An Integrated Multi-level Security Model for Malicious Attacks Resiliency in Vehicular Ad hoc Network (VANET)

ISSN (e) 2520-7393
ISSN (p) 2521-5027
Received on 25th Sept, 2017
Revised on 4th Oct, 2017
www.estirj.com

Irshad Ahmed Sumra[1], P.Sellappan[2], Azween Abdullah[3]

Department of Information Technology
Malaysia University of Science and Technology (MUST), Malaysia

Abstract: Road accident and traffic congestion are global issues faced by many countries around the world. Road accident led to fatalities and injuries, while traffic congestion led to inconvenient driving and fuel energy wastage. Vehicular Ad hoc Network (VANET), as part of Intelligent Transportation System (ITS), has the ability to provide safety and non-safety applications to users on roads for safe, reliable and comfort driving. In this paper, propose an integrated multi-level Security model and core purpose of this model is to provide the resiliency against malicious attack and aim to reduce incidents of road accidents, as well as to ease traffic congestions.

Keywords: *Intelligent Transportation System (ITS), Security, Multi-level integrated model, malicious attacks.*

1. Introduction

Road accident is one of the most common threats to human lives that has led to partial or complete disability and in many cases, resulted in death. In the United States of America alone, more than six million road accidents occurred and approximately more than 2.5 million people are reported to be seriously injured. Consequently, a loss of 40,000 lives and more than 2 million physical injuries from car accidents has been recorded every year [1]. The increase in reported figures in the past few years has alarmed government organizations and researchers to find effective solutions to decrease, and if possible, to prevent accidents in the future. It is extrapolated that failure to do so will place road accident as the third most serious threat to human life by 2020 [2]. One of the side effects of road accidents is traffic jams that in return results in wastage of time, fuel and effort of road users. Intelligent Transportation System (ITS) [3] is one of the technologies that has the potential to improve traffic systems by sending safety and non-safety information via Roadside-Infrastructure to Vehicle Communication (RVC) to users on highways [4]. However, while ITS offers many benefits to road users, its deployment for traffic management is still very expensive, especially in rural areas where the number of vehicles are less compared to urban traffic density.

The active social networker follows both companies and other people. However, the majority of the tweets are conversational messages between people. The third group, inactive social networkers, are not interested in the two-way communication aspect available on twitter, but as an information gathering resource. Regardless of which group the twitter user falls, the objective is to filter the abundance of available information into a manageable and customizable information stream. Twitter data collection has traditionally involved downloading user profiles individually and then partitioning them using community detection algorithms [4]; however, due to the time-consuming nature of this task, more real-time node-crawling and community structure building approaches have emerged [8] to effectively filter relevant tweets. Given the twitter's popularity, airline companies have created individual profiles to reach their customer base for a variety of reasons. In many cases, airlines use twitter as another marketing and sales conduit. In providing customer service, airlines use twitter for flight status update during a significant weather event.

We study how prevalent flight-related data is available on twitter in order to determine a commercial airline's quality of service to its customers in a significant weather event. We can then assess if twitter is a valuable communication network for air passengers and their travel needs. Vehicular Ad hoc Network (VANET) is a sub-class of Mobile Ad hoc Network (MANET) and is considered a promising approach for future ITS[12,13]. VANET monitors directly the vehicular traffic problems using its safety and non-safety applications. These applications prevent road accidents and make travel more comfortable by generating various warning messages and infotainment. Basically, VANET comprises of two types of wireless communications: Vehicle-to-Vehicle (V2V) and Vehicle-to-Roadside Unit (V2R) [5]. In addition, Dedicate Short Range Communication (DSRC) is a frequency band that supports all types of wireless communications between the V2V and V2R. VANETs have no fixed infrastructure and strongly rely on the vehicles themselves, for providing mutual communication network functionalities for vehicles on the road, i.e. network-on-the-fly [6]. Security is one of the key network requirements in VANET environment considering that if VANET is not secure from attackers, potential applications of VANET may not achieve its primary purpose to save human lives [7,8]. Through these applications, the safety of road user is improved through exchanging safety information in V2V and V2R *communications*. The safety applications may be at risk if

Corresponding Author Email Address: isomro28@gmail.com

the maximum level of secure communication is not obtained and provided to road users. For example, the Extended Brakes Light (EBL) application [9,10] and road-condition warning messages need to be securely communicated; otherwise an attacker may generate falsified warning messages and create problems for other users on the road.

This paper is divided into six sections: Section 2 describes the related work in the field of security in VANET. Section 3, discuss in detail the propose an Integrated multi-level Security model in VANET. The propose model has been divided into different levels and purpose of the levels to provide the resiliency against the malicious attacks in vehicular network. Sections 4 is the core module of the paper and explain the relationship of malicious attack with trust and propose the trust model and divide the trust model into different components. The Result and Discussion describe in Section 5 and the conclusion of the paper in last part of the paper in Section 6.

2. Related Work

M. Gerlach et al. [10] suggested a model for trusted applications for VANET. They described a situation where the characteristics of trust pertained to the trustee. The authors mentioned three key contributions which are given below.

- They proposed a security architecture that is integrated with various security measurements in vehicular environments.
- They proposed a trusted model for applications in VANET by utilizing the trust tagging principle.
- They proposed the idea of mixed content and defined the manner by which pseudonyms can be changed which prevents location tracking.

P. Wex et al. [14] discussed some issues of trust in vehicular networks. The general belief is that every component in a vehicular environment possesses its own system of trust which can make decisions about which components can be trusted. Below are the two basic options for establishing trust.

- Statically: By the static dependence on a security infrastructure.
- Dynamically: By the dynamic build up of trust in a way that is self-organizing.
  - Infrastructure-based Trust Establishment: there are various methods used to establish infrastructure-based trust. In principle, Infrastructure based Trust Establishment utilizes certificates to build this trust and is static over time.
  - Self-organizing Trust Establishment: VANET is very dynamic, and hence needs a style of trust establishment that is very adaptable, i.e., decisions related to the trustworthiness of other components must be autonomous; due to that fact, there is no possible connection to an online security infrastructure.

C. Jingwen et al. [15] proposed a trusted routing framework, which allowed authentication of messages, establishment of node to node trust and verification of routability, without the need for online Certificate Authorities (CAs). This particular method prevents identity impersonation, which suggests that links are available if they are false, and some other specific invalid routing protocol actions.

D. Huang et al. [16] proposed a trust architecture and a model called Situation-Aware Trust (SAT). This model deals with several important trust concerns present in vehicular networks and there are following contributions:-

- They proposed an efficient policy management for a wide variety of situations by utilizing cryptographic solutions, which are based on descriptive attributes.
- They proposed both off-line and on-line trust policies and requirements which are built for pro-action and prediction of future trust situations.
- They transformed the trust established in Internet social communities to VANET for the enhancement and promotion of VANET applications.

A data-trust security model was proposed in [17] and also designed theories for a social network in vehicular networks. A trust index for each message based on the relevance of the event was calculated by the proposed model. The contributions are given below:

- A solution to the security problems was proposed and it would make use of the theories of the social network.
- The proposed solution was evaluated by modelling and simulation.
- Claimed that the data trust security model had successfully prevented attacks (message alteration) in VANET.

Marmol et al. [18] presented the original proposal for trust and reputation which is called Trust and reputation infrastructure based proposal (TRIP) for VANETs. The main objective is to quickly and accurately distinguish malicious nodes spreading false or bogus messages throughout the network. The author described the three trust levels which are given below.

- Not Trust: If the targeting node is placed in the first level of trust in the network then its warning is discarded. The infrastructure is informed about the presence of a malicious node in the network and other node in the network.
- Trust: When traffic warning message is accepted and also retransmitted to the neighbouring nodes then if it is placed in the trust level called ‘‘Trust’’.
- ‘‘+/- Trust’’: When a message is accepted as reliable with a certain tunable probability, but this message is not forwarded to other nodes of the network, then targeting vehicle is placed in the trust level labeled as ‘‘+/- Trust’’.

3. Propose Integrated Multi-level Security Model

User is the main component of the vehicular networks and the main goal of this modern technology is to prevent them from road accidents and to provide better services to road users. It was studied that safety and reliability are key requirements of VANET users. The presence of security problem in VANET compromises the end users' safety on roads. Additionally, inexistence of trust and privacy may lead to non-trusted communications links between VANET's components. Keeping in view of these challenging issues, it is observed from literature review that an inter-related Security-Trust-Privacy (STP) model is important to consider for mitigating the overall safety and reliability problem in top down approach. Therefore, it is aimed to propose an integrated model that consists of Security, Trust and Privacy modules. Traditionally, Security remains an important issue for all types of conventional and next generation networks like VANET. The deployment of new applications raises many questions about the requirements for security in VANET. The vehicles possess high mobility on road and caused the change in network topology dynamically. The presence of this dynamic behavior of network, which is based on wireless medium, brings many possibilities for attackers to attack on the components of VANET. Figure.1.describes the different component of intergraded multi-level of security in VANET.

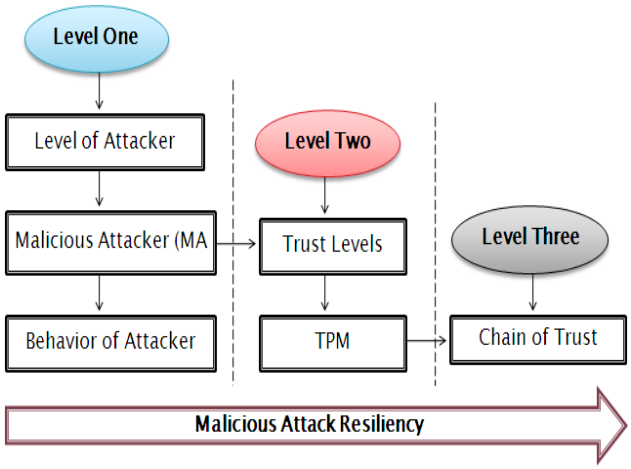

Figure.1. Integrated Multi-level Security Model

Level One: Attacker is one of the type of user in VANET and this component of the network is play key role while communication other component of the network. All possible attackers have been divided into three different levels on the basic of their threat levels and their priorities and this is the first step to deal with attacker in VANET. Malicious attacker is one of the types of attacker and their threat level is high as compare to other attacker users in network. Behavior of attacker user in network is directly affecting all component of network. It is necessary to define key features that differentiate the normal user behavior and attacker user behavior in network. Time interval, location and speed of the vehicle are key proposed features (parameters) which describe the behavior of attacker user in network.

Level Two: Trust and malicious attacker: Three Trust levels have been proposed and it has been showed the relationship of attacker with trust and how trust level is vary in different time interval and different locations in network. VANET trust model also proposed which describe the relationship of trust and attacks in the form of accuracy. Whenever attacker launch more attacks in network then network accuracy are decreases and it shows the role of attackers their effects on network.

Level Three: TPM based Chain of Trust (CoT): TPM is trusted security hardware module and it is provided the chain of trust mechanism between user and smart vehicle also provide the resiliency from malicious attacker and attacks in network.

The Figure 2. describes the resiliency measures with respect to security in VANET. The basic purpose of these measures to provides the resiliency from malicious attack on security in network. Behavior of attacker is dynamic thing and it is changes in different time interval and also location of the network. The speeds of vehicle, location of vehicle and time interval of message are key parameters to describe the behavior of attacker in network. Trust is part of security and it has direct relationship with malicious attack and trust level increases and decreases due to the malicious behavior of attacker. Zero trust, weak trust and strong trust are three different types of trust levels in VANET. TPM provides the chain of trust and provide resiliency from malicious attacker and attack.

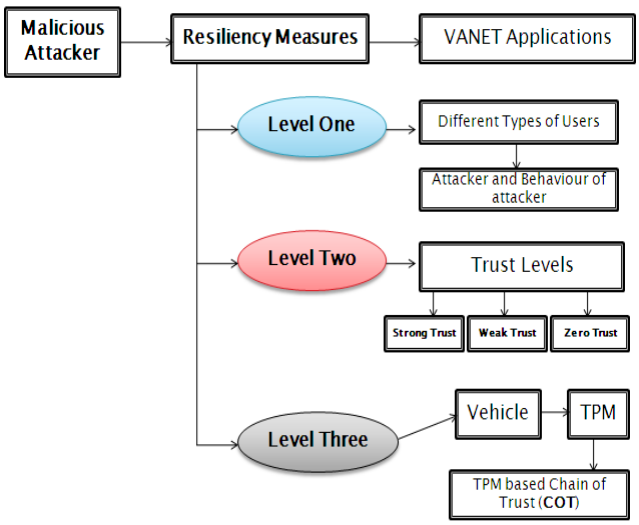

Figure.2. Resiliency measures in integrated Security model

4. Malicious Attacker and Vehicular Trust Model (VTM)

In this research work, a Vehicular Trust Model (VTM) has been proposed and VTM is part of multi-level security model. The VTM is divided into two parts which is given below.

- First part of the model is based on three trust levels whereby attackers and attacks are directly related to trust levels (trust grades).
- Second part of the model is based on TPM and it is used to establish chain of trust between components of the network and handle the attackers and attacks in network.

In this section, provides the detail description of three trust levels and their relationship between attackers and attacks. An attacker (malicious user) disrupts a network through different kinds of attacks and the level of trust depends on the nature of attacks. The accuracy of a network is increased when more connections are established between the vehicles in the network.

4.1 Trust Levels

The following describes three types of users in the proposed trust model and discusses in detail how trust levels are affected due to the behavior of malicious users and attacks in the vehicular network.

4.1.1 Zero Trusted User:

These types of users are part of the network but due to DoS attack, they are unable to access any services from the network. Channel jam is one type of DoS attack. In this attack, high frequency signals are sent out by the attacker that causes the communication channel between vehicles to be jammed. As a result, the vehicles are unable to send or receive safety or non-safety messages in the network. No services are available in that particular domain because of this attack and only upon leaving that domain, will they start to receive the messages. These users are assigned zero grades (0) and their recommendation is also zero.

4.1.2 Weak Trusted User:

Every vehicle has the ability to send or receive communication packets in V2V or V2R communication in a network. In this type, the use just sends communication packets in the network but could not receive any packets from other vehicles or from the RSU; however, the user remains part of the network. The user can also receive packets but however due to DoS attack, he/she is unable to communicate with other users. Grade (1) is assigned for such users and their recommendation level is (one) in the network.

- **Drop communication packet:** This is a feature related to the malicious behavior of attackers, where an attacker just drops communication packets; the goal of the attacker is to make sure that users are unable to communicate in the network through any means possible.
- **Overwhelm network resource**: In this attack, the attacker aims to overwhelm the resources of another user's vehicle in order to hinder its performance of other necessary tasks. The vehicle's network becomes overly busy in accessing the signals and this uses up all of its resources in trying to verify the messages.

4.1.3 Strong Trusted User:

Strong trust users are users who have the capability in performing all tasks (send/receive) in a network. Strong trust users have a strong recommendation level (Two) in the network and are an ideal user of the network.

Network Accuracy (AC)= $\sum_{i=0}^{n}(LT) + (Rh)$

Level of Trust

$$(\text{LT})=\left[\frac{-k(n+1)}{2}+1\right]L_0+\frac{1}{2}(K-n)L_2 \qquad \text{eq.(a)}$$

$$LT=\frac{K}{2}(AC)$$

Where, k is proportionality constant i.e $k \in [0,2]$

$$n=\begin{Bmatrix}1 & at & k=1\\ 0 & (k=0) & (k=2)\end{Bmatrix}$$

The equation (a). explains the relationship of trust levels with accuracy. More importantly, network accuracy is combination of level of trust and recommendation. Recommendation is based on number of hops in network. Whenever user have more trust level in network (strong level) then increase the number of hops. As long as there is strong trust between all components of the network and there is no attacker, then the maximum level of accuracy is achieved. As alternatively, the level of trust changes in the presence of an attacker and accuracy in the network changes as well.

4.2 Chain of Trust (COT)

Vehicular Chain of Trust (CoT) is second part of the proposed VTM model. In the proposed vehicular CoT environment, each vehicle possess a trusted hardware module (TPM) inside the smart vehicle. In concept, Vehicular CoT is built on a combination of many Trusted Modules. The CoT is able to convey life critical information in a more secure and trusted manner. There are following component of proposed vehicular Chain of Trust (CoT).

1. Trust Inside TPM
2. Trust between TPM and embedded Smart Vehicle Sensors
3. Trust between Vehicle to Vehicle (V2V)
4. Trust between Vehicle to RSU (V2R)

4.2.1 Trust Inside TPM

Trust Platform Module (TPM) is the first component of the chain of trust in VANET. Whenever vehicles start communication, first Trust Platform Module (TPM) measures the trust condition of its platform and this measurement is known as "internal trust" and then passes trusted information to TPM. Internal trust of TPM is actually based on root of trust mechanism which are reside the inside of the TPM and ensure the security of platform. Root of Trust (RoT) consists of Root of Trust for Measurement (RTM), Root of Trust for Reporting (RTR), Root of Trust for Storage (RTS). The Figure. 3. shows the relationship of TPM with smart vehicle and also with Root of Trust (RoT).

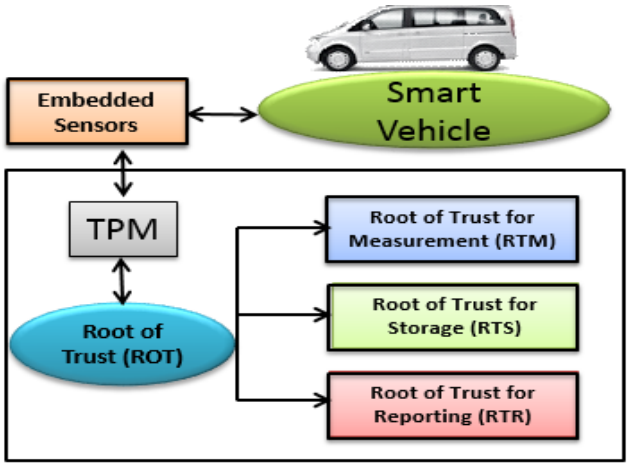

Figure.3. TPM with Root of Trust modules

4.2.2 Trust between TPM and Vehicle Sensors

At first level, TPM communicates with inside sensors of vehicle. The vehicle TPM wants to make sure those specific sensors within the vehicle communicates securely. Trusted vehicles are different from normal vehicles because of their functional components such as many types of embedded sensors and processing units inside these vehicles and its communication abilities. Global Position System (GPS), Radar Systems (RSs) and Communication Facility (CF) are these modules which are used inside the vehicle. It is the responsibility of TPM to communicate with these modules and to build the web of trust within the trusted vehicles. Figure 4. explains the process mechanism of from OBU to sensors and from sensors to OBU. In this whole process the TPM play a key role for developing the trust. At every level TPM check the right functionality of sensors, hardware, software and application.

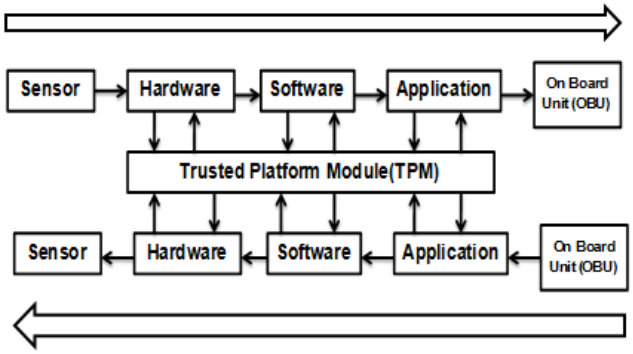

Figure.4. Trust from sensor to OBU and OBU to sensor

4.2.3 Trust between Vehicle to Vehicle (V2V)

When users receive any message (Safety or Non Safety) from other vehicles or from infrastructure, it should be trusted because users react according to the message. To establish the trust, it is required to provide trust between the users in V2V and V2R communication. The attackers try to change the contents of the message and break the trust between the vehicles. The Figure 5. explains third level peer to peer trust in vehicular communication. Third level trust depends on the first and second level chain of trust. For example, a trusted vehicle A communicates and does mutual attestation with vehicle B. Now that vehicle B becomes trusted and it does mutual attestation with vehicle C and so on. Finally peer to peer trust between vehicles makes a chain of trust in the network.

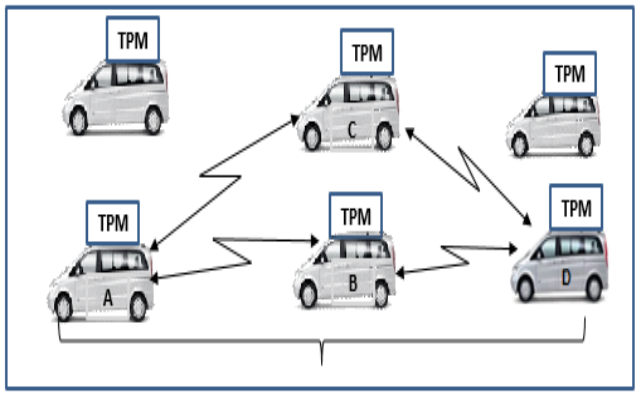

Figure 5. Chain of Trust between smart vehicles

Trust calculation from vehicles A to vehicle D using subjective logic.

$$W^{A}{}_{D} = (W^{A}{}_{B} \otimes W^{B}{}_{D}) \oplus (W^{A}{}_{C} \otimes W^{C}{}_{D})$$

$$[A,D] = ([A, B]: [B, D]) \diamond ([A, C] : [C, D])$$

The core purpose of TPM based chain of trust is to resist the attackers and attacks and ensure the secure the communication. There are following two cases provided the detail description of normal communication and attacker communication and solutions of attacks through TPM.

Case One (TPM with Normal User) : Whenever vehicle is secure through TPM, so now it is possible to communicate with other vehicle or with infrastructure. There are two content of the message of one message i-e security content (valid security key and signature), other contents includes vehicle ID, location of vehicle and speed of vehicle and message generation time. All parameters of any message are an important while start the communication in network. Figure 6, shows the communication through step by step process approach while start the communication in network.

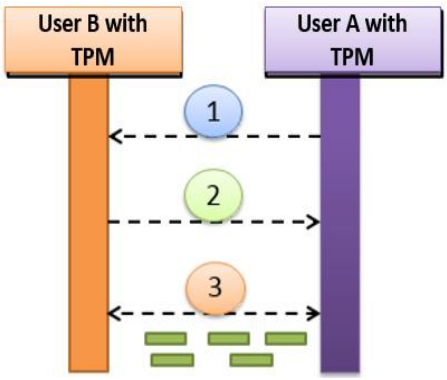

Figure 6. User A communication with other user B

Steps:

1. User A send HELLO message (MSG) to user B and this message sign with valid key i-e

Attestation Identity Key (AIK) and also attach signature.

Msg (vehicle ID, Time, location, Speed, Key (Aik), signature)

2. User B checks the valid security key, signature and also other content of the message.
3. If user have valid key, signature and also other parameters of the message then start communication with user B.

Case Two (TPM with Attacker User) : In this case an attacker communicate with RUS and want to alter the signal time slot. But TPM has responsibility to identify and stop their communication in network. The Figure 7 provides the detail description of case two.

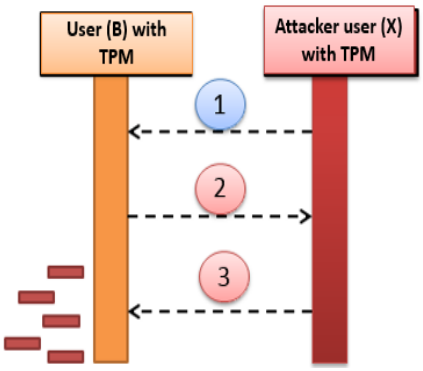

Figure 7. Comm. between attacker user and normal user

Steps:

1. In this case, attacker user (x) want to start communication with other vehicle B in network. So, malicious user send hello message to vehicle B
2. User B check their contents of the message, but their security key is not valid, this is one of the reason that to identify the attackers in network. The second reason is their key is valid but their location is not specific.
3. So, in both reasons either security key is not valid or location of the vehicle is not specific, it should consider as an attacker and drop their communication packets.

4.2.4 Trust between Vehicles to RSU (V2R)

The objective of trusted infrastructure is to ensure the availability of the network and provide secure communication in the network. We can extend the web of trust from vehicle to infrastructure so that availability is ensured. The role of infrastructure is important to verify the vehicles and provide information related to safety and non-safety applications. It is necessary for a vehicle to have TPM so that it communicates with RSU (infrastructure) and to build the trust with it. Figure 8 explains the indirect trust between the vehicles to infrastructure. Vehicle A has done mutual attestation with RSU (infrastructure) and which then do mutual attestation with vehicle E in the network. In doing so, vehicle E is making trust indirectly via the infrastructure and establishes trust with vehicle E. Hence, another kind of trust in infrastructure has been established from vehicle E to Infrastructure.

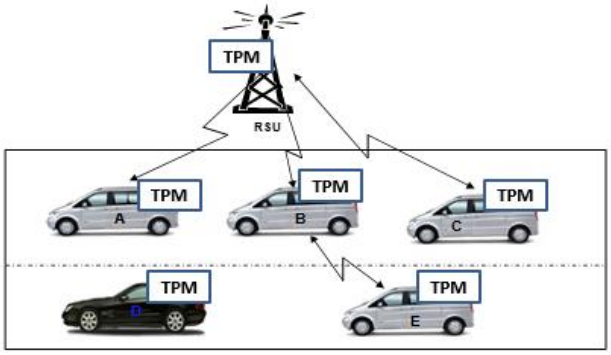

Figure 8. Chain of Trust between vehicle to RSU

Case One (Communication with TPM User) : In this case, user (A) start communication with RSU and take the internet services while travelling on highway. There are following steps involve to start the communication between normal user and RSU. Figure 9 explain the communication mechanism between user and RSU in vehicular network.

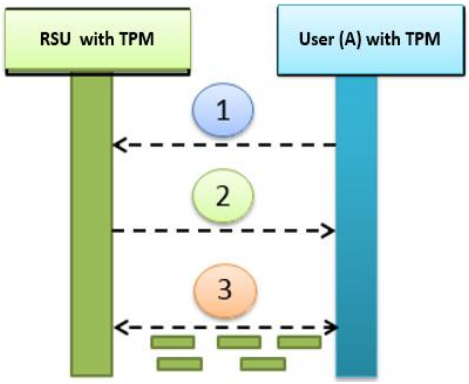

Figure .9 User (A) communication with RSU

Steps:

1. User (A) send message (MSG) to RSU and this message contain all users' information with security TPM key.
2. RSU check the user information and if information is valid and meet the RSU requirement then it is allow to take services from RSU.
3. After user verification, start the communications between user (A) and RSU.

Case Two (Communication with Attacker User) :

In this case an attacker user (X) communicate with RSU and want to lunch attack on RSU. Objective of the attacker is to down roadside unit (RSU) and their services for other user of the network. Through TPM, we can handle this attacks and drop their packets while they are launching this such of attacks on RSU. Figure 10. provides the detail description of case two.

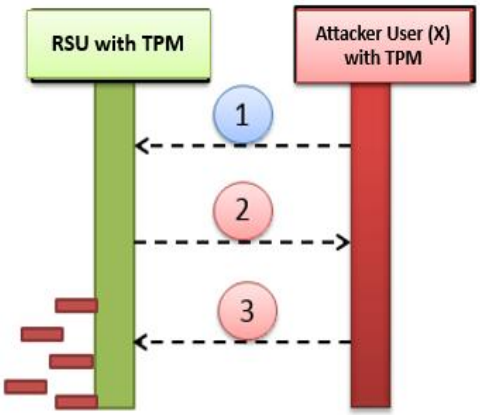

Figure. 10 Attacker user (X) communication with RSU

Chain of Trust Process: Attestation identity key (AiK) is key parameter of TPM and it play a key role to develop the chain of trust in network. Attestation is a process of vouching for the accuracy of information, and this is the feature trusting computing to assurance the endpoint trust. Attestation is provided the guarantee two long distance participant by using of identity authenticity and configuration integrity. TPM is provided many types of keys but for attestation purpose they are using Attestation Identity Key (AiK). AIK sign the applications and these applications communicating with other vehicle (V2V) and also with infrastructure (RSU). AiK is used as an alias of the endorsement key (EK) and Endorsement Key (EK) is a fundamental component of TPM and it must have an endorsement key pair, in this pair private key is more important and embedded in it. AiK is generated by the owner of TPM and it is non-migratable singing key and multiple AiK can be generated by TPM. Figure 11 shows the key generation and sign process between vehicle to vehicle and vehicle to RSU.

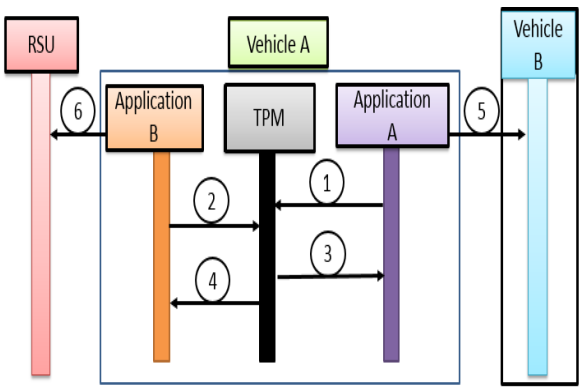

Figure 11. Chain of Trust comm. between V2V and V2R

Steps:

- Step 1 - Application A send request to TPM by signing the message using singing keys. Contents of the data can be different, its may be safety message of non-safety of the vehicle applications. One more thing is also attach with the data that is time and date of the message. When other vehicle received this message, it will be verified with their keys and time and date are extra contents that are used for security reason. Attacker may be change the time or date of the message. So it would be easy for other vehicle to check these two parameters.
- Step 2 - Application B also send request same request to TPM. In one vehicle it is possible multiples applications could be running and also used different keys for signing the data.
- Steps (3, 4) - TPM send message to application A with contents of certificate, this certificate is encrypt with AIK and AIK is encrypt with PCA.
- Steps (5, 6) - Finally message (MS1) send from application A to other vehicle (B) in the network its kind of vehicle to vehicle communication. Application B message (MS2) sends this message to road side unit (RSU).

5. Results and Discussion

TRMSim-WSN [122, 123] is the first trust and reputation tool which has provided proper environment in developing their own trust model for VANET. TRMSim-WSN provides the trusted and none-trusted nodes (malicious users) in the network. Both nodes have their own trust levels (grades) and non-trusted nodes affect the degree of trust in the network. Simulation was used to show how a malicious user decreases the level of trust in a network and in turn, decreases the network accuracy.

5.1 Chain of Trust (CoT) with number of Malicious Users (MUs)

TPM is core trusted module which is used inside the smart vehicle in VANET. TPM is providing key strong key structure mechanism to develop the chain of trust in VANET. Attestation identify key(AiK) one of the key which is used to attest the user while communication in network.MU is also part of network and the core objective of TPM is resist the MU in network and establish trust between user of network. TPM develop the chain of trust (COT) in VANET through attestation identity key (AiK) and COT is improve the accuracy of network. TPM is resist the MU and built the COT and when it will develop the chain of trust then also improve the accuracy of the network. So, here we will check the accuracy with different number of users in proposed model and check how chain of trust is improving the accuracy in existing MUs in network. It is also provides the detail description and the relationship of accuracy with malicious users (MUs) of three different models with different delay values and 5 meter (m) communication range. Table 4.4 show the list of simulation parameters which are used in different scenarios.

Table. I: Simulation Parameters

No.	Simulation Parameter	Parameter description
01	Number of Executions	20
03	Simulation Area	500 x 500
04	Communication Radio Range (Fixed)	5 meters (m)
05	First Scenario – Number of Nodes	50
06	Second Scenario- Number of Nodes	100
07	Third Scenario - Number of Nodes	150
06	Number of Malicious Users (%)	10, 20, 30, 40,50

First Scenario - 50 Nodes: In this scenario, total number of nodes is only 50 with 5 meters (m) communication range in network and when number of malicious user gradually increases then values of accuracy is decreases in network. The Figure 12 describes the whole scenario in which network accuracy is explain in both models on number of malicious users. When number of MUs is only 10% then accuracy of COT is 95% and at the same time TRIP provides 85% accuracy in network. The value of accuracy is gradually decreases when ratio of MU is increases in network and 72% accuracy is achieved in COT model and 65% accuracy value is received when number of malicious user are 50% in network. There is clear differences in accuracy values from 10% MUs to 50% MUs in network for both models. Finally, COT is achieve maximum accuracy also in network when MUs reached on 50%.

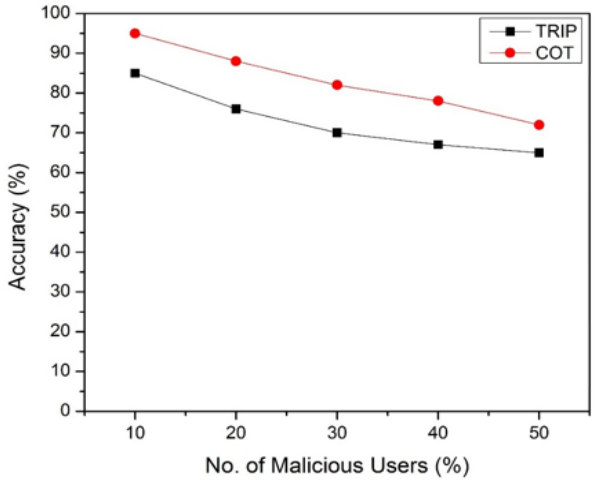

Figure 12: network accuracy with 50 nodes

Second Scenario - 100 Nodes: In this second scenario, the numbers of communication nodes are 150 and percentage of MU is same from 10% to 50% of total number of nodes in network. The Figure 13 describes the complete scenario and also shows the relationship of MU with accuracy in two different models in VANET. The network accuracy of COT model is 90% at 10% of MU and the same time the TRIP provides 78% accuracy at 10% of MU in network. But when increases the ratio of MU in network then gradually decreases the level of accuracy. The value of accuracy is reaches on 60% in TRIP model at 50% MUs and at the same time the accuracy of COT model is reached on 68% and graph of accuracy is slightly decreases in both model when increases the ratio of MUs in network.

Third Scenario – 150 Nodes: In this third scenario, the numbers of communication nodes are 150 and percentage of MU is remaining in first and second scenario which is 10% to 50% of total number of nodes in network. The Figure 14 describe the complete scenario and also show the relationship of MU with accuracy in two different models in VANET. The accuracy of network in COT model is more than 85% at 10% of MU and the same time the TRIP accuracy is 75 % at 10% of MU in network. But when increases the ratio of MU in network then gradually decreases the level of accuracy. The accuracy values is reaches on 55% in TRIP model at 50% MUs and at the same time the accuracy of COT model is reached on 65% and graph of accuracy is decreases in both model as compare to first and second scenarios.

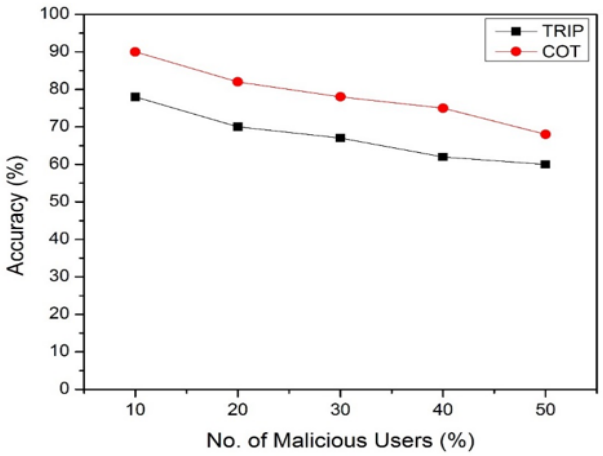

Figure 13: network accuracy with 100 nodes

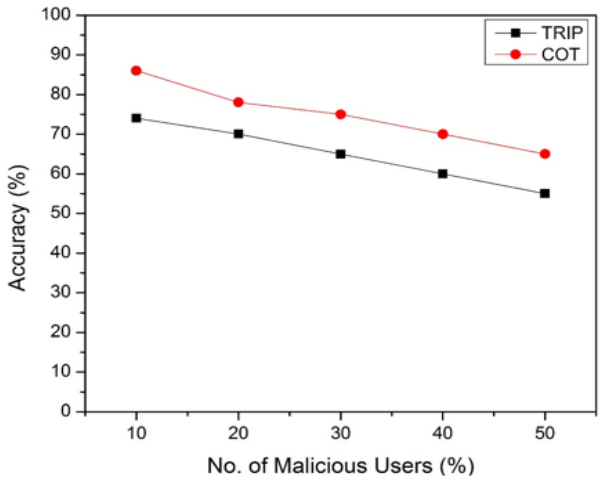

Figure 14: network accuracy with 150 nodes

Malicious User (MUs) with Communication Delay: In this section, we will check the accuracy of proposed and other model with different number of users with different communication delay values in network. Table II is providing the simulation parameters for different scenarios to check the network accuracy.

Table.II. Simulation Parameters

No.	Simulation Parameter	Parameter description
01	Number of Executions	20
02	Maximum number of nodes	100,150
03	Simulation Area	500 x 500
04	Communication Radio Range (Fixed)	5 meters (m)
05	First Scenario	5 ms delay
06	Second Scenario	10 ms delay
07	Third Scenario	15 ms delay
06	Number of Malicious Users (%)	10, 20, 30, 40,50

First Scenario - 05 ms Delay:

In this first scenario, communication delay is describes is only 05ms on 100 and 150 communication nodes with 5 meters (m) communication range in network. Figure 15 describes the complete scenario and also show the relationship of MU with accuracy in two different models in VANET with 5ms communication delay. When number of MUs is only 10% then accuracy of COT is 88% and at the same time TRIP provides 75% accuracy in network. The value of accuracy is gradually decreases when ratio of MU is increases in network and more than 65% accuracy is achieved in COT model and 58% accuracy value is received in TRIP when number of malicious users are 50% in network. The maximum accuracy is achieved in proposed model (COT) as compare to model TRIP in network.

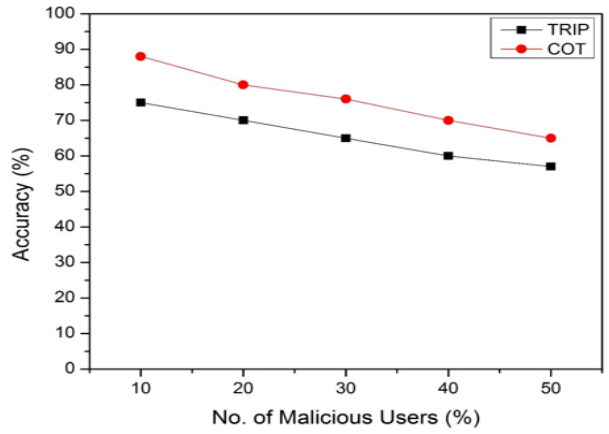

Figure15: Network accuracy on 05ms comm. delay with 100 nodes

The Figure 16 describes also the relationship of accuracy with MUs but as compare to Figure 15, Figure 16 is deal with 150 nodes in network on 5ms delay and 5 meters(m) communication range. The value of accuracy is also decreases on maximum number of users in network. When the number of MUs is only 10% then accuracy of COT is 85% and at the same time TRIP provides 72% accuracy in network. The value of accuracy is gradually decreases when ratio of MU is increases in network and 65% accuracy is achieved in COT model and 55% accuracy value is received in TRIP model when number of malicious user are 50% in network. The results of proposed model (COT) is better as compare to TRIP model with minimum node and also with maximum number of nodes in network.

Second Scenario - 10 ms Delay: In this scenario, the values of accuracy is check on 10ms communication delay for 100 and 150 nodes in network. The Figure 17 describes the complete scenario for 100 nodes on 10 ms delay for models in VANET. When number of MUs is only 10% then accuracy of COT is 85% and at the same time TRIP provides 73% accuracy in network. The value of accuracy is gradually decreases when ratio of MU is increases in network and below 65% accuracy is achieved in COT model and 56 % accuracy value is received when number of malicious user (MUs) are 50% in network. The maximum accuracy is achieved in proposed model (VTM) as compare to other model TRIP.

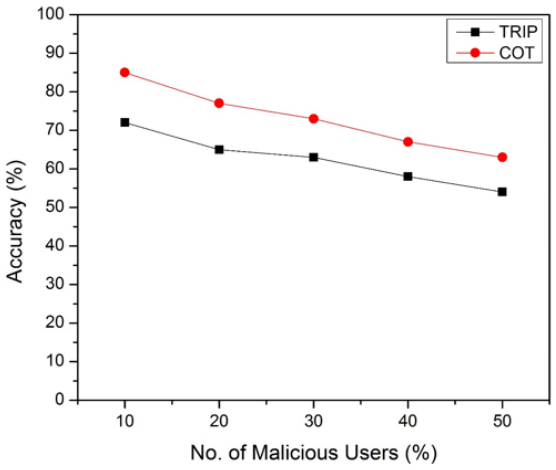

Figure16: network accuracy on 05ms comm.. delay with 150 nodes

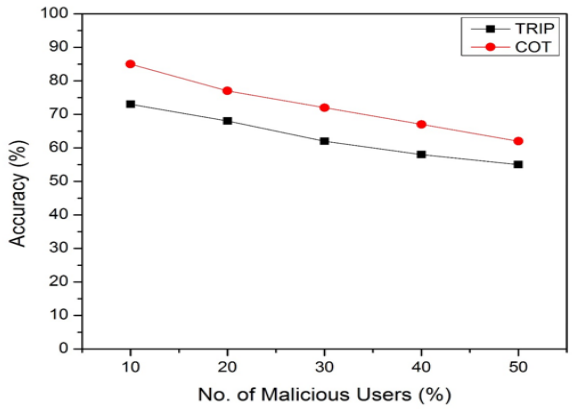

Figure17: Network accuracy on 10ms comm. delay with 100 nodes

The Figure 18 describes the accuracy of network on 150 nodes with 10ms communication delay. When number of MUs is only 10% then accuracy of COT is 83% and at the same time TRIP provides 70% accuracy in network. The value of accuracy is gradually decreases when ratio of MU is increases in network and above 60% accuracy is achieved in COT model and 50% accuracy value is received in TRIP when number of malicious user (MUs) are 50% in network. The Figure 17 shows the better accuracy values of both models as compare to Figure 18 where the communication nodes are 150 as compare to 100 nodes in network. The maximum accuracy is achieved in proposed model COT as compare to other model TRIP.

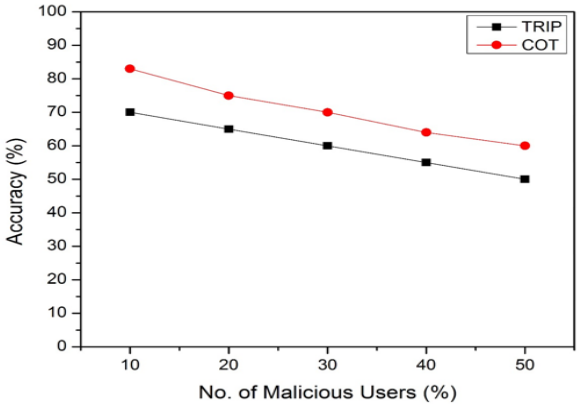

Figure18: Network accuracy on 10ms comm. delay with 150 nodes

Third Scenario - 15 ms Delay: Third scenario describe the maximum delay value (15ms) on both models and also describe the relationship of accuracy on 100 nodes and 150 communication nodes in network. The Figure 19 describes the accuracy of network on 100 nodes with 15ms communication delay. When number of MUs is only 10% then accuracy of COT is 82% and at the same time TRIP provides 70% accuracy in network. The value of accuracy is gradually decreases when the ratio of MU is increases in network and above 60% accuracy is achieved in COT model and above 50% accuracy value is received when number of malicious user (MUs) are 50% in network.

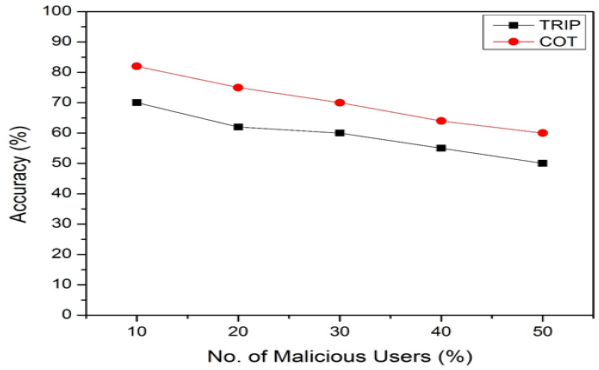

Figure 19: Network accuracy on 15ms communication delay with 100 nodes

The Figure 20 describes the network accuracy on 150 nodes with 15ms communication delay. When number of MUs is only 10% then accuracy of COT is 80% and at the same time TRIP provides 68% accuracy in network. The value of accuracy is gradually decreases when ratio of MU is increases in network and 60% accuracy is achieved in COT model and below 50% accuracy value is received when number of malicious user (MUs) are 50% in network.

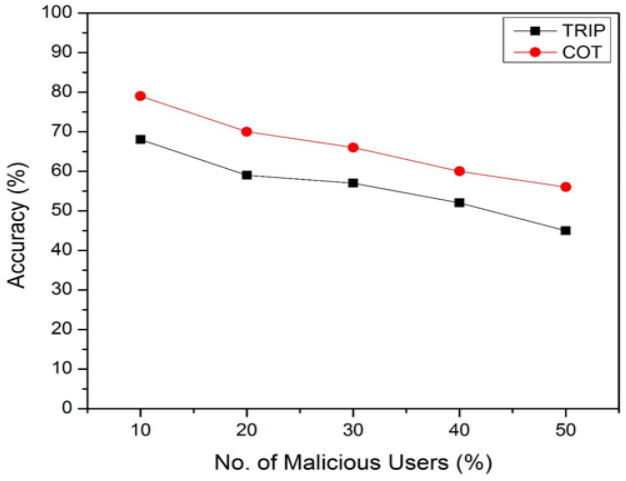

Figure 20: Network accuracy on 15ms comm. delay with 150 nodes

In this section, provides the detail description and the relationship of accuracy with malicious users (MUs) of three different models with different delay values and 5 meter (m) communication range. The comparison of three different models is given below with detail descriptions.

In given scenario, MUs has been increased and then check the accuracy of network with different delay values. One more important thing which discuss here that accuracy of three models has been compare on different delay values with 5 meter (m) communication range. Figure 21 describes the three models with number of malicious users and evaluates the values of accuracy in network. When ratio of MUs is only 10% then the value of accuracy in TRIP model is 75% and this values is gradually decreases and it will reached on 55% when number of malicious user is 50% in network. When the ratio of malicious user is reaches on 90% then TRIP provides only 30% accuracy in network. The VTM model performing better as compare to TRIP model with number of malicious users in network. When the number of malicious user is only 10% then VTM provides 85% accuracy in network and this value will be decreased and reached on 60% and when the ratio of malicious user is 50% in network. This accuracy values is more decreases and reach on 36% when number of malicious users' touches on 90%, but as compare to TRIP model, VTM is provides good accuracy values on high number of malicious users in network. The Accuracy values is reaches on 90% in COT on 10% of MUs and this values is decreases and reach on 65% on 50% MUs and finally accuracy values reached on 42% when the number of malicious users is 90% of total users in network with 5ms delay.

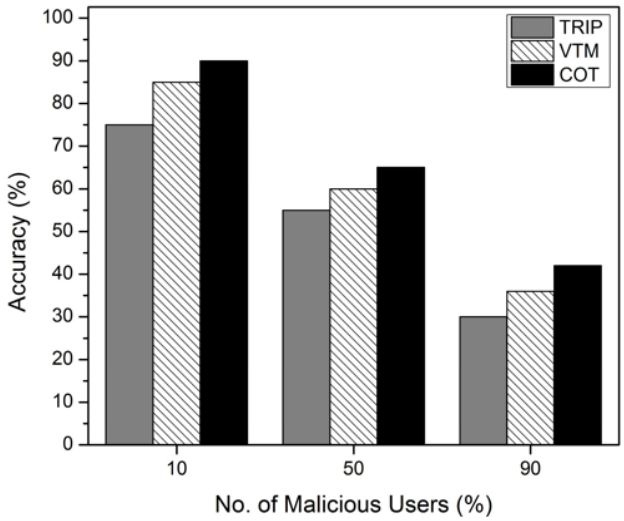

Figure 21: Network accuracy on 5ms communication delay

6. Conclusion

Security is the top level module that is always demanded for safe and reliable VANET communications. However, the dynamic nature of the vehicular network makes it difficult to identify the attackers, attack types and behavior of the attackers. The aim of an attacker is to launch attacks in the network and create problems for other users to achieve their particular goals. Whenever a normal user changes his/her behavior to become an attacker and launches an attack, this attack would create problems for other components of the network and users who utilize that particular component(s). Each attack has its own effect level and it is very hard to identify that particular attack in a particular region of network. So, in this research work, three trust levels were proposed and these trust levels have a direct relationship with attackers and attacks. Whenever the role of an attacker increases in the network, then the degree of trust decreases and network users are affected. The Vehicular trust model (VTM) was developed using the

open source java-based simulator (TRM-WSN). The developed trust model (VTM) was compared with another already available Trust model i.e TRIP and the proposed model showed far better improvement in the accuracy of the network. TPM based chain of trust (COT) model has been developed and it provided the resiliency from malicious attacker and improve the network accuracy.

References

[1] 1. Li, J.C., C., Achieving robust message dissemination in VANET: Challenges and solution. IEEE Intelligent Vehicles Symposium (IV), 2011: p. pp. 845–850.

2. http://www.fiafoundation.org/our-work/road-safety-fund/un-decade-of-action, 2014.

3. Figueiredo, L., et al. Towards the development of intelligent transportation systems. in Intelligent transportation systems. 2001.

4. Hartenstein, H. and K.P. Laberteaux, A tutorial survey on vehicular ad hoc networks. Communications Magazine, IEEE, 2008. 46(6): p. 164-171.

5. Dimitrakopoulos, G. and P. Demestichas, Intelligent transportation systems. Vehicular Technology Magazine, IEEE, 2010. 5(1): p. 77-84.

6. Luo, J. and J.-P. Hubaux, A survey of inter-vehicle communication. 2004.

7. Pathan, A.-S.K., Security of self-organizing networks: MANET, WSN, WMN, VANET. 2010: CRC press.

8. Raya, M., P. Papadimitratos, and J.-P. Hubaux, Securing vehicular communications. IEEE Wireless Communications Magazine, Special Issue on Inter-Vehicular Communications, 2006. 13 (LCA-ARTICLE-2006-015): p. 8-15.

9. Kargl, F., Z. Ma, and E. Schoch, Security engineering for VANETs. Proc. 4th Wksp. Embedded Sec. in Cars, 2006: p. 15-22.

10. Gerlach, M. Trust for vehicular applications. in Autonomous Decentralized Systems, 2007. ISADS'07. Eighth International Symposium on. 2007. IEEE.

11. Guette, G. and C. Bryce, Using tpms to secure vehicular ad-hoc networks (vanets), in Information Security Theory and Practices. Smart Devices, Convergence and Next Generation Networks. 2008, Springer. p. 106-116.

12. Serna, J., J. Luna, and M. Medina. Geolocation-based trust for vanet's privacy. in Information Assurance and Security, 2008. ISIAS'08. Fourth International Conference on. 2008. IEEE.

13. Lin, X., et al., Security in vehicular ad hoc networks. Communications Magazine, IEEE, 2008. 46 (4): p. 88-95.

14 Wex, P., et al. Trust issues for vehicular ad hoc networks. in Vehicular Technology Conference, 2008. VTC Spring 2008. IEEE. 2008. IEEE.

15 Cui, J., Q. Gao, and Y. Liu. A novel trusted routing scheme using attribute similarity for VANET. in Advanced Computer Control (ICACC), 2011 3rd International Conference on. 2011. IEEE.

16 Huang, D., X. Hong, and M. Gerla, Situation-aware trust architecture for vehicular networks. Communications Magazine, IEEE, 2010. 48(11): p. 128-135.

17 Mazilu, S., M. Teler, and C. Dobre. Securing vehicular networks based on data-trust computation. in P2P, Parallel, Grid, Cloud and Internet Computing (3PGCIC), 2011 International Conference on. 2011. IEEE.

18 Mármol, F.G. and G.M. Pérez, TRIP, a trust and reputation infrastructure-based proposal for vehicular ad hoc networks. Journal of Network and Computer Applications, 2012. 35(3): p. 934-941.

About authors

Irshad Ahmed Sumra is PhD candidate in Department of Information Technology Malaysia University of Science and Technology (MUST), Malaysia.

Professor Dr. P. Sellapan is the Provost and Dean of School of Science and Technology at Malaysia University of Science and Technology (MUST). Professor Dr. P. Sellapan has been serving in MUST since 2002. Prior to joining MUST, he was an Associate Professor at the Faculty of Computer Science and Information Technology, University of Malaya. He graduated from the University of Pittsburgh, Pennsylvania with PhD in Interdisciplinary Information Science. Professor Dr. P. Sellapan holds a degree in Economics (Statistics) from University of Malaya, Malaysia and a Master degree in Computer Science from University of London, United Kingdom. He has been actively involved in research and professional services in the areas of Network Communication System, Internet Technology, Computing and Information Technology, Network Security, and Web-based Applications. To date, Professor Dr. P. Sellapan has presented 36 academic papers at both localized and global scientific conferences. Furthermore, he has published 57 peer reviewed articles in profound journals and 16 books on his related topics of interest.

Prof. Dr. Azween Abdullah obtained his bachelor degree in Computer Science in 1985, Master in Software Engineering in 1999 and his Ph.D. in computer science in 2003. B.Sc Computer Science, Master of Software Engineering, PhD in IT (Cybersecurity), Stanford University-Advanced Computer Security Certified Research Scientist, Professor MUST, Taylor's University Malaysia His work experiences includes twenty years in institutions of higher learning in both the management and academic capacities, and fifteen years in commercial companies as Software Developer and Engineer, Systems Analyst and IT/MIS and educational consultancy and training. He has spent more than a decade with leading technology firms and universities as a process analyst, senior systems analyst, project manager, and lecturer. He have participated in and managed several software development projects. These have included the development of management information systems, software process improvement initiatives design and implementation, and several business application projects. His area of research specialization includes computational biology, system survivability and security, autonomic computing and selfhealing and regenerating systems, formal specifications and network modeling. His contributions include publishing several journal and refereed conference papers and in the development of programs to enhance minority involvement in bridging the ICT digital gap. Currently he is working on two projects funded by the Ministry of Science Technology and Innovation.