We are IntechOpen,
the world's leading publisher of
Open Access books
Built by scientists, for scientists

4,800
Open access books available

122,000
International authors and editors

135M
Downloads

Our authors are among the

154
Countries delivered to

TOP 1%
most cited scientists

12.2%
Contributors from top 500 universities

BOOK CITATION INDEX
CLARIVATE ANALYTICS
INDEXED

WEB OF SCIENCE™

Selection of our books indexed in the Book Citation Index
in Web of Science™ Core Collection (BKCI)

Interested in publishing with us?
Contact book.department@intechopen.com

Numbers displayed above are based on latest data collected.
For more information visit www.intechopen.com

Beyond Identification: Representing Real World Objects and Actors in Radio Frequency Identification

Krishan Sabaragamu Koralalage, Noriaki Yoshiura, and Takaomi Shigehara
Saitama University
Japan

1. Introduction

Due to the improvement of technology, the way human beings do things are changing day by day. Radio frequency (RF) identification has been acting a big role in recent technological developments. Although there are three types of Radio Frequency IDentification tags (RFID): active, passive and semi-passive, almost all the tags are being used to store only a unique number in addition to the processing information. For a particular application, all the relevant details of the tag have to be taken from the database system. There are several applications which are not viable under this infrastructure. Intelligent Transportation System (ITS) including railway, is one of them. ITSs can be improved using the characteristics and the behaviours of RF tagging systems. However currently available RF tags are not suitable for such applications, mainly as it does not provide role base access control mechanisms and have no ability to stand alone to enable offline communications. Thus there is a necessity to look into this area of research.

After extensive survey and hardships, a novel RF tag architecture called Object Tag (OTag), to represent the real world objects and actors in RF tags were designed with common communicational protocols. The OTag can provide access control mechanism and have abilities of being stand alone, being interoperable, being self-describing, and also being plug-and-playable. Then we defined common communicational protocols to communicate with reader/ writer and tag. Finally we derived possible applications using our architecture. Our architecture can be used in two ways: one is just as a real world object and second is as an actor or agent. Agent is a combination of a reader/ writer, processing unit and OTag. These three units together compose the actions of an agent that can work according to predefined instructions. Following sections describes how proposed technology work in real world by taking ITS as an example by deriving novel applications to support safe, reliable, comfortable, and productive social life in eco-friendly manner.

1.1 Motivation

The first motivation to develop novel architecture for ITSs was raised because there is no proper system to support emergency vehicles such as ambulance, fire brigade, and rescue vehicles which work on saving vital seconds of invaluable human life(Al-Khateeb et al., 2008). The main reason for that is the lack of proper communication among three actors:

users, vehicles, and infrastructure including vehicle to vehicle in ITSs. Here the passengers and the pedestrians are referred as users. Therefore there is a necessity to create a common platform to communicate among three actors to solve the above issue.

If it is possible to develop such a common platform, prioritizing emergency vehicles, changing traffic lights adaptively, prior informing of phase changing on traffic lights, understanding vehicle movements, detecting collisions before entering to intersections or merging points, enforcing rules and regulations such as speed enforcements, assisting elderly driving, understanding accidents, managing traffic congestions, vehicle registrations and ownership transference, can be automated to the maximum possible level (Lee et al., 2008).

RFID Technology can be considered as one of the best candidate technologies to develop a common platform to communicate among users, vehicles and infrastructure including vehicle to vehicle. Although there are a few applications in ITS like electronic toll collection (ETC) using RFID tags, those tags cannot be used for this purpose because they are unable to provide interoperability, ability to be stand alone, ability to be self describing, ability to be plug and play with role base accessing mechanisms.

Unlike current ETC systems, if such a platform is developed, there will be many readers in different systems reading the tag information in a given time. Each reader should be allowed to access only the authorized data depending on their rights. But this cannot be achieved using the existing or the previously proposed tag architectures. Instead it is necessary to have several tags to allow being read by different systems. Additionally, attaching several tags for different systems to work on vehicles are a burden for users as well as for managing authorities. Therefore existing tags cannot be used to develop a common communication platform. On the other hand, such a platform can only be built with one tag, if the access control to the stored data can be provided depending on the roles or the access privileges. Then, it will be possible to subscribe many services or allow different reader to read authorized portions of the tag and thereby the cost and management can be improved. Therefore, using one tag with above features and secure communication protocols, will lead to innovate novel era of ITSs enabling ultimate infrastructure support for autonomous driving in future. Nevertheless, there are no major weaknesses of current applications of ITS.

1.2 Goal and objectives

The goal of our research is to develop a novel RF Tag that can represent real world object and their attributes and behaviours. Then create autonomous agents with those objects to improve existing navigation systems and traffic management systems, enhance electronic fee collection system, assist safe driving, increase efficiency in infrastructure management and commercial vehicle operations and support public transport and emergency vehicle operations by enabling extensive communication among the user(pedestrian/ passenger), vehicle and infrastructure of ITS as shown in figure 1.

To achieve above mentioned goals we set following three main objectives: first is to design a novel radio frequency tag architecture with the ability of being intelligent, stand alone, self-describing, and plug & playable while enabling role based access controlling mechanisms to improve the ITSs. Second is to define security and privacy enhanced application layer protocols to communicate among user, vehicle and infrastructure including vehicle to vehicle. The third objective is to derive electronic vehicle registration and ownership transferring mechanism to improve the flow of tagged vehicles throughout their lifecycle.
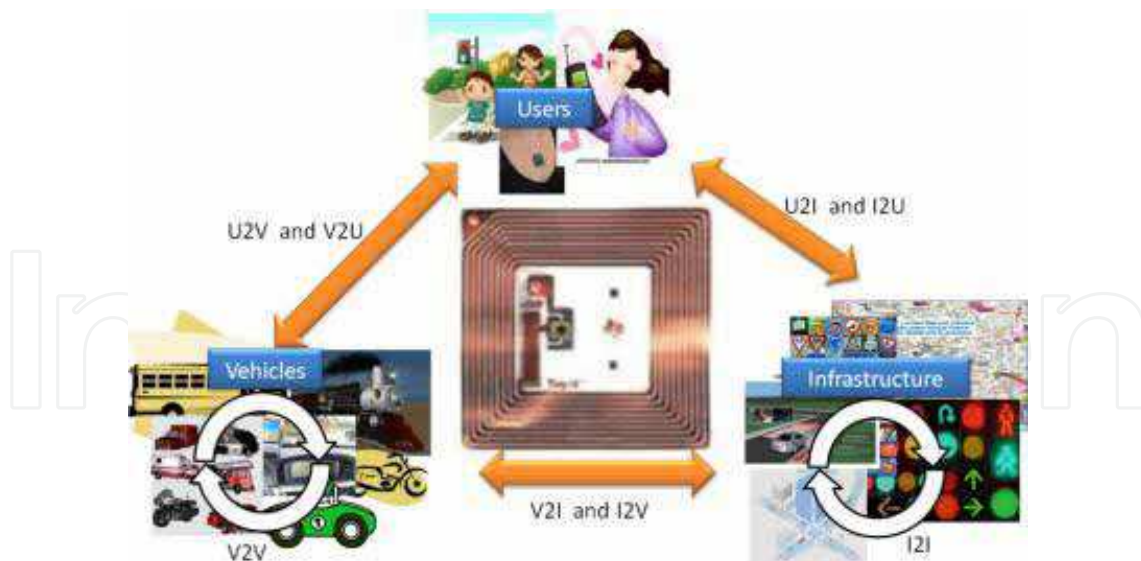
Fig. 1. Illustrate the focused communication among user, vehicle and infrastructure.

1.3 Organization of this chapter

The main aim of this chapter is to introduce the above architecture and communication protocols considering case studies on vehicle to vehicle and vehicle to infrastructure communication.

The remainder of this chapter is organized as follows. Section 2 describes the literature review on RFID and ITS. The proposed architecture and communication protocols are explained in Section 3 and Section 4 respectively. Applications of the proposed architecture in ITSs are described in Section 5 while brief discussion is made in Section 6 addressing sample cases with OTag architecture and finally the Section 7 concludes the chapter with future works and remarks.

2. Related work

As the characteristics and behaviours of RFID tags help to build the novel ITS applications RFID became a suitable candidate technology. Currently, there are RFID systems used in toll collection, parking management, transport payments and logistics management systems by using conventional RFID technology. However, when the capability of RF communication is properly analyzed, it can be seen that there are more possibilities beyond that.

After considering the characteristics and behaviours of RF communication, it is possible to build rich ITS applications that improve the infrastructure by ensuring the safety, security, comfort-ability, productivity, and interoperability in eco-friendly manner. Existing applications are using conventional RFID tags and store only a unique number and the data related to the tag is taken from the proprietary databases. Furthermore interoperability and plug and playable features are not supported.

Though the RF tag can play a big role to achieve safety, security, productivity and comfortability in ITSs, current usage of them are not up to the maximum possibility due to many reasons. They are mainly used for electronic toll collections and proprietary parking management systems. If a vehicle is to use both of these applications, vehicle should be equipped with two RFID tags to work with two different systems.

2.1 Tags used in automated toll collection system

Electronic toll collection (ETC), an adaptation of military "identification friend or foe" technology, aims to eliminate the delay on toll roads by collecting tolls electronically. It is thus a technological implementation of a road pricing concept. It determines whether the cars passing are enrolled in the program, alerts enforcers for those that are not, and electronically debits the accounts of registered car owners without requiring them to stop (Hae et al., 2004).

Enforcement is accomplished by a combination of a camera which takes a picture of the car and a radio frequency keyed computer which searches for a driver's window/ bumper mounted transponder to verify and collect payment. The system sends a notice and a fine to cars that pass through without having an active account or paying a toll (Isamu et al., 2005).

Norway has been the world's pioneer in the widespread implementation of this technology. ETC was first introduced in Bergen, in 1986, operating together with traditional tollbooths. In 1991, Trondheim introduced the world's first use of completely unaided full-speed electronic tolling. Norway now has 25 toll roads operating with electronic fee collection (EFC), as the Norwegian technology is called AutoPASS. In 1995, Portugal became the first country to apply a single, universal system to all tolls in the country, the Via Verde, which can also be used in parking lots and gas stations. The United States is another country with widespread use of ETC in several states, though many U.S. toll roads maintain the option of manual collection (Hae et al., 2004).

Electronic toll collection systems rely on four major components: automated vehicle identification, automated vehicle classification, transaction processing, and violation enforcement (Isamu et al., 2005).

2.2 Automated vehicle identification

Automated vehicle identification (AVI) is the process of determining the identity of a vehicle subject to tolls. The majority of toll facilities record the passage of vehicles through a limited number of toll gates. At such facilities, the task is then to identify the vehicle in the gate area.

Some early AVI systems used barcodes affixed to each vehicle, to be read optically at the toll booth. Optical systems proved to have poor reading reliability, especially when faced with inclement weather and dirty vehicles. Most current AVI systems rely on radio-frequency identification, where an antenna at the toll gate communicates with a transponder on the vehicle via Dedicated Short Range Communications (DSRC). RFID tags have proven to have excellent accuracy, and can be read at highway speeds (Keiichi et al., 2001).

2.3 Automated vehicle classification

Automated vehicle classification is closely related to automated vehicle identification (AVI). Most toll facilities charge different rates for different types of vehicles, making it necessary to distinguish the vehicles passing through the toll facilities.

The simplest method is to store the vehicle class in the customer record, and use the AVI data to look up the vehicle class. This is low-cost, but limits user flexibility, in such cases as the automobile owner who occasionally tows a trailer. More complex systems use a variety of sensors. Inductive sensors embedded in the road surface can determine the gaps between vehicles, to provide basic information on the presence of a vehicle. Treadles permit counting the number of axles as a vehicle passes over them and, with offset-treadle installations, also

detect dual-tire vehicles. Light-curtain laser profilers record the shape of the vehicle, which can help distinguishing trucks and trailers (Keiichi et al., 2001).

2.4 Transaction processing

Transaction processing deals with maintaining customer accounts, posting toll transactions and customer payments to the accounts, and handling customer inquiries. The transaction processing component of some systems is referred to as a "customer service centre". In many respects, the transaction processing function resembles banking, and several toll agencies have contracted out transaction processing to a bank.

Customer accounts may be post paid, where toll transactions are periodically billed to the customer, or prepaid, where the customer funds a balance in the account which is then depleted as toll transactions occur. The prepaid system is more common, as the small amounts of most tolls make pursuit of uncollected debts uneconomic. Most post paid accounts deal with this issue by requiring a security deposit, effectively rendering the account a prepaid one (Keiichi et al., 2001).

2.5 Electronic congestion pricing

Congestion pricing is a system of surcharging users of a transport network in periods of peak demand to reduce traffic congestion. Examples include road pricing, and higher peak charges for utilities, public transport and slots in canals and airports. This variable pricing strategy regulates demand, making it possible to manage congestion without increasing supply. At the same time, users will be forced to pay for the negative externalities they create, making them conscious of the costs they impose upon each other when consuming during the peak demand, and more aware of their impact on the environment (Lionel et al., 2004).

The application on urban roads is limited to a small number of cities, including London, Stockholm, Singapore and Milan, as well as a few smaller towns. Four general types of systems are in use; a cordon area around a city centre, with charges for passing the cordon line; area wide congestion pricing, which charges for being inside an area; a city centre toll ring, with toll collection surrounding the city; and corridor or single facility congestion pricing, where access to a lane or a facility is priced (Lionel et al., 2004).

Congestion pricing or urban toll schemes were implemented to enter the downtown area using ETC technology and/ or cameras and video recognition technology to get the plate numbers in several cities around the world.

2.6 Violation enforcement

A violation enforcement system (VES) is useful in reducing unpaid tolls, as an unmanned toll gate otherwise represents a tempting target for toll evasion. Several methods can be used to deter toll violators.

Automatic number plate recognition, while rarely used as the primary vehicle identification method, is more commonly used in violation enforcement. In the VES context, the number of images collected is much smaller than in the AVI context. This makes manual review, with its greater accuracy over fully automated methods, practical. However, many jurisdictions require legislative action to permit this type of enforcement, as the number plate identifies only the vehicle, not its operator, and many traffic enforcement regulations require identifying the operator in order to issue an infraction (Keiichi et al., 2001).

2.7 Tags used in automated parking management system

Automated parking management systems offer great benefits to owners, operators, and patrons. Some of the main benefits include reduced cash handling and improved back-office operations, high scalability, automatic data capture and detailed reporting, improved traffic flow at peak hours, improved customer service, cash-free convenience, and also provinces to arrange special privileges for VIP customers such as volume discounts, coupons, and other discounts for daily parkers (Keiichi et al., 2001).

RFID enabled automated parking access control systems eliminating customers' need to fumble for change, swipe cards, or punch numbers into a keypad. Vehicles can move smoothly through controlled entrances, and more parkers can be accommodated, thereby increasing revenues. There are no cards to read, tickets to read and sort, and the whole system is a convenient, hands-free way to ensure easy vehicle parking (Lionel et al., 2004).

TransCore is one of the pioneers to provide parking access control systems which offer using RFID technology. They uses proven eGo® and Amtech®-brand RFID technology to deliver reliable, automated parking access control systems solutions. TransCore's parking control systems facilitate airport security parking and parking at universities, corporations, hospitals, gated communities, and downtown parking facilities (Lionel et al., 2004).

ActiveWave is another company who provide such systems using RFID technology. In their system, surveillance cameras or video recorders can be triggered whenever a vehicle enters or exits the controlled area (Lionel et al., 2004).

Although there are number of companies who provide RFID based parking management systems, almost all the systems are proprietary, and provide no interoperability. Some of them are using passive RFID systems. As described in Chapter 1, there is no stand alone, self-describing, plug and playable, interoperable and access controlling mechanisms built into those tags. Hence, all the existing and previously proposed RFID tags are not suitable for the real requirements that are demanded by ITSs.

3. New architecture: OTag

Object tag (OTag) is a radio frequency (RF) tag which can represent real world objects such as vehicles. Considering the main concepts of Object Oriented Architecture, RF tag was designed with its own attributes and methods to stand alone by itself. The tag can be developed as active, passive or semi-passive depending on the application requirement. The attributes and the methods of the OTag may differ according to expected characteristics and behaviors of the real world objects. In other words the attributes and the methods are defined according to object class. For instance, the attributes of a vehicle OTag differ from the attributes of a road symbol OTag. Each OTag can be considered as an instance of an object class. If a vehicle is the object class, tags attached to all vehicles are considered as instances of vehicle object class like in object oriented concepts. Furthermore, each attribute of the OTag has got access modifiers to manage the access to its information based on roles. They are categorized as public, friendly, protected and private. With above features OTag is capable of being stand alone, interoperable, self-describing, and also plug-and-playable. Interoperability is provided by developing common communicational protocols to communicate between tag and interrogator (reader/ writer). Howeer the access modifiers used here are not exactly the same as in object oriented concepts.
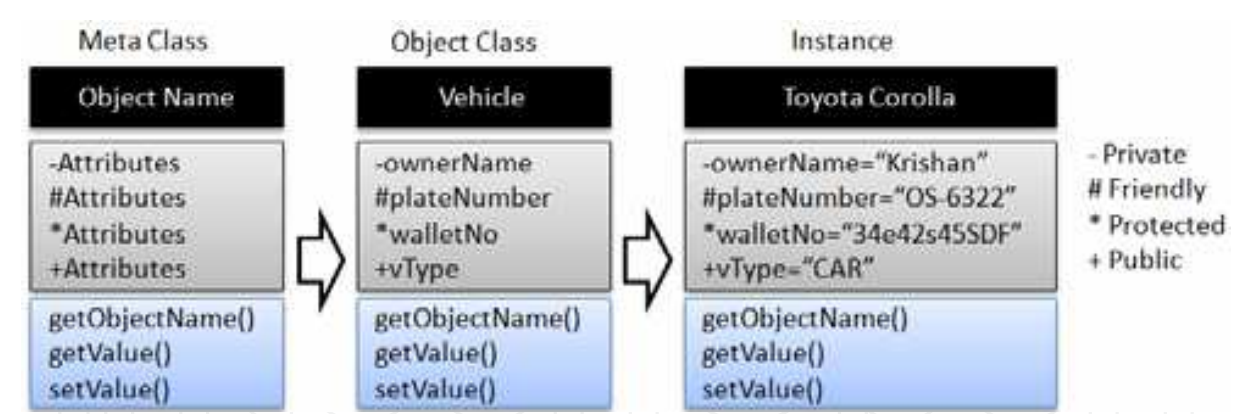
Fig. 2. Illustrate the Instantiation Process of Object to Instance.

OTag architecture can be used in two ways: one is just as a real world object and the other is as an agent. For example when it is necessary to enable communication with vehicle, attaching vehicle OTag instance to the vehicle enables the communication with vehicle. If vehicle need to act autonomously, vehicle will be installed with an agent which is a combination of a reader/ writer, processing unit and OTag as shown in figure 3. These three units together compose the actions of an agent that can work according to predefined instructions (Krishan et al., 2009).

Fig. 3. Illustrate the composition units of OTag agent.

Access modifiers can be considered as roles and one of the four access modifiers is assigned to each attribute. With the help of those modifiers, OTag acts four roles: public, friendly, protected and private. Public means no security and any reader can read any attribute value of public area. Private, Protected, and Friendly attributes of the OTag need secure access. Furthermore the writing permission is also available for these areas, but that is controlled by both keys and memory types. For instance write once memory is used for some attributes in friendly area to prevent updating fixed attribute values whereas rewritable memory is used for dynamically changing attribute values according to the behaviors of object class. Details of each role definition are described in later paragraphs.

Figure 2 represents the Object, Class and Instance structures of the OTag. This is the process of instantiation. Any object in the real world should contain its own characteristics and behaviors. In other words each object should have attributes and methods to access those attributes. Tag object has such attributes and methods with access modifiers. When defining a class from object, the class name will be given. Therefore, OTag gets its class name such as vehicle which is a class level attribute, plus implementations of get and set methods that are defined at the time of fresh OTag class creations. In other words, when a vehicle class OTag

is created, it will consist of vehicle attributes and vehicle method implementations inside the tag. Such a tag becomes an instance after attaching it to a vehicle. Such as attaching to the vehicle OTag into a vehicle and populating its attribute values make the proper instance of vehicle OTag. Similarly other objects, classes, and instances can be defined.

Once the OTag instance is created, that instance of OTag becomes self-describing and stand alone using the features of object oriented architecture and radio frequency technology. Furthermore it has a common interface to communicate and thereby interoperability is guaranteed.

Plug and playability is a capability of automatically recognizing, configuring and resolving resource conflicts when attached or detached a hardware component to or from a system when running or ceased without user intervention by notifying its availability to the relevant actors. Thus it provides ease of use, maintenance and scalability while supporting the phase base implementation which is worth when installing OTag at many of places. To achieve plug and playability, tag must be self-describing, stand alone and have common communication protocols to communicate with any actor in a system.

3.1 Logical structure and roles of OTag

Role base accessing methods are implemented using access modifiers, memory types and encryption algorithms. As described in the above paragraphs, four roles of vehicle OTag are defined here.

Fig. 4. Illustrate the Logical Structure of an OTag Class.

Memory types used here are ROM, EPROM, and EEPROM. OTag controls writing permissions according to the process flow by using these three types of memories. ROM is used for read only data and they are created by time of fresh tag manufacturing. EPROM is used for one time writing data and they are all about product information. EEPROM is used for all the rewritable data and those data may be changed in any stage of the product lifecycle by relevant authorities. For example, if the attribute values belong to the owner may change after some time of usage. Such as address changing after changing the residence.

Public modifier allows reading and writing of any attribute value by any interrogator who has a common communication interface. Private role is granted to the vehicle owner. He has the permission to read/ write any attribute of his own vehicle other than the protected area which is used by one government authority such as department of motor vehicle registration. If the owner needs to change some attribute value in friendly area, he must use the key of friendly area. Thus an owner has two keys with him: private key and friendly key in addition to a PIN to provide secure transference of ownership of the vehicle.

Protected modifier controls the area used by the government authority in vehicle tag. After first registration of the vehicle, rewriting or updating of attribute values in this area can only be done with the protected key. Vehicle's license plate number, inspection expire date and etc are available in this area.

Friendly modifier allows several services to be catered in effective manner. The owner of the vehicle must register with friendly key to allow reading/ writing of such area to use the service render by the service provider. For instance ETC or automated parking collection facility can be provided after prior registration with relevant authorities. Emergency vehicles like ambulances, fire brigade, rescue, and police petrol use this area for traffic signal prioritizations.

Figure 4 illustrates the clear image of the memory types, access modifiers, and respective keys of each role. Encryption algorithm used hers is AES-128 stream cipher. Therefore each key size is fixed to 128bits. No secured information is transmitted without sufficient authentication.

OTag contains methods, data "Initial", 128-AES algorithm and processing module. OTag generates nonce N_I whereas the reader generates three nonce values N_T, ID_I, and ID_T to carry out proper mutual authentication. In addition that three role keys and PIN are stored to ensure the security of data.

OTag can store its own attribute and methods inside the Tag. Therefore, there is no need to run a database lookup to retrieve detail information from a database. Thus it provides stand alone capability. Unlike conventional RFID tag, OTag can also control and manage role base accessing depending on four roles: public, friendly, protected and private. Furthermore, the OTag itself contains the necessary information to describe its characteristics and behaviours. Thus OTag can represent any object and when combined with interrogator it can also act as an agent.

4. Communication protocols

OTag has five main protocols: non-secured reading, secured reading, secured writing, key updating and transferring tag ownership. Transferring ownership of OTag is a combination of above protocols. It is only used in authorized centres since specific readers will carry out this task. Section 5.1 describes the usage of ownership transference in detail.

Protocol notations are as follows.

K_{prv} - *Private Key (128bits)*
S_{prv} - *Shared Key or PIN (48bits)*
K_{pro} - *Protected Key (128bits)*
K_{frn} - *Friendly Key (128bits)*
PIN   - *Personal Identification Number (48bits)*
N_I - *Nonce generated by Interrogator (40bits)*

N_T - *Nonce generated by Tag (40bits)*
ID_I - *Interrogator generated ID (16bits)*
ID_T - *Interrogator Generated ID (16bits)*
Initial - *Publicly defined initial message (16bits)*
R   - *Response value – Attribute Value, or Successful /Failed [1/0]*
{M}K   - *Message "M" encrypted by Key "K" using AES128 steam cipher algorithm*

4.1 Non-secured reading protocol

As figure 4 illustrates, non-secured reading protocol is used for public reading. Any reader can query the public attribute values by passing the attribute name to the OTag. For that attribute names of the given object class must be available for the reader to query the attribute value. For instance, attribute name list of vehicle class should be available with the interested readers. Interested readers can query "Type" attribute value from OTag. Then the OTag will answer with value "CAR".
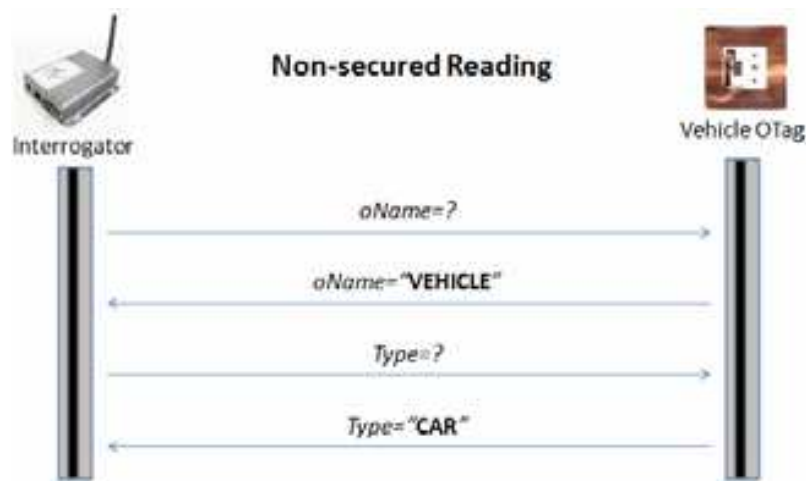

Fig. 4. Illustrate the public reading protocol.

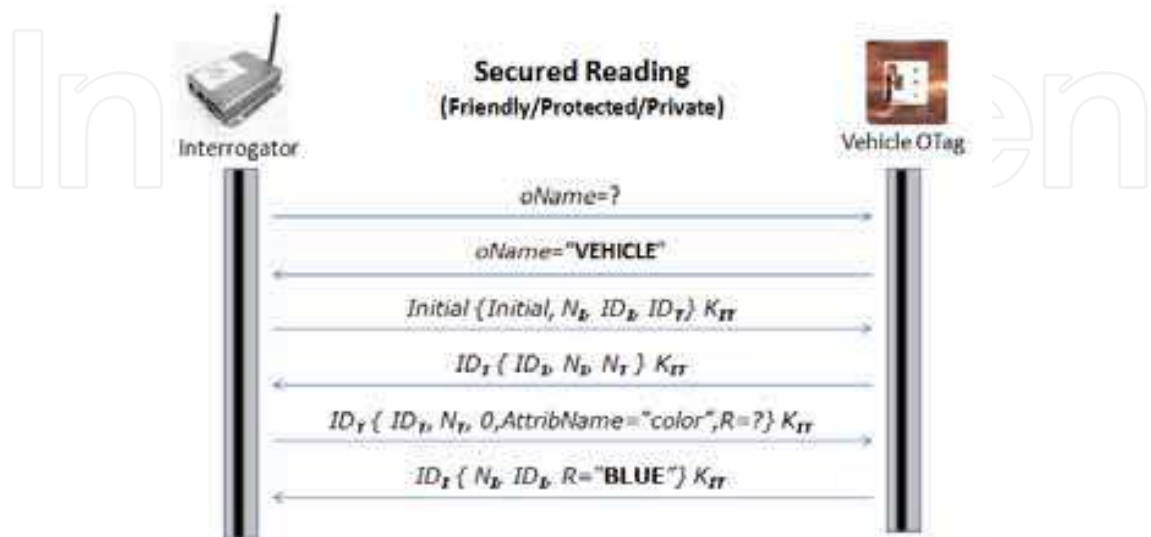## 4.2 Private, protected and friendly reading

Fig. 5. Illustrate the secure reading protocol with private, protected and friendly role keys.

Each role attribute values should be managed securely. Reading is allowed only after successful mutual authentication. Here the K_{IT} denotes the Encryption key used in each party. For instance, K_{IT} denotes the private key in private reading where as K_{IT} denotes the protected key in protected reading. Reading is only granted for authorized parties and they can only read the data which belong to them. To ensure security of each reading messages are encrypted with authorization key and send as shown in Figure 5.

4.3 Private, protected and friendly writing

Same as in the secure reading, the secure writing needs successful mutual authentication. Attribute name and attribute value pair should be passed for each writings. After successful writing, interrogator will be acknowledged as shown in Figure 6.
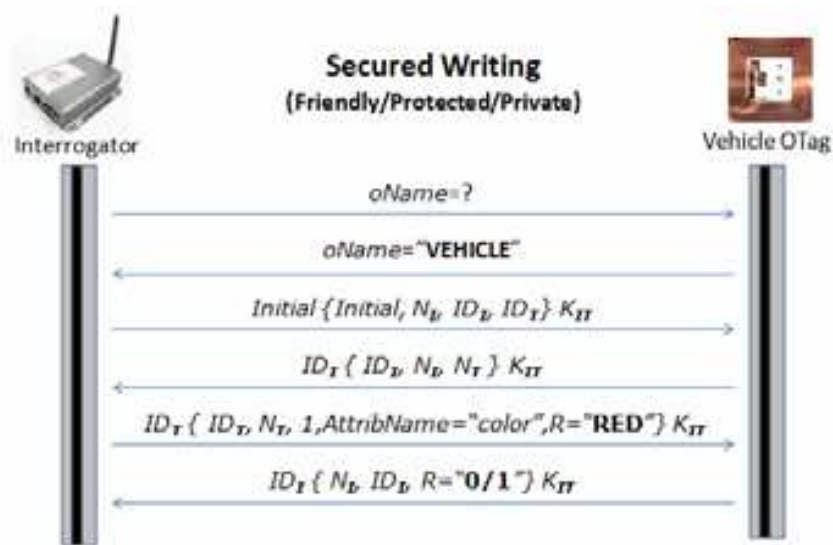

Fig. 6. Illustrate the secured writing protocol with private, protected and friendly role keys.

4.4 Secure key updating

Unlike secure writing as shown in Figure 7, it is necessary to confirm the keys to be updated before actual key updating because the communication will be no longer possible if a wrong key is set. Therefore, there are two more passes in this protocol other than secure writing as shown in Figure 6.

4.5 Transferring the ownership

This is also a secured writing process. Before transferring the ownership, personal data must be deleted. Therefore all the private data are deleted using secured writing protocol. After successful deletion, key updating will be carried out. If the new owner and the old owner are present, keys will be updated on the spot. Otherwise keys will be converted to temporary secrets and passed to the authorized agents to handle ownership transferring process. This process is carried out by a specific reader place in authorized centres.

Once the ownership is transferred the predecessors cannot read the tag as they are unable to provide new keys to get the access to the area now belonging to successors. Therefore, predecessors' and successors' security and privacy are ensured.
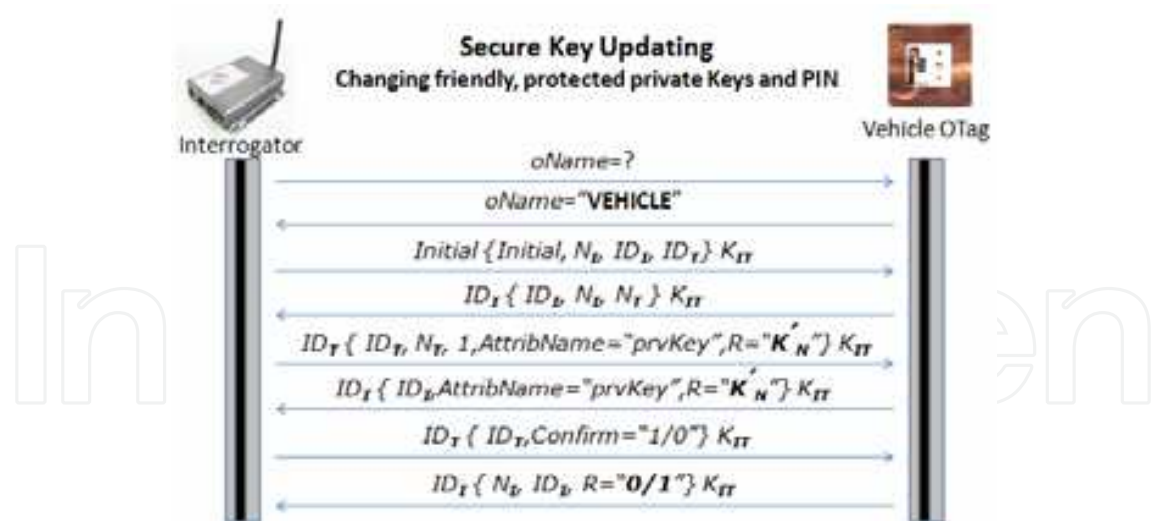
Fig. 7. Illustrate the role key update protocol for private, protected and friendly role keys.

5. Possibilities and applications with OTag

As explained in Section 3, OTag inherits all the characteristics and behaviours of RF communication. Additionally, OTag is intelligent, stand alone, self describing, plug and playable, and interoperable with role base accessing system that allows to communicate with different actors. Here the OTag agent is embedded into a vehicle.
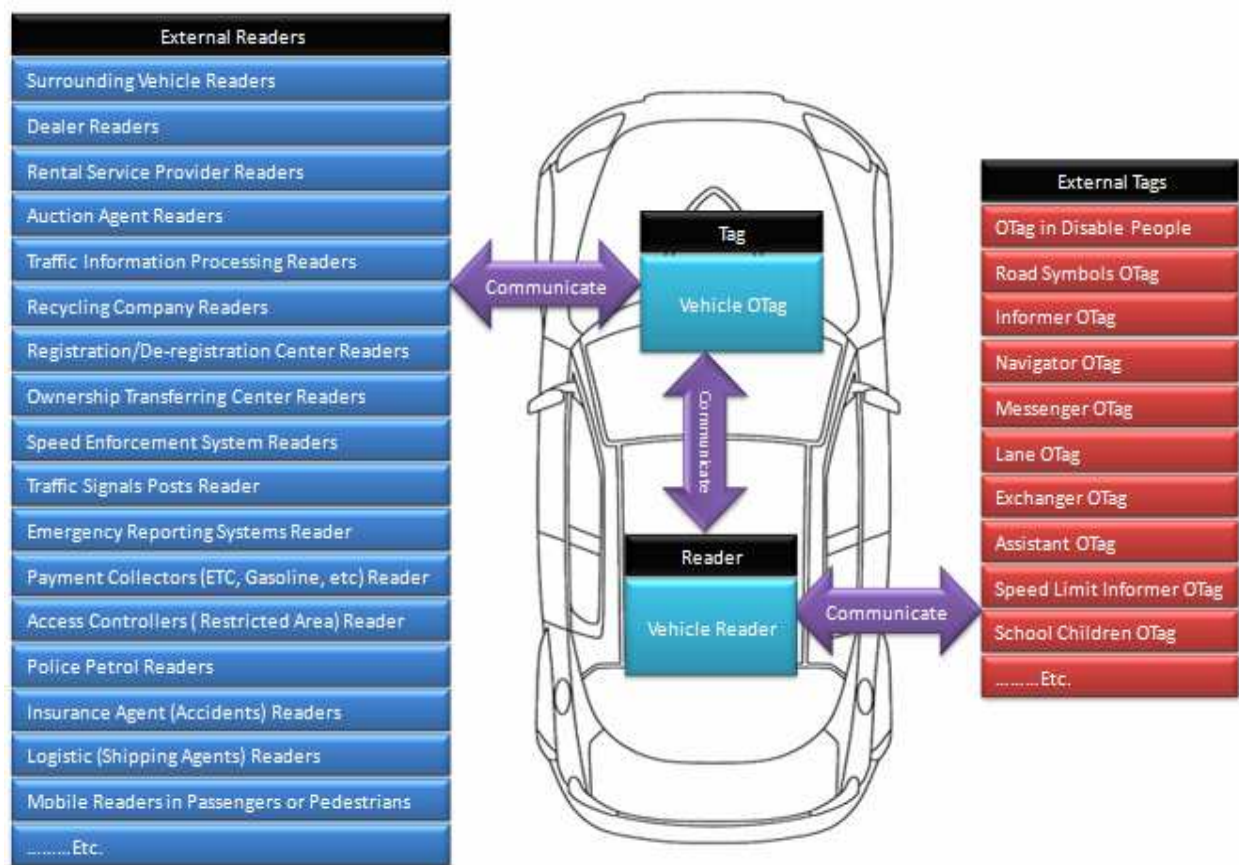

Fig. 8. Illustrate the actors in ITS as readers and tags.

OTag can be used to represent most of the agents in the ITS system. Each Object that interacts with ITS system can be modelled as an OTag. For instance, the main object in ITS system is the vehicle. Other than that there may be traffic signals, road symbols, road guides, disable assistants, information providers, rules and regulation controllers, etc. As OTag can be used to create an interactive agent for each task, efficient and effective infrastructure can be built to support ITSs.

Figure 8 illustrates the different actors in ITS, that are interested in communicating with the main actor vehicle. External Readers can read OTag in vehicles and the readers in vehicle can read infrastructure and passenger or pedestrian OTags.

5.1 OTag in vehicle

Fig. 9. Illustrate the Logical Structure of an OTag instance in Vehicle.

Imagine that each vehicle has got a RF reader and an active OTag in it. This arrangement makes vehicle an intelligent interface. Therefore, OTag enables large array of applications to improve ITSs.

Figure 9 represents the logical structure of an OTag in vehicle. Four areas for four roles are marked with A, B, C and D as described in section 3. Information stored in the public area can be read by any reader whereas the friendly, protected and private areas are secured with reading and writing permission. Each area is used by different agents throughout the lifecycle of the vehicle. Four areas of the vehicle OTag can be used as follows.

Public area stores the object class name, type, anonymous ID, intention and customizable attribute called PblAttrib01. Information stored in this area can be used to understand object and its movements. Identifying those public information leads to applications like collision avoidance, traffic signal management, real time traffic information, obstacle identification, road congestion management, road rule enforcements, disaster messaging systems, driving assistant systems, etc.

Friendly area stores the payID or walletID, riderMode, two customizable attributes named as frndAttrib01 and frndAttrib02. Information stored in this can be used to subscribe variety of services provided by companies. Any registered service provider can use this information to provide the comfortable service to the vehicle user. Electronic fee collection systems like toll collection and parking can use walletID whereas riderMode can be used to prioritize emergency vehicles.

Protected area stores the colour, model, manufactured year, frame number and type, engine, capacity, weight, size, license plate number, date of first registration, inspection validity, and tax payment status. Additionally it also has got two customizable attributes named as prtcdAttrib01 and prtcdAttrib02.
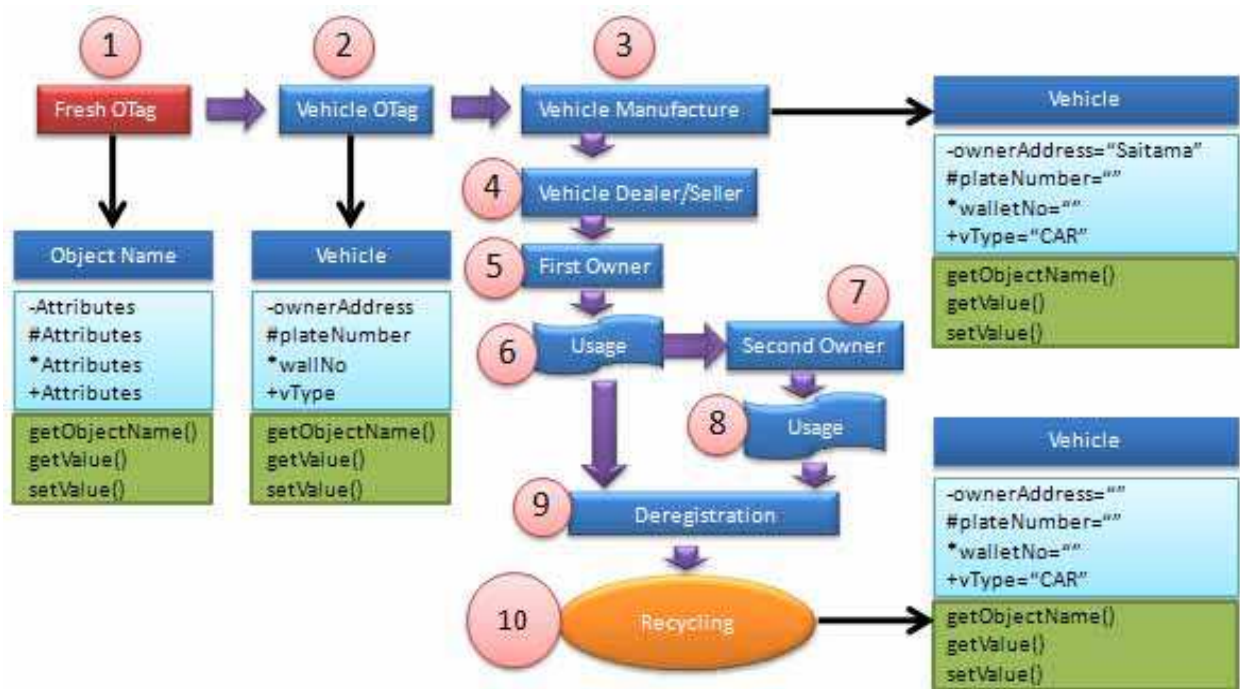

Fig. 10. Illustrate the flow for the OTag embedded vehicle lifecycle.

Information stored in this area is devoted to the vehicle governing authority. Mostly this is the government service. Therefore, after first registration the data stored in this area can only be manipulated by government authority such as department of motor vehicle registration. Additionally, protected information can be read only by the owner or the granted authorized persons in police. Inspection validity, insurance, tax, etc. helps to identifying the current status of the vehicle. Recognizing illegal, fake, clone, stolen or altered vehicles, issuing fines for inspection expired vehicles, verification of tax payments, management of carrying garage, temporary and brand new vehicles are some of the main applications using this area.

Private area stores owner name, address and one customizable attribute named as pvtAttrib01. Information stored in this area is to prove the ownership of the vehicle. No one

can read or write data into this area without the permission of the owner. When the vehicle is sold ownership information will be changed.

5.2 Tag flow

As shown in Figure 10, step 1 creates fresh OTags according to the object class. Each class has got different attributes as of the real world object. In this step, the tags contain the attribute names "oName" and "anonymousID". Then the OTag instance for vehicle class is created in step 2. It contains the attribute names relevant to vehicle class. Only the values of attribute names "oName" and "anonymous ID" are filled in vehicle OTag before attaching to a vehicle. The value of "oName" is "VEHICLE" and that of "anonymous ID" is a random unique number. Next the OTag is passed to the vehicle manufacturer.
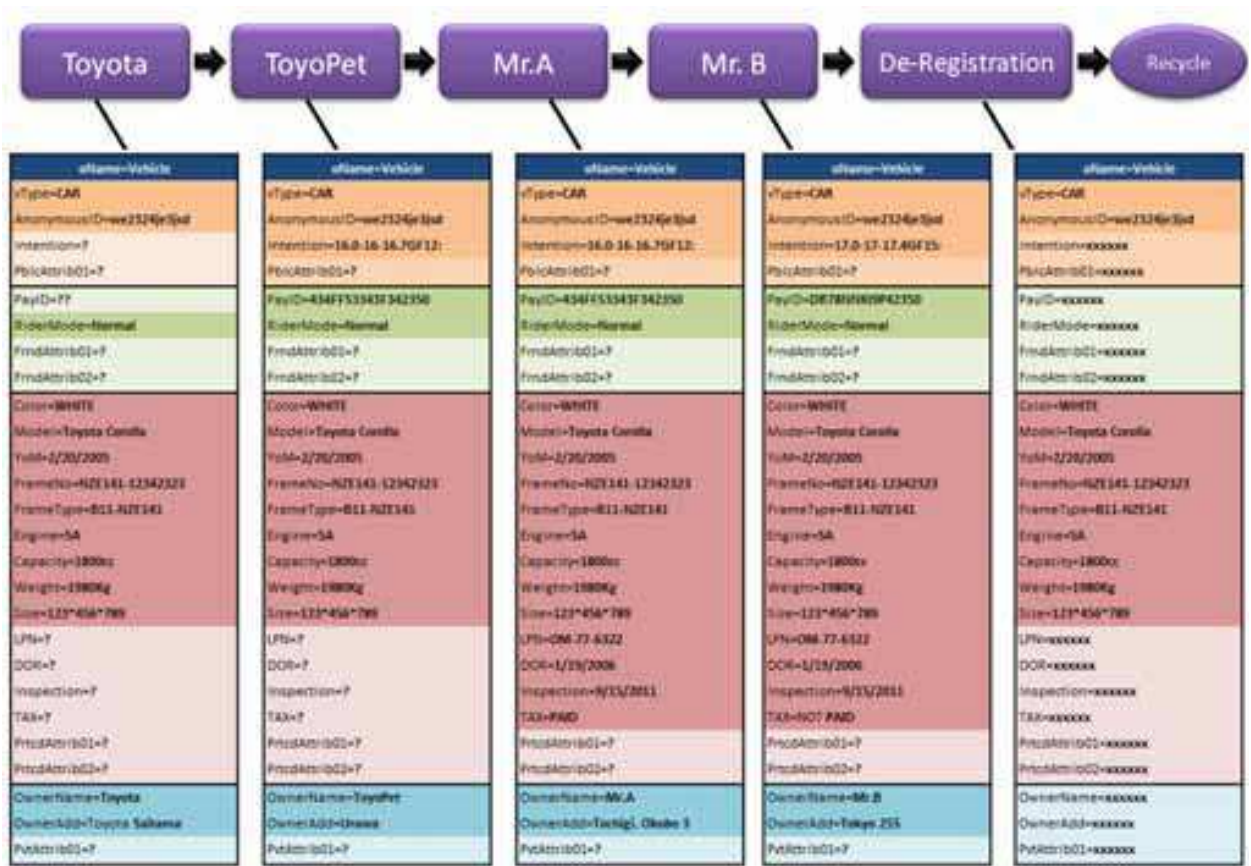
Fig. 11. Illustrate the sample flow for the vehicle OTag throughout its lifecycle.

Step 3 when vehicle manufacturers receive the vehicle OTag instances with empty attribute values except "oName" and "anonymousID". Additionally the three role keys and the PIN are set to their secrets. All the relevant instance attributes will be fed to the OTag. For example Toyota may request 1000 vehicle OTags to attached in brand new vehicles and then feed the instance attribute values such as vehicle type, frame number, engine etc as shown in Figure 12. Then the vehicles are passed to the dealers or sellers after transferring the ownership to the dealers.

In step 4 vehicles in dealers possession contains all information fed by the manufacture but the ownership information, role keys and PIN are changed to dealers' secrets. When a

customer bought a brand new vehicle as in step 5, first registration will be carried out. By that time the protected role key will be handed over to the vehicle governing authority while friendly, and private role keys with PIN will be changed to the customers' secrets as shown in Figure 11. Additionally the ownership information will also be changed to his own details. Since the customer has the friendly key to allow secure communication between desired service provider and his own vehicle, services like electronic toll collection, parking payments, gasoline payments, etc. can be subscribed easily.

Step 6 and step 8 emphasize the usage of the vehicle. During the usage period customer may extend the inspection period, pay taxes, etc. Then the relevant OTag attribute values may be updated as shown in Figure 11. When the customer needs to sell the vehicle to someone, ownership information should be transferred by visiting the authorized centres' readers.

In step 9 if the vehicle may be no longer needed, cancellation of registration can be done in the same centre and pass the vehicle for recycling as shown in step 10. By the time of de-registration only the minimum required information will be kept and other information including personal data will be deleted to protect security and privacy of users as shown in de-registration tag information in Figure 11. Then the recycling company also can use RF communication to improve their process of gathering information on recycling units.

Note that each user's ability of writing is also controlled by using three memory types: ROM, EPROM and EEPROM.

6. Sample applications and discussions

After having installed the infrastructure and vehicle with OTags and interrogators, whole lot of possibilities will be opened up. Vehicle to Vehicle communication and Infrastructure to Vehicle communication are focused for sample cases.

Detecting vehicle to vehicle collisions at intersections, at merging and demerging and when changing lanes has a vital importance in ITS. If one vehicle can understand how other vehicles' move, the collisions can be detected. Once the collision is detected, precautionary action can be taken. Though the prior detection is very important, guaranteeing the avoidance is not an easy task but the consequences due to collisions can be reduced.

6.1 Identifying and expressing the intension of the vehicle

Identifying the current position and intended action including driving direction is very important to avoid fatal accidents. For that each vehicle should express its intended movements at least within a given block or time slot. Following paragraphs explain how a vehicle can express its intension to other vehicles or infrastructure in detail.

There is OTag class called Informer who can explain the next target, current position, current route and next crossing lane, etc. to a requester vehicle. These tags are positioned in the centre line of the road. It can be read by the vehicles running towards the both directions.

As shown in Figure 12. Informer OTag contains the next target information in the form of attribute name and value. Once the immediate previous 16.1 Informer OTag position is passed by a vehicle, intended action "16.1GF" of that vehicle is sent to the 16.2 Informer OTag via the vehicle reader requesting the next target information. Then the Informer OTag will respond with the next target information to the vehicle. If there is no previous Informer, the reader in the vehicle requests yourPosition attribute of first Informer OTag to understand the current position. Informer OTag can be of type passive.
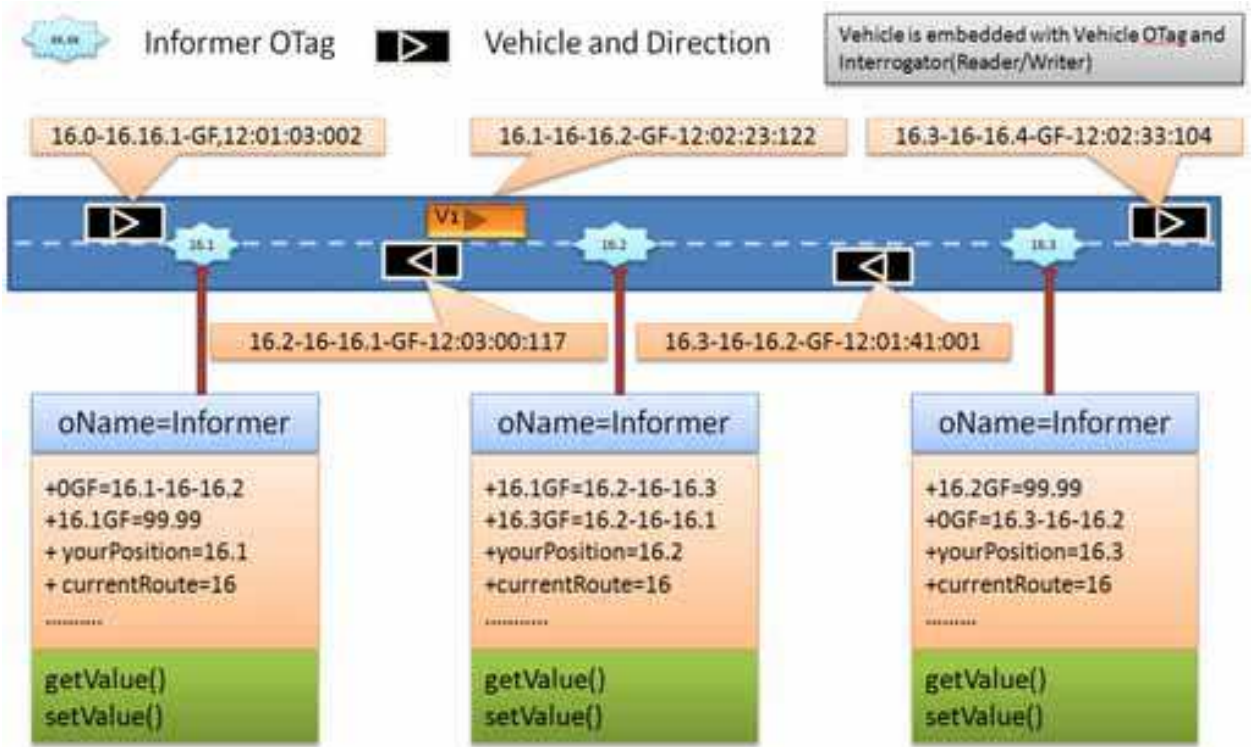
Fig. 12. Illustrate the informer instances of OTags and positions on the roads with moving vehicles.

As described, when a vehicle passes the very first Informer, the interrogator in the vehicle gets to know the next immediate target information. After that, the interrogator writes that information with intended action, running speed, and expected reach time of current immediate target and lane number if it exists, to the public area of the vehicle OTag. If there is no lane number, or previous position information before the Informer, the predefined not applicable dummy values will be used to compose the intention attribute. Once the vehicle OTag is filled with intention, it will start expressing the intended movements as shown in Figure 12. This process continues until the no Informer tag is found. Whenever changes happened to the values relevant to the parameters used to compose above message, recalculation is done and vehicle OTag starts retransmitting the new message. For instance, if the speed is changed the recalculation is done and after that the retransmission starts. A target message interpretation is represented in Figure 13.

If a moving vehicle could not pass any Informer tag, the vehicle OTag will transmit only the available information with predefined dummy values. In this situation, the vehicle that is lacking main information must take care of its mistakes, and only simple warning about surrounding vehicle can be given to such vehicles. This can happen if a vehicle enters to the road between two Informer tags.

Here the intended action is divided to seven categories: Turn Left (TL), Turn Right (TR), Go Forward (GF), Go Backward (GB), U-Turn (UT), Hazard Stop (HS), and Emergency Accident (EA). Intended movements are not expressed when a vehicle is in parking mode.

The message in Figure 13 is interpreted as a vehicle is moving over the route number 16 by passing the Informer position 16.0 and heading forward (GF) to 16.1. Current estimated reach time to the 16.1 is 12:02:23:122 and the vehicle is running at a speed of 60kmph in lane 0. Here the lane 0 means road has only one lane for one side.

Fig. 13. Target message expressed by moving vehicle.

6.2 Vehicle talking to vehicle

In this section we explain two main cases to avoid collisions when crossing an intersection and changing lanes. For both of them it is necessary to understand the movements of the surrounding vehicles. Our solution considers six types of vehicle to vehicle collisions. They are the collisions that may occur when crossing the intersection, when changing the lanes,
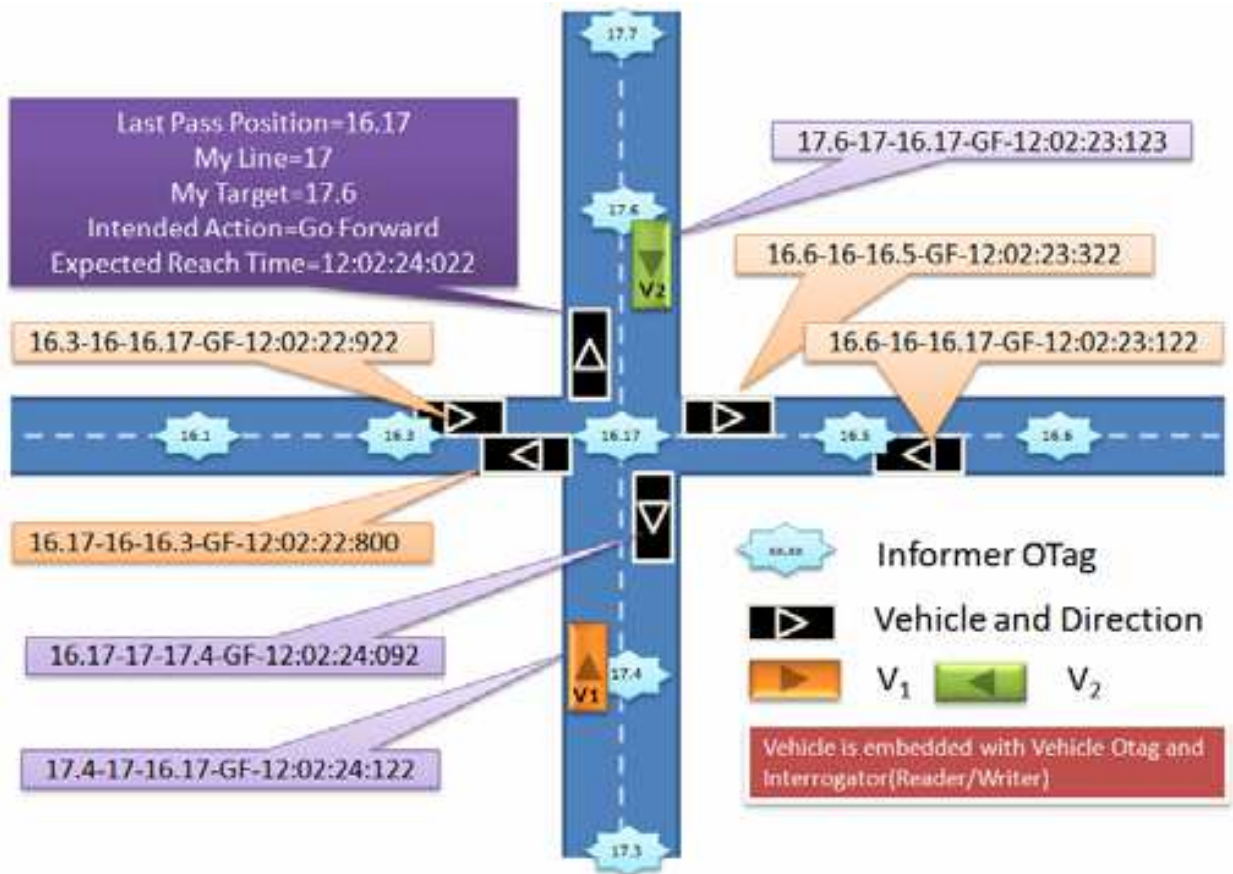

Fig. 14. Illustrate Detecting collision in intersection with 8 vehicles from 4 sides going forward.

when merging and demerging, when running face to face, when running to front vehicle and when backing up. Though it is possible to solve each of them with the method proposed in following section, only crossing intersections and merging lanes are discussed here.

To identify the vehicle movements, following assumptions were made.

1. Infrastructure Informer OTags have to be placed according the following diagram.
2. Each Informer OTag know its position, and immediate Informer position.
3. Vehicle should be equipped with interrogator (Reader/ Writer) and Vehicle OTag.

6.3 How to detect the collisions at intersection

Consider the route number of the vertical route as 17 and horizontal route as 16 as shown in Figure 14. Suppose that the vehicle V1 is moving towards the intersection passing the 17.4 position in the route 17. V1 explains others about his intended movements in his message as shown in the same figure. This message means that the V1 is heading forward (GF) his next immediate target 16.17 by passing the 17.4 over the route 17 and he is supposed to reach the target by 12:02:24:122.

Similarly, in his assistant screen there will be an image similar to Figure 14 explaining how the other vehicles are coming towards the intersection and also leaving the intersection by interpreting their intended movement messages. Since real time calculation is done and also every change is calculated once change occurs to any of the parameters used to create the message, reach time of each vehicle can be estimated accurately. If two or more vehicles are reaching a same target by the exact time, there is very high possibility to collide them. Therefore once the reader in the vehicle could understand such situation, the driver can be warned or asked to take precautionary steps to avoid the predicted collision.

In case of turning vehicles, the message explains their intensions by setting the composed value with TL or TR. Suppose that the vehicle V1 is going straight and the vehicle V2 is going to take a V1's left, V1 must understand the possible collision and take precautionary steps. If V2 is going to take the turn to right side of the V1, no collision will be happened. Thus quick decision can be taken and smooth, safe and fast crossing of intersection can be realized with OTag.

6.4 How to detect the collision when merging lanes

Figure 15 illustrates the movements of merging points. There are three main types of actions which lead to collisions: merging, demerging and turning to right or left. Each movement should be properly identified and drivers are informed possible collision.

Consider the route number of the road in Figure 15 as 16 and it has got two lanes for one direction and one merging point as illustrated. Informer OTag (16.3) should also been placed at exact line of the merging point shown in the Figure 15. The number of the entering lane is considered as 100. One Informer OTag (16.2) must be installed in the entering lane (100) before reaching the merging point and two lane tags must be also installed in lane 110 and 111 to recognize the lanes as shown in the Figure 15. When lane tag is passed the vehicles get to know their own lanes via their readers. Entering lane is one way and one lane, thus the Informer OTag 16.2 contains the lane number as 100 with next target (16.3) information. Therefore, there is no need to place another lane tag in the entering lane.

Suppose that the vehicle V1 is running straight forward over the route 16 while the vehicle V2 is coming towards the merging point to merge with lane 110. V1 expresses his intended

movement as 16.0-16-16.3-GF-12:02:23:082-110-95 which means that V1 is heading forward (GF) over the route 16 passing the 16.0 Informer and targeting the 16.3 Informer. Also V1 can reach the target by 12:02:23:082 as he is moving at a speed of 95Kmph in lane 110 whereas V2 express the message that can be interpreted as V2 is heading forward (GF) over route 16 lane 100 passing 16.2 targeting 16.3 at a speed of 40Kmph and his estimated reach time is 12:02:23:122 by the intention "16.2-16-16.3-GF-12:02:23:122-100-40".

Fig. 15. Illustrate detection of collisions when merging lanes.

Since the estimated time is so close, both of them will be informed by each other's screen that the drivers of V1 and V2 are heading to a possible collision. Then they can take precautionary actions while V2 must know that it has the lowest priority in this scenario. Similarly, all the vehicles driving towards the merging point can be informed possible collisions. Then the drivers can decide their next steps or autonomous system may tackle it in future.

Installation of these tags can be done in essential points where accidents occur frequently. Specially, in toll roads, accident rates are high when merging and demerging. Though it is possible to make safe and smooth merging with two lane tags and four or five Informer OTags, implementing same method in lane changing throughout the road needs to have more lane tags installed over the road which is costly at the moment. Therefore the essential points can be identified and installed.

6.5 Infrastructure talking to vehicle

Infrastructure will be consisting of tags and readers. The following cases are described assuming that there is a reader in the traffic signal post and it knows the friendly key of four emergency vehicle types: ambulance, fire brigade, rescue and police patrol.

6.6 How to prioritize emergency vehicles

One main application we consider is changing the traffic signal in intersection to green when the emergency vehicle is reaching the traffic signal post. Secure identification of emergency vehicles such as ambulance, police petrol, fire brigades and rescue vehicles should be in place to prevent frauds. Otherwise some vehicles may act as an emergency vehicle and try to get the advantage of signal prioritizing silently.

Currently all the emergency vehicles are identified by the tempo and tone of the siren hone. When the siren signal is heard, everybody has to stop and arrange the road to pass the emergency vehicle. This is always not successful; as there are long queues in congested situations which rarely could allow any movements before the traffic signal changes to green. Additionally in the intersections such system cannot prevent accidents because someone may enter to the intersection according to the traffic light guidance without understanding that an emergency vehicle is heading towards the intersection. With OTag, it is possible to change the signal for emergency vehicles' path and allow smooth traffic. By this way time taken to reach the destination by emergency vehicles can be reduced and thereby lives can be saved greatly.

There is a reader in the Intersection traffic signal post. It has the friendly key of the emergency vehicles. When the OTag in the emergency starts to say that I am an emergency vehicle, reader validate the vehicle and change the colour light to green to allowing emergency vehicle to pass smoothly. The changing logic will work as shown in Figure 16.
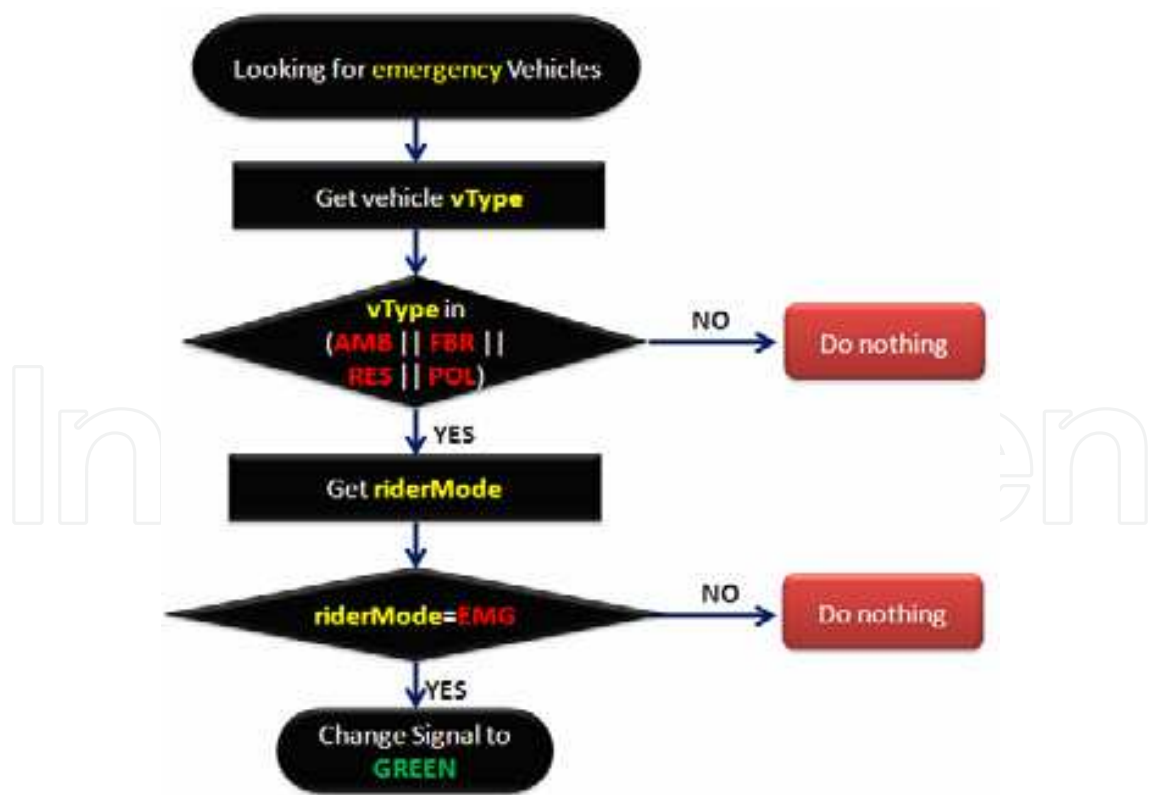
Fig. 16. Illustrate decision flow chart of changing colour lights according to the emergency vehicle request.

Emergency vehicles can change the status from NORMAL to URGENT depending on the patients condition. Then the OTag will describe its status to readers in the traffic signal. Once the reader understands the vehicle type, reader authenticates the vehicle and the green signal is issued for emergency vehicle to cross the intersection smoothly with others.

On the other hand drivers in the normal vehicles are informed that the emergency vehicle is approaching using vehicle to vehicle communication described in above section. Thus they can cooperatively help to pass the emergency vehicle without any tension, delay or accident.

6.7 How to enhance intersection traffic

Varying traffic volumes during the peak hours and midday makes it very difficult to enhance traffic signals. Similarly the areas that experience heavy traffic congestion, needed traffic signal timing improvements to implement effective traffic flow as well as air quality and fuel consumptions. Currently several methods are being used to detect and count the vehicle coming towards the intersection. Several systems are capable of monitoring the traffic arrivals and adjusting timings based on the detected inputs. Traffic detectors may range from metal detectors, infrared readers, image detectors, etc. Metal detectors are the most popular in use though they provide minimum information. Image detection devices exhibit numerous problems including degradation during bad weather and lighting.

Consider that there is a reader who has a reading distance of 100meters radius is installed in the traffic signal post as shown in Figure 17. All the vehicles are embedded with OTag and
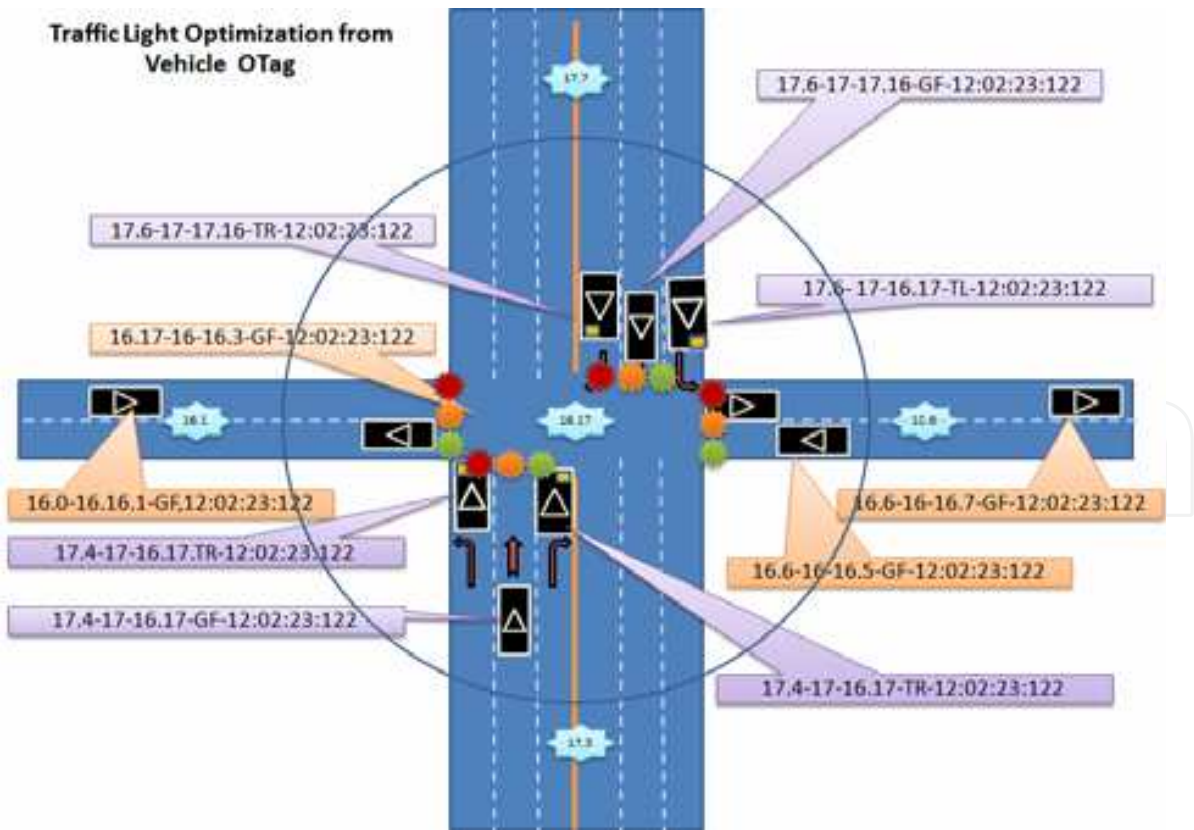
Fig. 17. Optimization through adaptive reading via Vehicle OTag and traffic signal agent.

they are expressing intended movements. By reading this message the reader in the traffic signal post understands the number of vehicles, in its range, their intended directions and the number of vehicle types including the availability of emergency vehicle or common transportation units such as bus, etc.

Depending on the policy of the country, traffic optimizing algorithm can be implemented considering above knowledge. Unlike in other conventional intelligent traffic systems, an extra knowledge can be mined and that knowledge can be used to optimize the traffic signal adaptively because OTag can provide detail information to take a better decision. Additionally if a tag is installed in the signal and set to describe starting and ending phases of transition to incoming vehicles, vehicle stopping can be made smooth and collision due to misinterpretations can be minimized.

6.8 How to prevent collisions in railroad crossings

In railway crossings, collision between vehicles and locomotives can be avoided using the similar arrangement. In this case the priority is given to the locomotive, so the vehicle passing the crossing must take the precautionary steps or its system might take such action automatically if driver neglect to act accordingly. Since the same arrangement is proposed for vehicles and railways, interrogator in the vehicle can understand that there will be a possible collision with moving locomotive if it proceeds without any precautionary action as shown in figure 18.
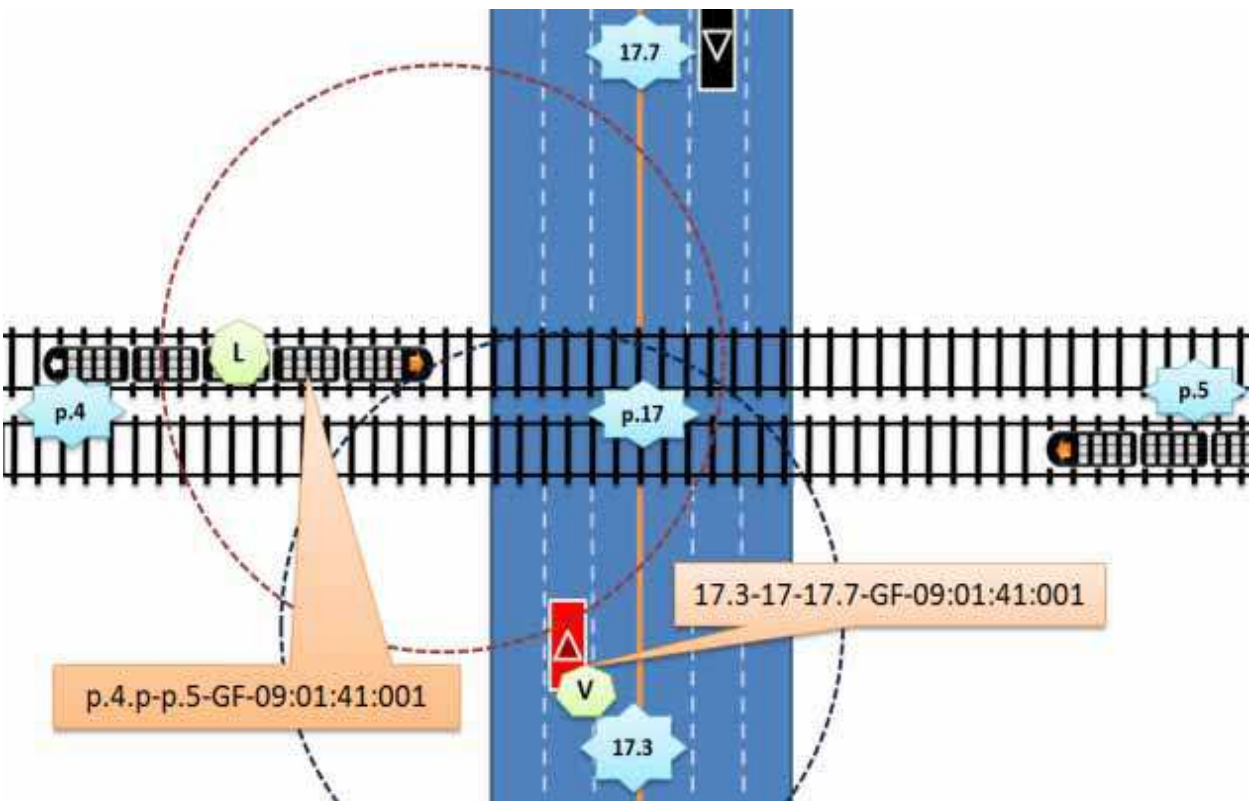

Fig. 18. Collision detection between vehicles and locomotives in rail road crossings.

Here the locomotive L is heading forward to pass the crossing and detect that there is a possible collision ahead but locomotive will not take any action unless and until IA issues any instructions to stop since the locomotive is given the first priority. A vehicle V heading forward towards the railway crossing detect that there will be a possible collision with passing locomotive and ask the driver to take precautionary steps to avoid accidents or activate automated breaking system. Thus collisions can be avoided or consequences due to the collision can be reduced.

6.9 Benefits and possibilities

Since the OTag's rich infrastructure supports intelligent, stand alone, self-describing, plug and playable, interoperable features with role based access controlling mechanism, main benefits like time savings, improved throughput, reduced crashes and fatalities, cost avoidance, increased customer satisfaction, and energy and environment friendly technology can be achieved while providing the safe, secure, productive and comfortable life in eco-friendly manner.

6.10 Other possibilities

As traffic signs provide the driver various information for safe and efficient navigation, one of the important areas is representing traffic signs on OTag. Then the automatic recognition of traffic signs can be provided to support for automated driving or driver assistance systems. Therefore the reader in vehicle can understand the road sign and explain the driver or control the vehicle according to the instructions. OTag can also be used to control the speed of a vehicle according to the road condition or climate changes. It also could be used to control the maximum allowed speed as well as the minimum speed. Similarly, there are scenarios where one vehicle trying to enter a single lane without seeing the coming vehicle due to building etc. Such situations can be mitigated without much infrastructure facilities and thereby eliminate the unnecessary movements of vehicles creating traffic congestions.

Not only that but also vehicles can be registered electronically, transferring ownerships can be automated, uninsured vehicle restrictions and taxations can be enforced without human intervention while many more innovative applications can be developed with this system as each chip has got user memory area for such applications including supporting for future autonomous driving infrastructure systems.

7. Concluding remarks

OTag is introduced to improve the existing intelligent transportation systems enabling large array of novel applications. The architecture of the OTag, communication protocols, capabilities, and usage are being explained. Collision detection in intersections and merging points, traffic signal prioritizing for emergency vehicles and adaptive traffic signal improving systems are discussed under vehicle to vehicle and vehicle to infrastructure communication.

As a conclusion, if the OTag can be implemented and used in vehicles and infrastructure, the power of the identification technology beyond the unique number creates a platform to communicate among user, vehicle and infrastructure assuring the safety, security, comfortability and productivity in eco-friendly manner.

In future we will release the other infrastructure tag designs by complying with OTag using the same protocols proving the interoperability, self-describing ability, ability to be stand alone, and plug and playability with role base access control mechanisms.

8. References

Al-Khateeb A. S., et al., "Dynamic Traffic Light Sequence Algorithm Using RFID Khalid" Journal of Computer Science 4 (7): 517-524, 2008 ISSN 1549-3636 c 2008 Science Publications.

Hae D. C,"Using RFID for Accurate Positioning",Samsung Electronics Co., LTD, Presented at GNSS 2004, The 2004 International Symposium on GNSS/ GPS.Sydney, Australia 6?8 December 2004.

Isamu Y., et al., "Secure Active RFID Tag System " Ubicomp2005 Workshops.

Ishida Y.,"Strategic Railway Systems Using ADS Technologies in Japan", Proceedings of the Sixth International Symposium on ADSous Decentralized Systems (ISADS'03) IEEE, pp.1-5, 2003.

Jun L., et al., "The Security and Privacy of Smart Vehicles" Joint work with Srdjan Capkun

Kitahara F., Kera K., Bekki K.,"Autonomous Decentralized Traffic Management System", Proceedings of ADS2000 International Workshop, pp.87-91, 2000.

Keiichi M, et al."Development of Wireless Communication Technology for ETC System", Mitsubishi Heavy Industries, Ltd.Technical Review Vol.38 No.3 (Oct. 2001)

Krishan S. K, M. R. Selim, J. Miura, Y. Goto, and J. Cheng, "POP Method: An Approach to Enhance the Security and Privacy of RFID Systems Used in Product Lifecycle with an Anonymous Ownership Transferring Mechanism", In Proc. SAC, ACM Press, 2007, pp. 270-275.

Krishan S. K. and Yoshiura N., "OTag: Architecture to Represent Real World Objects in RF Tags to Improve Future Intelligent Transportation Systems", International Journal of Convergence Information Technology(JCIT), Vol. 4, No. 2, pp. 30- 48, June 2009..

Lee L. T. and Tsang K.F., "An active RFID system for railway vehicle identification and positioning", International Conference on Railway Engeering(ICRE 2008), pp.1-4, 2008.

Lionel M. Ni and Yunhao L, "LANDMARC: Indoor Location Sensing Using Active RFID". Wireless Networks 10, 701?710, 2004 Kluwer Academic Publishers. Manufactured in The Netherlands.

Matthias S, et al., ERTICO ? ITS Europe, Tanja Kessel, EICT, "Preventive and Active Safety Applications Integrated Project". eSafety for road and air transport report.

Samuel S. Gould, "How Auto-Identification and Data Collection (AIDC) is Transforming in the RFID" World Manufacturing Advantage Conference May 21, 2008.

Song Z. and Z. Qiu, "The application of UHF RFID technology in mine locomotive positioning system", IT in Medicine and Education 2008(ITME2008) IEEE, pp.1079-1082, 2008.

Takashi K, J Nishiyama, H Sugahara, T Okada, F Yamato and M Matsumoto, "A Railway Signal Control System by Optical LAN and Design Simplification", Journal of Networks (JNW) VoL3 NO7, pp.8-15, 2008.

Takenori W., K. Bekki and Y. Yokosuka, "Leading-Edge Solutions for Next-Generation Railway Systems" Journal of Hitachi Hyoron Vol87No9, pp.699-704, 2005.

Yoshimichi S and Koji M,"Development and Evaluation of In-vehicle Signing System Utilizing RFID tags as Digital Traffic Signs" International Journal of ITS Research, Vol. 4, No.1, December 2006.

Sustainable Radio Frequency Identification Solutions

Edited by Cristina Turcu

Radio frequency identification (RFID) is a fascinating, fast developing and multidisciplinary domain with emerging technologies and applications. It is characterized by a variety of research topics, analytical methods, models, protocols, design principles and processing software. With a relatively large range of applications, RFID enjoys extensive investor confidence and is poised for growth. A number of RFID applications proposed or already used in technical and scientific fields are described in this book. Sustainable Radio Frequency Identification Solutions comprises 19 chapters written by RFID experts from all over the world. In investigating RFID solutions experts reveal some of the real-life issues and challenges in implementing RFID.

How to reference

In order to correctly reference this scholarly work, feel free to copy and paste the following:

Krishan Sabaragamu Koralalage, Noriaki Yoshiura, and Takaomi Shigehara (2010). Beyond Identification: Representing Real World Objects and Actors in Radio Frequency Identification, Sustainable Radio Frequency Identification Solutions, Cristina Turcu (Ed.), ISBN: 978-953-7619-74-9, InTech, Available from: http://www.intechopen.com/books/sustainable-radio-frequency-identification-solutions/beyond-identification-representing-real-world-objects-and-actors-in-radio-frequency-identification

INTECH
open science | open minds