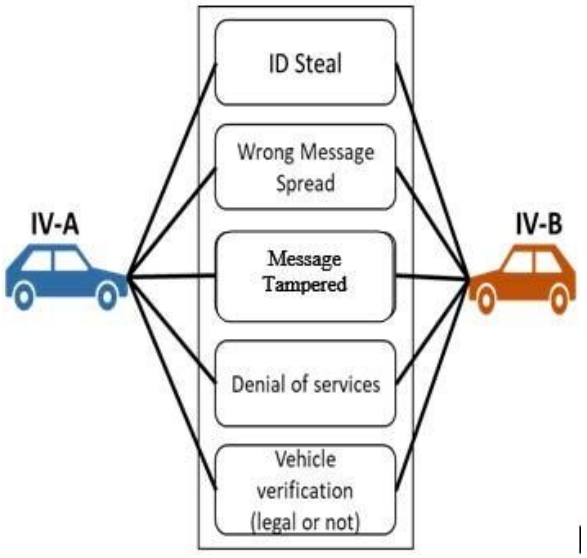

Fig. 2.Vehicles Communication Problems

Until the time, many researchers have proposed multiple security mechanisms for IV communication but almost all of them have primarily worked on providing static security mechanisms using requirements engineering, but in this paper, we discuss dynamic security features or reconciling requirements [8]. IV security need to improve the following security mechanism during the communication such as, Message Authentication, Integrity, Message Non-Repudiation, Access Control, Message Confidentiality, Privacy, and Liability Identification [9]. These security mechanisms are very important for vehicles communication. We have illustrated the possible security solutions of security issues in vehicle communication in fig.3.

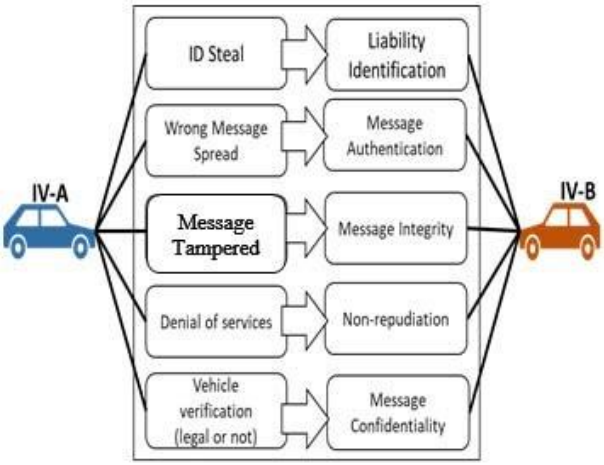

Fig. 3.Possible solutions for secure vehicle communication

We propose reconciling security requirements for connected vehicles, which can protect the complete communication process with the help of the legal authorized connected vehicles.

3. RECONCILE SECURITY REQUIREMENTS FOR INTELLIGENT VEHICLES

The environment of the system i.e. the connected vehicle is very unpredictable, changeable and vulnerable. As in the environment, there will be humans driving the car, pedestrian moving on the pathway, one IV communicating to other IV through V to V communication, so human's nature could be unpredictable, and they can make some mistakes, and there can be some malicious users who can intentionally create threats. Therefore, the system should sense and analysethe system all the time and accordingly abstract the relevant information and plan. For example, if a hacker A in a vehicle sends tampered traffic message to other connected vehicle IV-B then IV-B can suspect the hacker IV-A by its identity, verify the message from the Certificate Centre (CC), and alert other drivers in the range of the unexpected event. The system's main requirement is "Security," therefore; the other IVs can block the hacker IV for further communication.

3.1 Methodology

Our proposed model uses MAPE-K method to provide secure communication in IV environment at runtime. In our proposed reconciling security mechanism, we consider security challenges in IV and how to find a reconciling solution for each of the security challenge such as liability identification, message authentication, integrity, non-repudiation, and privacy. We illustrate our approach by explaining an example covering all the security problems.

For Example, Intelligent Vehicle (A) receives a message from Intelligent Vehicle (B). IV (A) can directly communicate using reconciling (MAPE-K) security model. However, this security model gives effective results based on following rules. We describe the connectivity between security requirements and MAPE-K process below and shown in figure 4.

Monitor: In the Monitor phase, the sender's (IV-B) information (identity) is checked to find if it is a legal vehicle (registered with the Certificate centre) or not. IV-A can directly check IV-B's certificate in its own maintained database (containing log information of all communicated IV's) or can verify from the Certificate Centre, if it does not find in its database.

Analysis: After the authentication of the sender (IV-B) in the Monitor phase, the mechanism will now analyse the authentication of the message received. In the Analyse phase, it is analysed whether the message received from the

originator is authentic message and is not intercepted in between.

Plan: After message authentication in the Analysis phase is done, the receiver IV-A plans for a secure communication with the sender IV-B using cryptographic protocols, maintaining privacy of the receiver.

Execution: After the receiver IV-A plans for a secure communication then it will communicate with the sender IV-B. The message will be sent according to the plan, and the sender or receiver cannot deny of any message exchange between them. These phases will be adhered based on the predefined rules stored in the knowledge base.

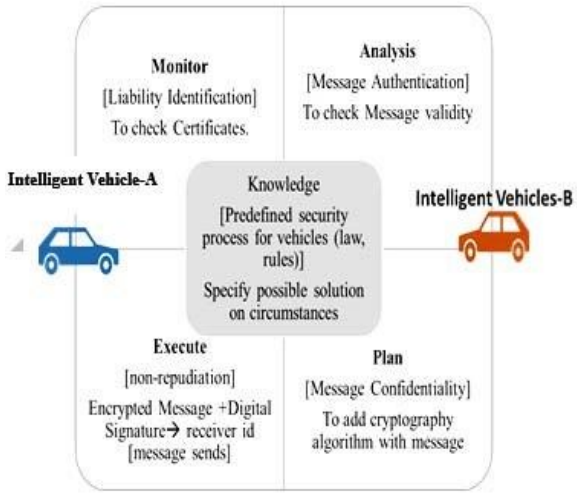

Fig. 4.Reconciling Security mechanism for Intelligent Vehicles

In addition to sensors, our system gathers data on battery status, engine status, GPS, and others. Data analysis means understanding the vehicle's context through various sensors. The vehicle also includes a law subsystem, which is responsible for reasoning with knowledge of security law, traffic law and legislation for autonomous vehicles. Our scope is a system that uses information from sensors and data centre. We have used Objective tool [7] for defining reconciling requirements for connected vehicles security perspective with the help of KAOS model [8].

3.3 Reconcile Security Requirements Functionalities with MAPE-K

In this section, we discuss how existing static security mechanism can be converted to reconciling security and solve the security issues in real time. During communication, IVs can secure itself from other vehicles'/Road Side Units, using the MAPE-K reconciling model. We define the reconciling security process based on the functionalities of vehicle communication.

In table 2, we describe the basic security functionalities for the vehicle communications for connected vehicles. It shows the pre-and post-conditions of the security functions.

Table 2. Security functionalities for Vehicle Communication

Function	Name	Pre-Condition	Post–Condition
F 1.	Liability Identification	Every vehicle must have a certificate issued from Certificate centre.	Verify legal certificate with the centre.
F 2	Privacy	Information shall be encrypted	Vehicles must Support high-performance cryptographic algorithms.
F 3	Message Authentication	Message Received must be authentic.	Message receiver verifies suspicious message with certificate centre.
F 4	Message Integrity	Message sender's Information shall not be tampered.	Check message is tampered or not with security algorithm.
F 5	Message Non-repudiation	Message Sender entity must be verified by CC.	The receiver must verifysender entity with CC.
F 6	Message Confidentiality	Message must be encrypted.	Communication entities should verify each other.

Our proposed mechanism has two actors, who are responsible for providing reconciling, secure communication among connected vehicles and Road Side Units in real time. The first actor is self-diagnosis agent, which has predefined actions for taking decision for secure communication. The self-diagnosis agent is enabled in connected vehicles for secure communication. Second is certificate centre, which is responsible for issuing a certificate, monitoring the communication process, providing the specific information to IV such as authentication, tampered message or liability of any IV for communication and spread message during an emergency. We show the responsibilities of the self-diagnosis agent in figure 5 and certificate centreagent in figure 6 respectively.

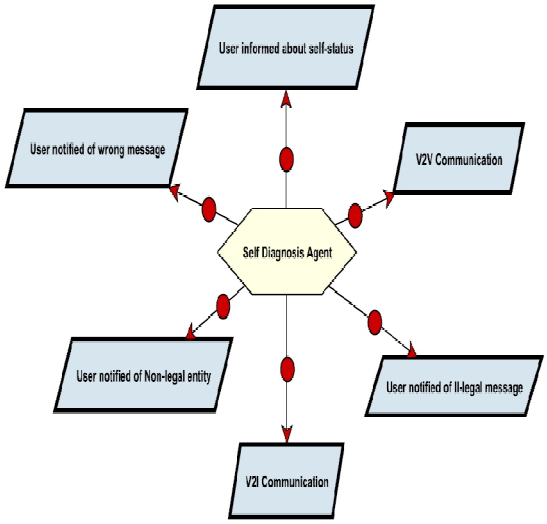

Fig. 5.Self-Diagnosis Agent Responsibility

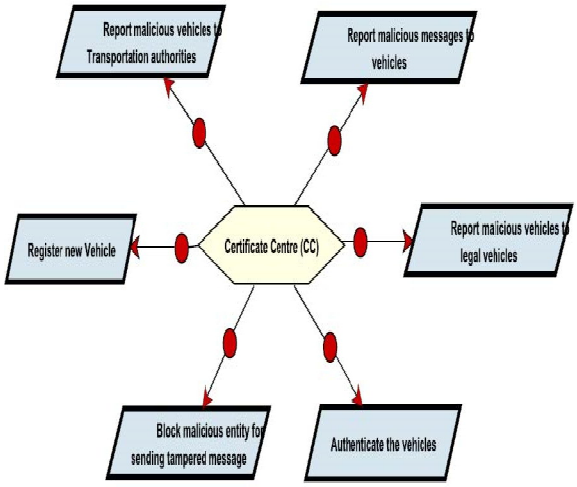

Fig. 6.Certificate Centre Agent Responsibility

Monitoring Function: In this step, the receiver IV monitors the message sender IV. For this, it needs to check liability Identification security function. Liability Identification shall monitor whether the source of the message is verified source or not, and the members for communication are legal or not. IV can also monitor previous track record of the sender in its database (if previous communication exists with the IV) or can ask liability verification from RSUs. Locations, where there is no Certificate authority to authenticate the IV's, communications will be based on secure protocols using public and private key and authenticated by digital signature.

Analysis Function: The reconciling security mechanism second step is to analysemessage reliability. The receiver IV checks the message authentication and integrity of the received message from the sender IV. The integrity of information can be authenticated by verifying the information from the information broadcasted by multiple IVs at the same time. This process is done to protect any misleading or wrong information spread. After analysis of the received message, reconciling security mechanism goes for next step, which is Plan.

Plan Function: In this step, receiver plans for a secure response to the sender. For message securing, it will make sure that only receiver can reply to its message. For this, it will use message confidentially security function. To make a confidential message, it will use public key cryptographic algorithms to encrypt and decrypt the messages.

Execution Function: The final step of the reconciling mechanism is execution. After plan phase, IV can transmit its reply with a digital signature. We use digital signature for non-repudiation security functionality. Both sender and receiver shall append a signed digital signature for sending and receiving data. Digital signature is used to remove deniability action between them.

Knowledge Function: All these reconciling mechanisms will work based on the predefined communication rules and situations for the secure mechanism process stored in the database called the knowledge base. Self-Diagnosis mechanism will infer the knowledge base for the right action.

IV. GOAL MODEL FOR INTELLIGENT VEHICLES

The goal model starts from the main goal of providing ‘security in the IVs.' The goal model is based on KAOS model in which we decompose the main goal into sub-goals and then refine the sub-goals until we reach explicit, unambiguous requirements of our system. The bold parallelogram represents the requirement or the action to be taken to achieve secure communication among IVs. The main goal i.e. security in IVs is obtained by decomposing it into sub-goals such as Liability Identification, Message Authentication, Message Integrity, Message Non-Repudiation, Message Confidentiality and Privacy. Each of these sub-goals (we refer them as security functionalities in the paper) are decomposed further until we get the requirement of our system. While decomposing each security capability, we encounter some obstacle represented by an orange parallelogram and a counter action (requirement) is addressed to overcome the obstacle. When we get the requirements at the leaf nodes or at an early stage, we hand over the obligation to the agents (which have responsibilities) of the system such as Self-diagnosis agent and the Certificate centre agent which act in accordance with the requirement. Fig7 shows the notation of KAOS, which we used to develop the complete reconcile security model in fig.8.

V. CONCLUSION

This article has proposed reconciling security requirements for IV to understand the problem domain for business needs. We need to understand the customer's needs as precisely as we can. We also elicited what s/he does not say, but it might be substantial and we must eventually provide a secure communication solution, which is unambiguous, complete, arguable and reasonable. For this, we have proposed a reconciling security mechanism for IVs. We have used Objective tool, which uses the KAOS goal model. Our complete reconciling security requirement is based on Monitor, Analysis, Plan, Execute and Knowledge. Any suspicious communication vehicle first monitors the situation, then analyse then plan, and then execute or take decision according to the predefined knowledge. Our proposed reconciling security requirements can solve security issues in the runtime scenario. For future work, we aim to provide safe and secure infrastructure for Connected Vehicles.

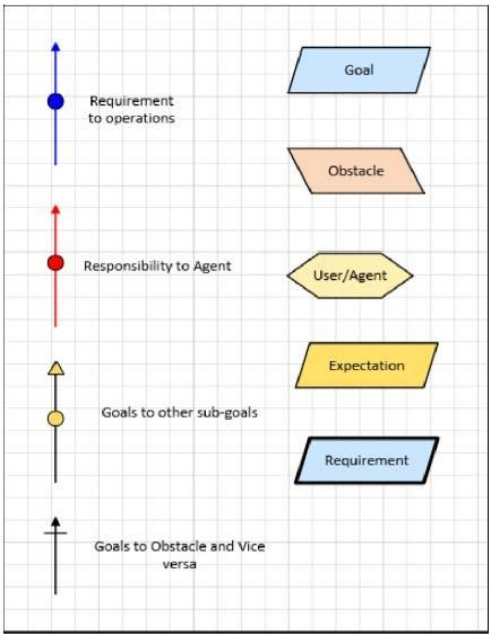

Fig. 7.KAOS Notation

VI. ACKNOWLEGEMENT

This work was supported by Institute for Information & communications Technology Promotion(IITP) grant funded by the Korea government(MSIT)

(No.2017-0-00560, Development of a Blockchain based Secure Decentralized Trust network for intelligent vehicles).

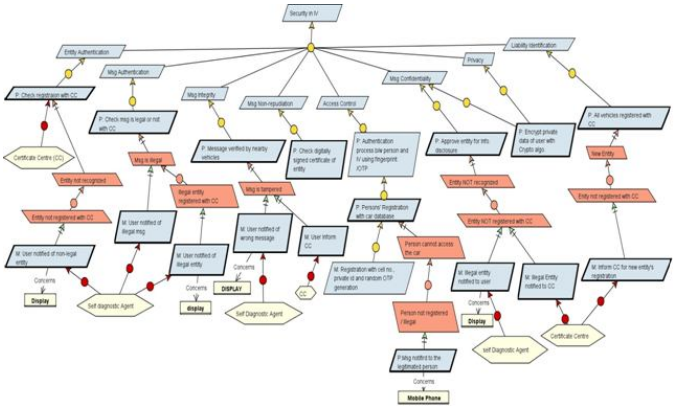

Fig. 8.Security Requirements Goal Model for IV.

REFERENCES

[1] Matthias Weber and Joachim Weisbrod, "Requirements Engineering in Automotive Development: Experiences and Challenges," IEEE Software, IEEE Computer Society, pp.16-24, 2009.

[2] Silva Souza, Vítor E., Alexei Lapouchnian, William N. Robinson, and John Mylopoulos. "Awareness requirements for reconciling systems," The 6th International Symposium on software engineering for adaptive and self-managing systems, p.60-69, 2011.

[3] Ingolfo, Silvia, and Vítor E. Silva Souza, "Law and adaptively in requirements engineering," The 8th International Symposium on Software Engineering for Adaptive and Self-Managing Systems, p. 163-168, 2013. doi: http://dl.acm.org/citation.cfm?id=2487362

[4] Morandini, Mirko, Loris Penserini, and Anna Perini, "Towards the goal-oriented development of adaptive systems," The 2008 international workshop on Software engineering for adaptive and self-managing systems p. 9-16, 2008. doi:10.1145/1370018.1370021

[5] This tutorial is the official tutorial made by respectIT, the team from the University of Louvain who maintain and develop the KAOS methodologynowadays. http://www.objectiver.com/fileadmin/download/documents/KaosTutorial.pdf

[6] The tool has drawn up by respectIT, a spinout company from the University of Louvain.

[7] http://www.objectiver.com/index.php?id=4

[8] Mohamed Amin, Zaid Tariq, "Securing the car: How Intrusive Manufacturer-Supplier Approaches Can Reduce Cybersecurity Vulnerabilities," Technology Innovation Management Review, p. 21-25, 2015.