Fuzzy Logic Based Secured Routing In Vanets

J. Stalin[1], R. S. Rajesh[2]
[1]Research Scholar, Department of Computer Science and Engineering,
Manonmaniam Sundaranar University, Tirunelveli - 627 012, Tamil Nadu, India. E-mail:
maria.jeba.stalin@gmail.com
[2]Professor, Department of Computer Science and Engineering, Manonmaniam Sundaranar University, Tirunelveli - 627 012, Tamil Nadu, India. E-mail: rsrajesh@msuniv.ac.in

Article History: Received: 11 January 2021; Revised: 12 February 2021; Accepted: 27 March 2021; Published online: 10 May 2021

Abstract: Vehicular Adhoc Network (VANET) is becoming a fundamental important component of Intelligent Transport System (ITS). VANET is one of the evolutionary network for providing safety related services, management of traffic and other user related services. VANET communication involves either Vehicle to Infrastructure (V2I) or Vehicle to Vehicle (V2V). In the current scenario, Multi-hop Authenticated Proxy Mobile IP (MA-PMIP) scheme is used in VANET where only 3G networks is considered and the scheme is unable to support transmission of substantial massive data while maintaining the security. The performance of MAPMIP drastically degrades during transmission of huge volume of data which leads to huge power dissipation. To overcome these problems a novel Fuzzy logic Based Secured Routing (FBSR) mechanism is proposed. The FBSR prevents Sink hole attack and Sybil attack. In order to avoid collision during large file transfer, TDMA and multi-threading concepts are introduced in FBSR. Furthermore, the performance of FBSR is compared with contemporary routing protocols OLSR and AODV.

Keywords: VANET; Fuzzy; LTE; Authentication; Routing;5G; Sinkhole attack; Sybil attack; TDMA;

1 Introduction

Intelligent Transportation System (ITS) aims to provide innovative services for vehicular communication. The unique characteristics of VANET are predictable mobility, rapid changing topology, availability of geographic position, variable network density and high computational ability. Due to mobility, the vehicles do not stay longer time in the communication range and the link established for communication has chances to be broken within a short period of time.

In V2V communication, the vehicles collaborate and transfer data with each other without infrastructure. In a V2I communication scenario, road side units, cellular gateways and wireless local area network access points are used as bridge and bind with Internet to allow and enable vehicular applications[1][24].

VANET is used to improve the road safety during vehicle movement by incorporating services such as collision avoidance, co-operative driving, lane change warning, speed limit, intermediate collision warning, traffic optimization, peer to peer application sharing, internet services and other services like collection of toll payment and penalties for traffic violation[2].

The major technical challenges of VANET are network management, collision and congestion control, MAC design, environmental impact and security [2][3][4] [5][24]. During authentication and transmission either between two vehicles (V2V) or infrastructure to vehicle (I2V), privacy must be satisfied to guarantee that the message is not from the unauthorized vehicle[2]. In a VANET, there is also possibility for malicious vehicles entering in to the network, through which it can paralyse the whole network. The attacker may be either internal attacker or external attacker. Security can be provided by Road Side Units (RSU), which acts as Trusted Authority (TA). TA is responsible for authentication of the network and OBU. The outgoing and incoming messages are encrypted and the external attacker can be restricted using cryptographic methods such as digital signature and message authentication. The internal attacker may be one of the network users and can’t be detected easily. From the literature, it is found that few protocols are available for secured routing on VANETs.

Another challenge in VANET is its inability to handle high volume of data [6]. Several works reported in the literature address only the low volume data transfer in 3G data links.

Main motivation behind this research work is that VANET lacks the framework for a full-fledged application that includes security, routing data and transfer of high volume of data such as mobile TV or other multimedia streaming.

In this paper, we have proposed a new method of VANET routing framework that includes the following features to alleviate the problems noticed in other protocols.

(i) Authentication is provided during the communication between the vehicles to safeguard them against various attacks occurring in the network.
(ii) Heterogeneous network which includes LTE/5G network for effective handover in VANET.
(iii) Fuzzy logic based rules are used for effective path selection.
(iv) Time Division Multiple Access (TDMA) with multi-threading for transferring huge volume of data.

The performance of the proposed routing is assessed in the presence of Sybil and Sink Hole attacks. We have conducted an analysis through simulations of the proposed framework. Simulation results show improvements in throughput, packet delivery ratio, average end-to-end delay, communication overhead and authentication delay compared with classical techniques. The paper is organized as follows: Section-2 presents related works carried out to improve the network services. Section-3 describes the proposed framework with tools, techniques and its implementation, Section-4 deals with simulation of the proposed scheme, Section-5 discusses observed results and Section-6 concludes this paper.

2 Related works:

2.1 Routing:

In [7], the authors discussed and classified different kinds of topology and geography based VANET routing protocols. Industry, academicians and researchers show substantial interest to develop a well-organized routing protocol in the VANETs to provide pervasive connectivity and effective vehicle to vehicle and vehicle to road side units to implement ITS in VANETs.

In [8], AODV routing protocol was simulated in WiMAX network environment. Optimized link state routing protocol (OLSR) [9], a proactive routing protocol, which periodically exchanges different messages to maintain the topology information. OLSR uses ‘Hello’ and Topology control (TC) messages. In OLSR, all participating nodes maintain routes to all nodes within the network. The multipoint relay selection plays a pivotal role in OLSR protocol. The selection of relay will be based on ‘Necessity first algorithm’.

In [10][11][12] and [13], the authors proposed a fuzzy based routing protocol which uses either topology or position based information such as co-ordinates of the nodes and velocity of nodes for fuzzy routing. Fuzzy Logic Based Greedy Routing (FLGR) [13] protocol consists of three phases (i) fuzzification (ii) fuzzy interference system and (iii) defuzzification. For fuzzy decision making, two parameters namely the distance from neighbouring node to current forwarding node and position information is taken in to account for each neighbour. Out of two methods available for fuzzy decision (Mamdani and Sugeno), the authors used Mamdani model. It is assumed that source node is away from the destination node and the route to the destination node is through several intermediate nodes. Hence the algorithm identifies the neighbour node which is far away from source node as next hop. In defuzzification step, crisp output is got from ‘Centroid of Area’ (COA). Higher value of COA will give better neighbour node for forwarding the packet. Vehicle mobility is not considered in this approach. Deciding handover points at access points and base stations of the heterogeneous network is proposed in [14]. Four types of differentiated service classes of Wi-Fi are mapped to the five integrated service classes of WiMAX. Bandwidth reservations and admission control at WiFi access points and WiMAX base stations are considered for taking handover decision. Certain percentage of bandwidth is reserved for service classes such as video, audio and back ground data. If the bandwidth is insufficient, the mobile node is not allowed to join access point. Admission control is decided depending upon on available bandwidth and total number of mobile nodes. If the bandwidth of the service class exceeds the threshold, the access point initiates load balancing. The mobile nodes is directed to perform inter base station horizontal handover if possible. If the mobile node could not perform handover, the access point sends the context message through back haul.

2.2 Security:

In [15], the authors discussed various security challenges in VANETs. Frequently, the Sybil attack is caused by creation of fake nodes that broadcasts the false information. Here the vehicle can send multiple copies of messages to other vehicles with different identity. Even in some cases the false information is sent to the vehicles. Attackers purposely send false information to other vehicles. For instance, the attacker can send false information on congestion, accident or road block in order to clear the road from traffic. There is even possibility of the attacker to find the location of the vehicle and track that particular vehicle. A node which creates number of virtual clones of it, for spoofing the other nodes with multiple identities is said to be Sybil attack. This is an act of the malicious node that attracts traffic with multiple identities. With the multiple identities, it can send false messages. Sinkhole attack generally sends fake routing information to the nodes. Malicious node eavesdrops with the aim to collect the data sent from neighbour nodes. Sinkhole attacker node itself advertises that it has a valid shortest route for transmission. It also acts as an attractive relay node in the multi-hop route. This type of attacker nodes may consume the intercepted packets without forwarding and subsequently results in non-availability of network. Various security threats in VANET [3] such as false position information and Sybil attack are discussed. A solution to security is also proposed in which the secret cryptographic information is stored in Tamper Proof Device (TPD). Here authentication is provided by Certificate Authority (CA). By this CA the malicious node's certificate is removed. For revocation of certificates, two protocols namely (1) Revocation protocol using Compressed Certificate Revocation Lists (RCCRL) and (2) Distributed Revocation protocol are used. The false position information is solved by sensor's observation with calculation of threshold. Two types counter measures are discussed in [16]. The first one is a posteriori approach in which punitive actions were taken such as revocation of certificates by the TA. The second one is a priori approach which will prevent the injection of false fraudulent messages. In VANET the packets have the possibility to be corrupted or lost due to channel error and collision.

Key management is another important aspect to be addressed in security. RSU distributes group keys supported by hash key technique [17]. Though the technique provided authentication, the keys are distributed without the verification of vehicle's identity. During handover the maintenance of the security aspects should be ensured. In MA-PMIP scheme [18] is proposed and in this method, secure handover of IP services in VANENTs are studied. Handover messages through V2V paths are authenticated before reaching infrastructure. PMIP has two infrastructures (i) Local Mobility Anchor (LMA) and (ii) Mobile Access Gate way (MAG). MAG detects the new available attachments and detachments based on one-hop communications. In MA-PMIP, Neighbour table is used to select the relay for packet transmission. Default gateway table is for the purpose of handover. In their approach geographical and traffic information (based on Green Shields model) are two parameters considered for predictive fast handover as per RFC5949. Authentication mechanism is provided for handover when I2V2V communication happened. Vehicle moving to a new service area, the messages are sent between the previous MAG and current MAG for establishing a tunnel and forwarding packets to access the current available network. For authentication the keys are generated at the Mobile Router (MR) based on symmetric polynomials. This authentication scheme comprises of three stages namely key establishment part, registration part and authentication part. In first phase keys are generated based on the network polynomials. Secondly in registration phase MR joins with the PMIP domain. As the MR is directly connected with MAG, the MR self-authenticates with MAG. Thus MR stores the identity of the first MAG to which it is attached. Finally, in third stage it keeps up the authentication between the arriving vehicle and the Relay Router (RR). Here security maintenance was effective but traffic condition is not taken in to account and so the load is not balanced effectively.

2.3 Data Transfer:

In Network and Multi resolution coding [19] single multimedia data is segmented into a stream of fixed equal sized frames, the missing pieces are pulled from neighbours and reconstructed using matrix inversion. VIRTUS [20] was deployed for the purpose of video streaming in VANET with the objective of reducing the end-to-end delay, scalability and frequent retransmission. VIRTUS protocol delivers the data packets within a reasonable time frame. To start with, the control packets are sent periodically from source node to destination node for the relay selection process. In this protocol the video streaming is decoupled from the relay selection process. Vehicle density is used as an important parameter in VIRTUS. Nodes in VIRTUS are considered to have three phases such as idle, scheduled and relay. The destination nodes will change into a relay node and requests for video to the source node. The destination keeps the same state till the end of the transmission. The source node also changes to relay node for replying for the video transmission to destination. But this protocol is applicable only for unicast video streaming transmission and not for multicast [21]. Earliest Deadline First based Carrier Sense Multiple Access (EDF-CSMA) scheme [4] is proposed for channel utilization and QoS support in VANETs. The DSRC was comprised of one Control Channel (CCH) and six Service Channels (SCHs). This scheme comprised of two steps namely (i) WAVE Service Group (WSG) configuration and (ii) Multi-channel access mechanism. The function of WSG is to group the nodes in the network which is similar to the process of creating a cluster. In WSG there is single Group Head (GH) and multiple Group Members (GMs). The node which is situated at the centre of WSG that node is elected as GH.

The entire process is executed only for one-hop nodes. GH configures every adjacent node periodically by sending JOIN-INVITE packet and gets back the JOIN-REPLY packets from GMs. After completion of receiving all one-hop nodes reply, the GH broadcasts Media Access Control (MAC) addresses list (MAL) packets to all GMs. With this first step gets completed then the second step is further classified into two phases. The two phases are (i) QoS parameter Collection and (ii) Channel Coordination. In the first phase GM starts to send an initiative Request for Service (RFS) packet to GH. Then the GM receives acknowledgement in response. If all the GM's QoS requirements were completed then the End Of Service (EOS) packets is delivered to GH. Then the second phase uses Carrier Sense Multiple Access/ Collision Avoidance (CSMA/CA) method for channel access where in general CSMA/CA is first listen, speak later policy. But this method is not suitable for multi-hop heterogeneous VANETs. Sections 2.1-2.2 discuss the existing algorithms for routing, security and data transfer in VANETs. In the proposed scheme, fuzzy logic based routing, shared group key with cipher text re-encryption algorithm with respect to security and TDMA with multithreading concept are introduced.

3 Proposed approach: Fuzzy logic based secured routing (FBSR)

3.1 Security and Key management

Data streaming approaches that are based on multi-hop routing in heterogeneous VANET has a wide exposure to attacks. Without the guarantee of complete security and key management, the attackers can tamper the behaviour of the network. In this section a novel framework is proposed to overcome the major issues discussed in Section-1 and 2. The schematic of the proposed scheme is illustrated in Fig. 1.

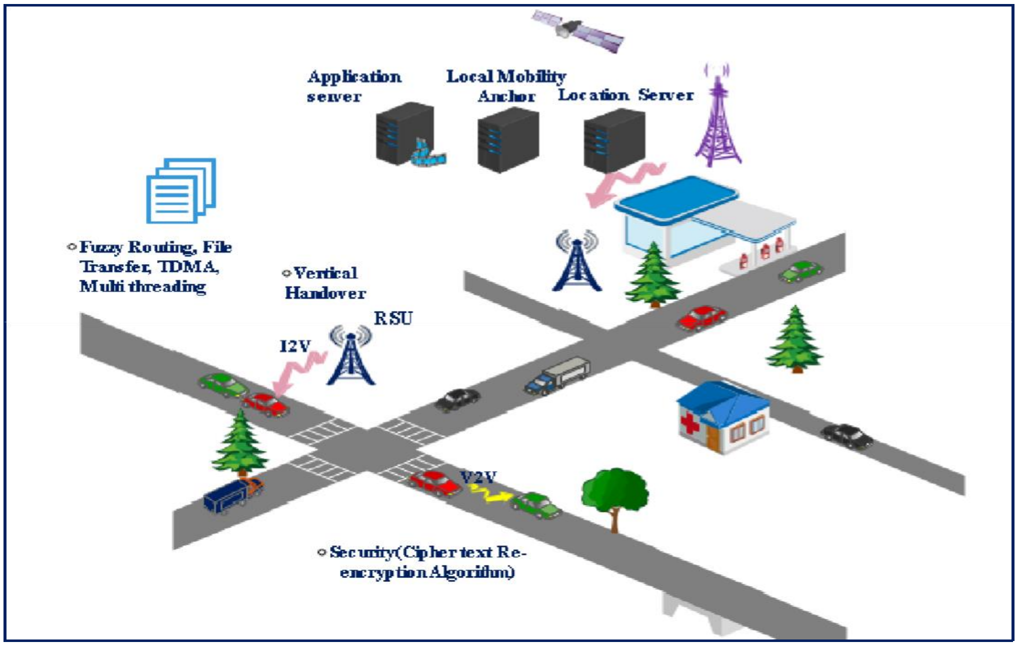

Application server
Local Mobility Anchor
Location Server
Fuzzy Routing, File Transfer, TDMA, Multi threading
Vertical Handover
RSU
I2V
V2V
Security(Cipher text Re-encryption Algorithm)

Fig. 1: Proposed Scheme.

Proxy Mobile Internet Protocol (PMIP) (RFC 5213) is a network mobility management protocol instead of host based network management. In PMIP, the node does not participate in IP mobility and information related with mobility is not required. The network manages mobility of IP instead of mobile node. PMIP defines two functional entities. (1) Local Mobility Anchor (LMA) and (2) Mobile Access Gateway (MAG). LMA is considered as a home agent for a mobile node and topologically broadcasting point for the mobile node. LMA also manages the binding state of a mobile node. The unique identifier of the mobile node and network prefixes of the mobile node are stored and maintained by LMA. LMA establishes a tunnel to send and receive packets with MAG which is directly communicating with mobile nodes. MAG tracks the mobile node’s movement to and from the access links and signals the LMA about the mobility information. In our scheme RSU acts as MAG. The IP packets are downloaded from application server through LMA. The location server stores the location information of the mobile nodes and the position of the mobile node can be accessible by other nodes through query when the other mobile nodes need the location information to forward the packets. Local Mobility Anchor (LMA), application server, location server and RSUs are considered to be fixed, trusted infrastructure based networks. The LMA and RSUs are responsible for establishing shared keys among the communication entities. This work considers both V2V and V2I types of communications. Each RSU in the network domain creates four variable f(w,x,y,z) symmetrical polynomial to the LMA. From the collected polynomials from different RSUs, the LMA computes another polynomial which is sum of the network polynomials received from ‘k’ number of RSUs.

$$DP(w,x,y,z) = \sum_{i\in R^n}^{k} f_i\,(w,x,y,z), 2 \le k \le n \quad \dots\dots\dots\dots\dots \text{(1)}$$

Where ‘n’ is the number of RSUs connected to the LMA. The computed polynomial thus obtained is evaluated for each RSU with its id ID_{RSU}. DP(ID_{RSU},x,y,z) is evaluated for each vehicle to generate shared secret key. For vehicle-1 (V_1) the polynomial is computed as DP(ID_{RSU},ID_{V1},y,z). The keyGen function is used to generate public and private keys as per PKI for each vehicle as per homomorphic encryption with 1^{λ} as security parameter. The evaluate function is simple circuit function such as ‘AND’ and ‘XOR’.

In cipher text re-encryption algorithm, the keys generated are small in size and efficient for security and key management. This process involves two-fold encryption and reduces the noise in the given plain text. Cipher text ReEncryption (CRE) algorithm is proposed to maintain secured communication among the vehicles where its processing speed is high and key generation time is also low. Cipher text re-encryption algorithm efficiently supports authentication of vehicles by signature verification. By adopting authentication, Sybil attack and Sink hole attack can be prevented. The processing time for encryption depends upon the number of bits in the cryptographic key and the processing time observed are 6 mSec, 12 Sec and 24 Sec for 1024 bits, 2048 bits and 4096 bits key respectively.

Algorithm 1 explains the complete process that takes place in the Cipher text re-encryption algorithm.

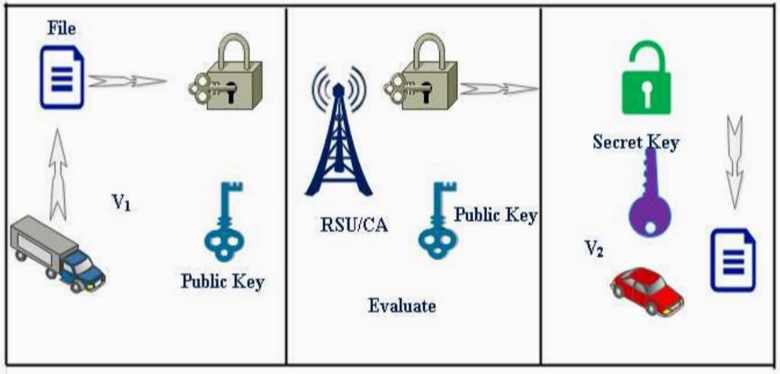


Fig. 2: Ciphe text re-encyrption.

Fig. 2 clearly shows the working of our cryptosystem between two vehicles (Vehicle-1 (V_1) and Vehicle-2 (V_2)). If V_1 wants to transmit data to V_2 then V_1 should register with LMA for authentication key before transmission. Here the validity of the IDentity (ID) corresponding to the V_1 is checked by LMA through RSU. If the user is legitimate, then LMA provides authentication Key and Signature by which V1 encrypts the original message and sends it to RSU.

Algorithm 1 Cipher Text Re Encryption

```
Define message $\mathbf{m}$
Define private key $\mathbf{p_k}$
Define secret key $\mathbf{s_k}$
Define security parameter $\lambda$
Define random odd number $\mathbf{e}$
Begin:
Input $\mathbf{m}, \lambda$ :
Key Generation:
    Generate public key $\mathbf{p_k} := 1^{\lambda}, \mathbf{e}$
    $\mathbf{s_k} = \mathbf{e}$
Encryption:
    $C := (\mathbf{m},\mathbf{p_k})$
Evaluate:
    $f(\psi) := (f,C,\mathbf{p_k})$
Decryption:
    $\mathbf{m} := (f(\psi),\mathbf{s_k})$
End.
```

RSU performs evaluation operation and sends it to the vehicle V_2. Then V_2 checks the authentication of V_1 and decrypts the cipher text with the private key and retrieves the original data. Here a malicious node can be entangled at the time when the RSU checks its ID during data transmission.

3.2 Prevention of Attacks:

Algorithm 2 and Algorithm 3 clearly explains how the Sybil and Sinkhole attacks are prevented in proposed scheme. The prevention of these attacks in proposed framework need not require any separate process as it is included in our cryptographic algorithm itself. These harmful attacks are detected by RSU of network.

Algorithm 2 Prevention of Sybil Attack

```
Define Signature $\mathbf{SG}$
Input:
    $\mathbf{m},\lambda,\mathbf{e},\mathbf{SG},\mathbf{p}_k,\mathbf{s}_k$
Begin:
    (Before Start to Transmit data)
Register:
$V_s$registers with LMA
Key Generation:
    $\mathbf{p}_k \leftarrow 1^{\lambda}, \mathbf{e}$
    $\mathbf{s}_k \leftarrow \mathbf{e}$
$V_s$ Gets:
    $\mathbf{SG},\mathbf{p}_k,\mathbf{s}_k$
Encryption:
    $C \leftarrow (\mathbf{m},\mathbf{p}_k)$ @$V_s$
Evaluation:
    $f(\psi) \leftarrow (f,C,\mathbf{p}_k)$ @RSU
    (Received Data)
Verification:
    $\mathbf{SG}(V_s)$verified by$V_d$
Decryption:
    $\mathbf{m} \leftarrow (f(\psi),\mathbf{s}_k)$
End.
```

Algorithm 3 Prevention of Sink hole Attack

```
Define $\mathbf{S}_n$ as Sequence Number
Input:
    $\mathbf{m},\lambda,\mathbf{e},\mathbf{p}_k,\mathbf{s}_k$
Begin:
(Before Start to Transmit data)
Request:
    ($V_1$) sends RREQ to RSU
Screening:
    (ID,$S_n$($V_1$))@RSU
    If (ID,$S_n$== Original)
    Goto next step
    Else
    Discards the RREQ
    End if
Key Generation:
    $\mathbf{p}_k \leftarrow 1^{\lambda}, \mathbf{e}$
    $\mathbf{s}_k \leftarrow \mathbf{e}$
Encryption:
    $C \leftarrow (m,p_k)$
Evaluation:
    $f(\psi) \leftarrow (f,C,\mathbf{p}_k)$
Decryption:
    $\mathbf{m} \leftarrow (f(\psi),\mathbf{s}_k)$
End.
```

Prevention of Sink hole attack: Sinkhole attacker node usually generates a bogus RREQ (Route REQuest) in the routing process either to get the information of other transmission or to drop the packets unwantonly. The attacker node adds itself in the route, as if it has shortest path to the destination. This can be detected if the sequence number of RREQ is greater than the current sequence number then it can be found that the RREQ is from an attacker node (i.e.) sinkhole attacker node. To prevent such attack initially the V_1 sends the RREQ to RSU. Then RSU checks with the sequence number and the source ID of V_1, if it is fake, then the RREQ is discarded by the RSU, if legitimate vehicle then RSU re-encrypts and forwards the data packet to V_2. By this encryption process sinkhole attack can be prevented.

3.3 File Transfer:

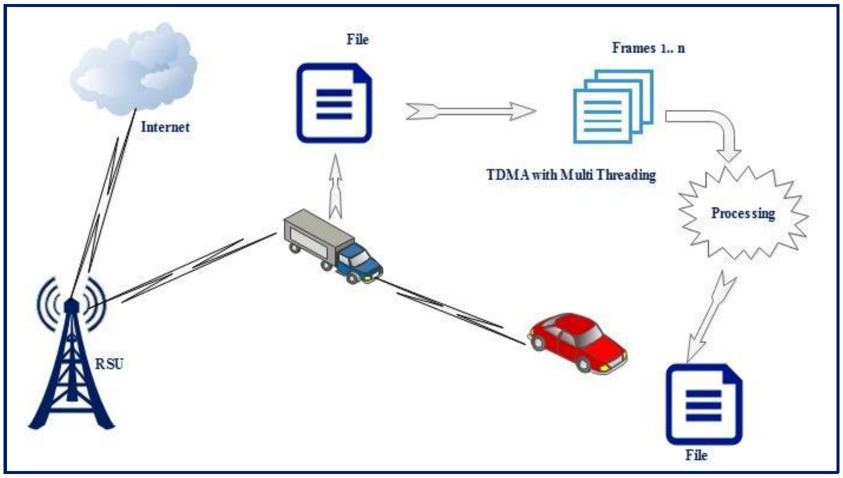


Fig. 3: File Transfer.

Transferring huge files (Video/Data) is a cumbersome task in VANET environment due to asymmetric links. This problem can be solved by “Time Division Multiple Access (TDMA)” and multithreading which can provide continuous streaming coverage of whole VANET efficiently (Ref Fig. 3). The combination of TDMA and multithreading reduces the time consumption and greatly reduces the processing time in VANET. TDMA is free from collisions at MAC layer. In TDMA, delivery time is divided in to number of slots. The time is allotted based on the size of the file. Multithreading is a type of multitasking, which has the capability to perform the process in parallel manner. Let G be the total size of the video file in Mega bits (Mb). Based on the size of the data file, time T is allocated for the file, which is ready to send. The given file size ‘G’ is divided into number of frames (g_1,g_2,.....g_n) with respect to the time assigned for the file. Each frame is allotted with the time slots t_1,t_2,t_3...t_n. Here all the frames are simultaneously sent with the help of multithreading.

In TDMA, the channel access time is divided into the number of synchronized time intervals which depends on length of the total size of the file. Multithreading can be applied to enable parallel execution of the given input data. Due to this parallel processing of the data there is no delay in transferring file in VANET when the vehicle moves in high speed. For example, Let us assume the total size of the file is 2 GB. The entire file is divided into frames. Here the file is divided in to 8152 frames. Based on TDMA, the time to send the file is estimated and then the frames are processed by multithreading. By using both TDMA and multithreading, collision among the transmission in the network is greatly reduced.

3.4 Routing and Handover

Routing in VANET is required to deliver the data packets to the mobile vehicles in the communication range in a timely manner without any packet losses. Finding a stable route is very difficult process in VANET environment. Based on the mobility of the nodes, ’handover’ is transfer of the service for a node from one network to another. The proposed framework uses vertical handover. The topology of VANET changes rapidly and results in disconnection of link frequently. Hence it is difficult to construct an efficient and stable routing protocol for VANETs. In the proposed framework, a novel Fuzzy logic Based Secured Routing (FBSR) is used. Two routing protocols one from proactive and other form reactive are considered. “Optimized Link State Routing (OLSR)” protocol is a proactive type and an “Adhoc on demand Distance Vector routing (AODV)” which is a reactive protocol. Fuzzy logic is used for resolving the uncertainty in connectivity parameters.

In case if routing is selected based on the reactive protocol, the routing process takes place between either V2V or V2I. An enhanced fuzzy rule based routing and handover process is implemented by considering two parameters viz; mobility and traffic conditions. In VANET mobility of the vehicle and traffic in network do not remain constant. Due to the frequent changes in these two parameters, we consider these parameters as input parameters for simulation study. There will be V_i (i=1, 2, 3....n) vehicles in the network at time T_i. The selection of routing method requires dynamic routing conditions without ambiguity, hence we apply fuzzy logic to resolve the uncertainty in determining the connectivity parameters.

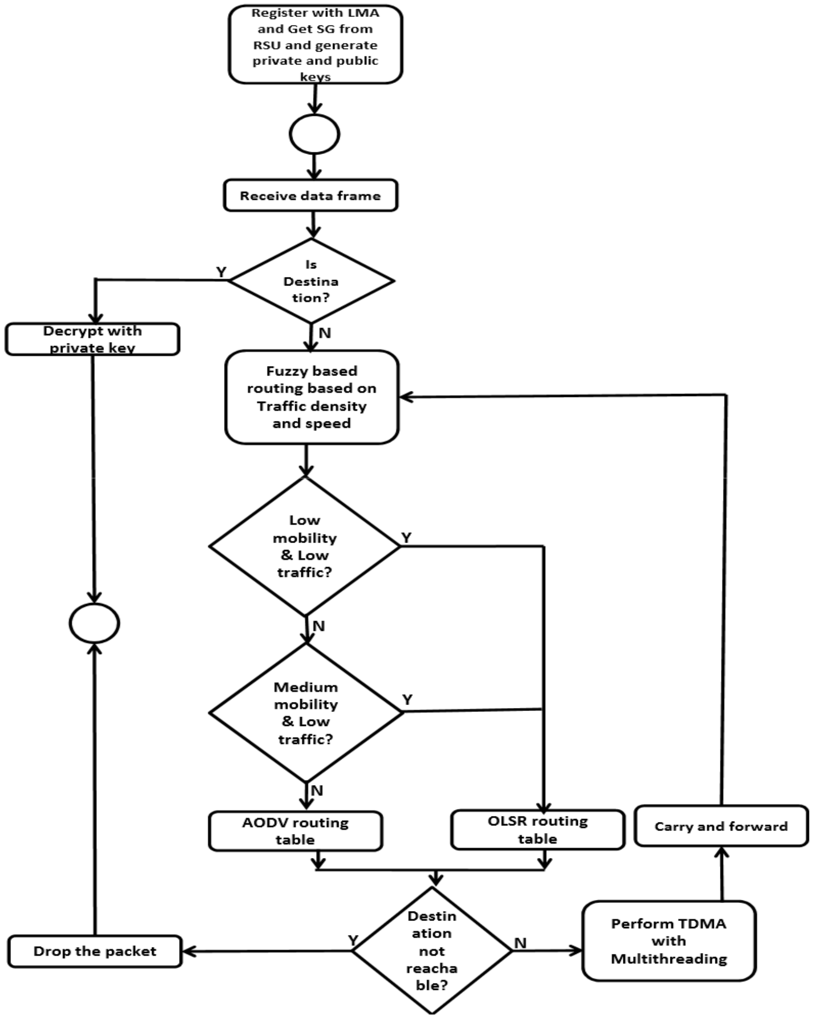

Register with LMA and Get SG from RSU and generate private and public keys
Receive data frame
Is Destination?
Y
N
Decrypt with private key
Fuzzy based routing based on Traffic density and speed
Low mobility & Low traffic?
Y
N
Medium mobility & Low traffic?
Y
N
AODV routing table
OLSR routing table
Carry and forward
Destination not reachable?
Y
N
Drop the packet
Perform TDMA with Multithreading

Fig. 4: Flowchart of FBSR

The fuzzy routing depends on the number of vehicles (traffic) and speed of the vehicle. Four membership functions are defined for linguistic variables [22] as shown in equations (2), (3) and (4) and the fuzzy rules are specified as per Table-1. The crisp output is based on weighted average method. The mobility of vehicle is calculated as average velocity of 5 samples of velocities of each vehicle. The handover to RSU or back haul network takes place depending upon the Fuzzy logic Based Secured Routing (FBSR). Flow chart (Fig. 4) explains steps involved in the FBSR.

$$Triangle(x;a,b,c) = \begin{cases} \frac{(x-a)}{(b-a)} & a \leq x \leq b \\ \frac{(c-x)}{(c-b)} & b \leq x \leq c \\ 0 & Otherwise \end{cases} \quad \text{....(2)}$$

$$Z(x;d,e) = \begin{cases} 1 & x \leq d \\ 1-2\left(\frac{x-d}{c-d}\right)^2 & d < x \leq \frac{d+e}{2} \\ 2\left(\frac{x-e}{c-d}\right)^2 & \frac{d+e}{2} < x \leq e \\ 0 & x > e \end{cases} \quad \text{............... (3)}$$

$$S(x;f,g)=\begin{cases}1 & x\le g\\ 2\left(\frac{x-f}{g-f}\right)^2 & f\le x\le\frac{f+g}{2}\\ 1-2\left(\frac{x-g}{g-f}\right)^2 & \frac{f+g}{2}<x<g\\ 0 & x\le f\end{cases} \quad \ldots\ldots\ldots\ldots\ldots\ldots \textit{(4)}$$

$$Output_{Crisp}=\frac{\sum_{j=1}^{n}\mu_j w_i}{\sum_{j=1}^{n}\mu_j}\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \textit{(5)}$$

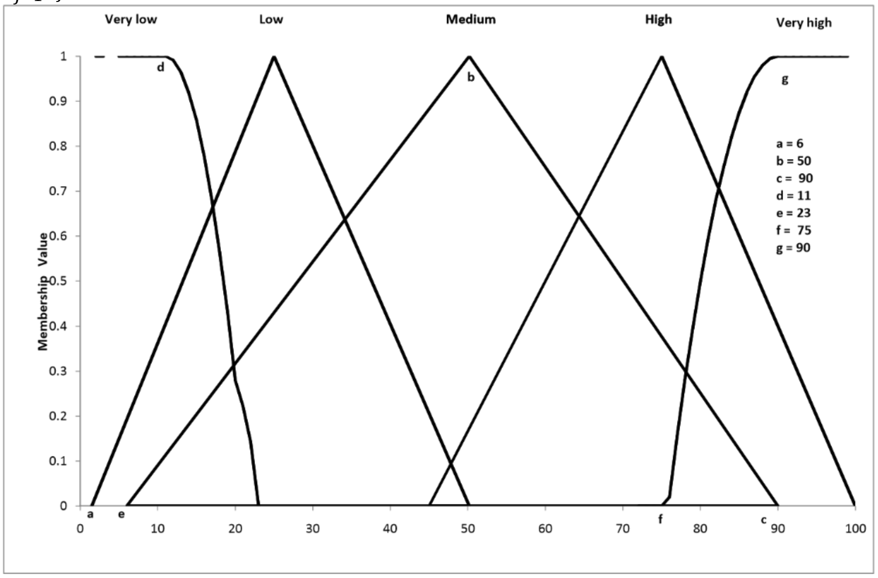


Fig. 5: No. of vehicles (Traffic)

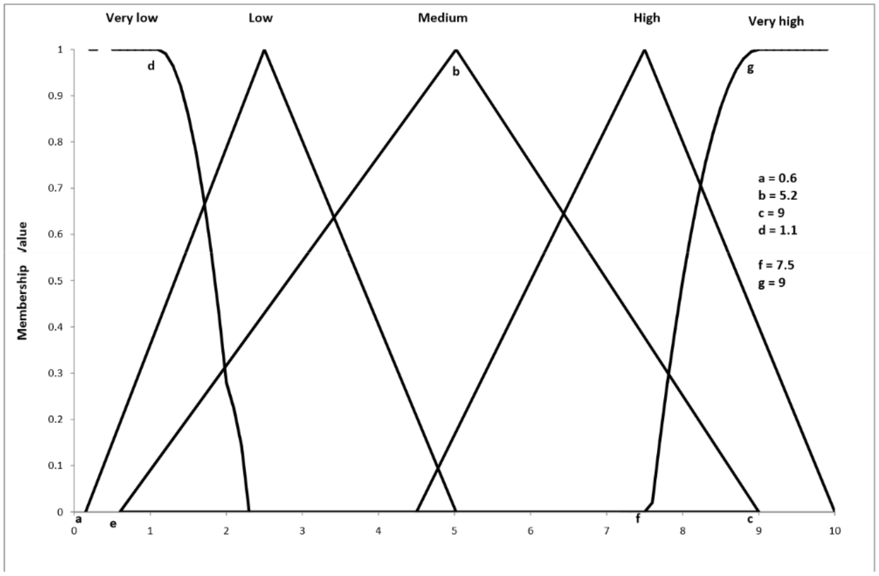


Fig. 6: Mobility

Table 1: Fuzzy Rule for Routing

Sl. No	Mobility	Traffic	Output
1.	VL	VL	Proactive
2.	VL	Low	Proactive
3.	VL	Moderate	Reactive
4.	VL	High	Reactive

5.	**VL**	**VH**	**Reactive**
6.	**Low**	**VL**	**Proactive**
7.	**Low**	**Low**	**Proactive**
8.	**Low**	**Moderate**	**Reactive**
9.	**Low**	**High**	**Reactive**
10.	**Low**	**VH**	**Reactive**
11.	**Moderate**	**VL**	**Reactive**
12.	**Moderate**	**Low**	**Reactive**
13.	**Moderate**	**Moderate**	**Reactive**
14.	**Moderate**	**High**	**Reactive**
15.	**Moderate**	**VH**	**Reactive**
16.	**High**	**VL**	**Reactive**
17.	**High**	**Low**	**Reactive**
18.	**High**	**Moderate**	**Reactive**
19.	**High**	**High**	**Reactive**
20.	**High**	**VH**	**Reactive**
21.	**VH**	**VL**	**Reactive**
22.	**VH**	**Low**	**Reactive**
23.	**VH**	**Moderate**	**Reactive**
24.	**VH**	**High**	**Reactive**
25.	**VH**	**VH**	**Reactive**

V L …………… Very low
VH……………. Very High

4. Simulation

The validation of proposed FBSR algorithm is done through simulation experiments in OMNeT ++ which includes pre-simulation environment with SUMO package. The simulation parameters of OMNeT++ are listed in Table-2. For experiments, up to 120 vehicles spread over 2500 x 2500 meters are considered and the number of nodes is not maintained constant in VANET since the vehicles moves at high speed. The node speed is varied between 2 – 10 meters per sec. 10% of the nodes are introduced in the VANET as ’Attacker nodes’ during simulation. In order to introduce heterogeneity, two RSUs for Long Term Evolution (LTE) and one Access Point for Wi-Fi are included in the simulation. Simulation of proposed framework is considered only in a parallel two lane road.

Table 2: Simulation parameters

Parameter	**Value / Range**
Number of Nodes	1-120
Speed	2-10 Mps
RSU-LTE	2
AP-WiFi	1
Area	2500 x 2500 m
Carrier Frequency	2.4 GHz
Transmitter power	2 mW
Beacon Interval	1 sec
No of lanes	2
Video Size	**20MB**

5. Performance Analysis

In this section, the performance of the proposed FBSR framework is compared with existing work proposed by PMIP [18] in terms of communication overhead and authentication delay. The methods are analyzed in terms of the performance metrics and the results are summarized in Table-3.

5.1 Average End-to-End Delay

"End to End Delay (E2E delay)" or latency is the sum of the MAC layer delay to transmit the packet, "queuing delay" and propagation delay of a packet from source to destination node. E2E delay depends on several factors such as hop count, network congestion etc. Throughput of the network is affected due to undue E2E delay. If the TTL goes beyond the limit, the packets will be discarded. Once the packet is discarded, ICMP will be sent to source node to retransmit the packet which in turn affects the throughput. E2E delay can be calculated as follows [23]

$$D_{End\_to\_End} = \sum_{n=1}^{N} TR_n - TS_n \dots\dots\dots\dots\dots(6)$$

Where,

TR_n– Time taken to receive n^{th} data packet

TS_n – Time taken to send n^{th} data packet

N - Number of packets received

The average E2E delay Vs Number of communication sessions and E2E delay Vs Number of nodes are plotted as illustrated in Fig. 7(a) and 7(b) respectively. As the number of communication sessions increases, FBSR shows constant E2E delay of 20 msec compared to other classical routing methods such as AODV, OLSR and MA-PMIP. Similarly when the node density increases, the E2E delay is less than 45 msec.

5.2 Packet Delivery Ratio

"Packet delivery ratio (PDR) is defined as the ratio of the number of data packets delivered to the destination and the total number of packets send from the source". For better performance of the network, PDR value must be high. PDR is calculated [23] as,

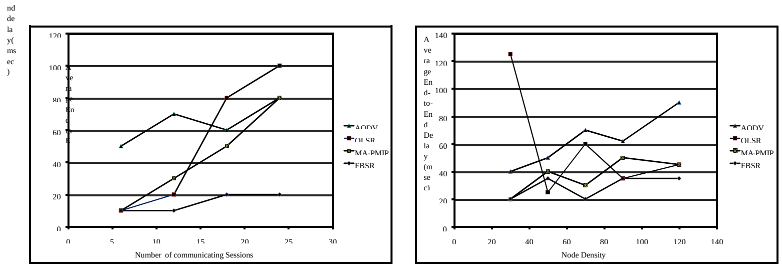
$$PDR = \frac{\sum N_r}{\sum N_s} \dots\dots\dots\dots\dots\dots\dots\dots\dots\dots (7)$$

Where, N_r – Number of packets received, N_s– Number of packets sent

The PDR is 100% always and remains constant whenever OLSR is selected as the routing algorithm. When AODV is selected as routing algorithm, the PDR varies from 90 to 95%.

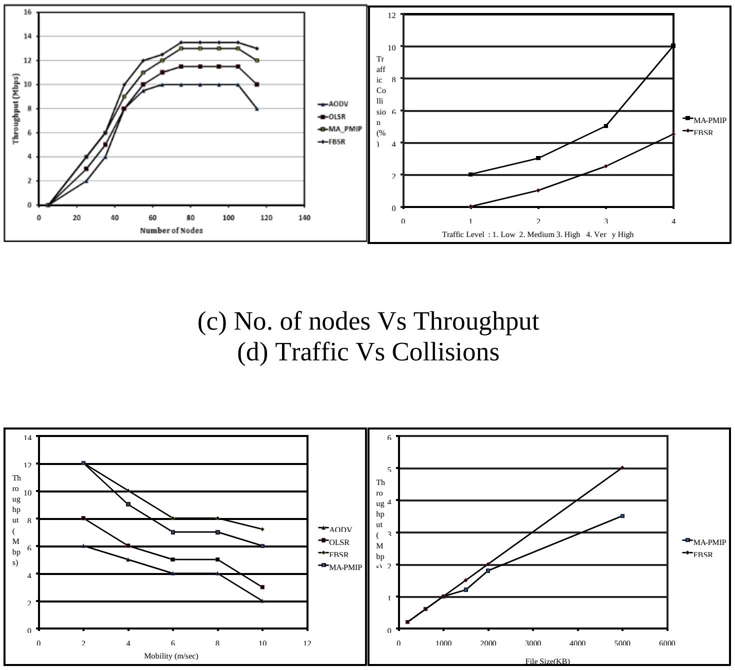
5.3 Traffic Collision

Generally, if more than one user communicates to a particular destination at the same time then collision occurs. Here traffic collision occurs when there is participation of more number of vehicles in data transmission simultaneously. The scheduling of packet dispatch using TDMA with multi-threading technique reduces the collision considerably.



(a) No. of comm. sessions Vs End to End delay

(b) No. of nodes Vs End to End delay



(c) No. of nodes Vs Throughput
(d) Traffic Vs Collisions

(e) Mobility Vs Throughput
(f) File size Vs Throughput
Fig. 7: Performance analysis

5.4 Throughput

Throughput is a most important parameter to be considered in VANET. Throughput refers how much data that can be transferred from source to destination in a given amount of time. Throughput is the rate of successful message delivery over a communication channel. Generally throughput is expressed as,

$$T = \frac{N_S}{Total\ time} \ldots\ldots\ldots\ldots\ldots(8)$$

Where T – Throughput, N_s – Number of packets successfully received

Throughput is plotted with respect to number of nodes, mobility of the nodes and file size as illustrated in Fig. 7(a), 7(b) and 7(c). Throughput of the FBSR excels compared with other schemes. However either number of nodes or mobility increases, the throughput starts decreasing trend.

Table 3: Comparison of FBSR with MA-PMIP

Features	**MP-PMIP**	**FBSR Framework**
File Transfer	Does not Support Large sized files	Supports large sized files
Collision	Collision occurs at the time of Streaming	Collision does not occur
Encryption	Takes more Time	Less Time

5.5 Authentication Delay

The time taken for a vehicle to send authentication request and receive back an authentication reply from the requesting vehicle is said to be authentication delay. The observed authentication delay is 6 to 10 mSec.

5.6 Communication overhead

In case if more numbers of requests are received at the same time then there will be a heavy load on the network. The communication overhead increases as more number of vehicles are participating in a VANET so formed with RSUs.

6 Conclusion

VANET is moving towards next stage of its evolution. Providing secured data transmission in VANET environment is still a challenging task. The proposed framework FBSR with cipher text re-encryption prevents Sink hole and Sybil attacks. The metrics such as throughput, packet delivery ratio, average E2E delay, traffic collision and authentication delay showed improvement compared with previous work. During data transmission, the proposed FBSR framework, the average E2E delay and traffic collision are reduced. Based on enhanced fuzzy rule, the routing and handover are executed by AODV and OLSR protocols effectively based on mobility and traffic conditions. The application of file transfer has been implemented without collision using TDMA and multi-threading concepts. Thus the proposed FBSR framework is applicable for the heterogeneous network video streaming and mobile television. In future, decision making for routing and handover process can be performed using geographic information from GPS and the simulation setup can be enhanced for multi-lane roads and junction points of the roads.

References

1. Kabir, M.H.: Research issues on vehicular ad hoc network. Int J Eng Trends and Technol **6** (2013) 174–179
2. Raw R.S., et al: Security challenges issues and their solutions for vanet. Int J Netw Secur and its applications **5** (2013) 95–105
3. Ertaul, L. et al: Proc intl conf on wirel netw usa. In Arabnia, H.R., et al., eds.: The Security Problems of Vehicular Ad Hoc Networks (VANETs) and Proposed Solutions in Securing their Operations, CSREA (2009) 3–9
4. Chang, C.Y et al: V2V QoS Guaranteed Channel Access in IEEE 802.11p VANETs. IEEE Trans Dependable and Secure Computing **99** (2013) 1–13
5. Tamilarasan, A.K., Krishnadhas, S.K., Sabapathy, S. et al. A novel design of Rogers RT/duroid 5880 material based two turn antenna for intracranial pressure monitoring. Microsyst Technol (2021). https://doi.org/10.1007/s00542-020-05122-y
6. Ucar S. et al: Multi hop Cluster Based IEEE 802.11p and LTE Hybrid Architecture for VANET Safety Message Dissemination. IEEE Trans On Vehicular Technol **64** (2016) 2621– 2634
7. Stalin, J., et al: A survey on topology and geography based routing protocols in vanets. Int J Appl Eng Research **13** (2018) 14813–14822
8. Bhagat, S.M. et al: Performance Evaluation of AODV Routing Protocol using WiMAX on VANET. Int J Comput **108** (2014) 36–39
9. Patil, K.V. et al: The enhanced optimized routing protocol for vehicular ad hoc network. Int J Advanced Research Comput And Comun Eng **2** (2013) 4013 – 4017
10. Kadivar, R.: Fuzzy logic based stable routing in vanet. Elixir Adhoc Netw **56** (2013) 13413 – 13416
11. Lin, C. et al: Fuzzy interference based vehicle to vehicle connectivity model to support optimization routing protocol for vehicular adhoc networks. J Advanced Computational Intell Inform **18** (2014) 9–21
12. Gad, W., et al: 10th int comput eng conf. In: A Fuzzy based Routing Protocol For Metropolitan Area Mobile Adhoc Networks, IEEE (2014) 33–138
13. Agarwal, S., et al: Enhancing greedy routing using fuzzy logic for vehicular ad hoc networks. In: Proc Int Conf On Advances in Comput Control Netw, SLEEK DL (2015) 98–102
14. Sarma, A., et al: Deciding Handover Points based on Context Aware Load Balancing in a WiFi WiMAX Heterogeneous Network Environment. IEEE Trans Vehicular Technol **65** (2015) 248–357
15. Dak, A.Y. et al: A literature survey on security challenges in vanets. Int J Comput Theory and Eng **4** (2012) 1007–1010
16. Zhang, J. et al: Privacy preserving authentication protocols with efficient verification in vanets. Int J Commun Systems **27** (2013) 3676–3692
17. Sasikala, G. et al: Key management techniques for vanets. Intl J Comput Applications **2** (2012) 13–6
18. Cespedes, S. et al: A multi hop authenticated proxy mobile ip scheme for asymmetric vanet. IEEE Trans Vehicular Technol **62** (2013) 3271–3280
19. Park, J., et al: Emergency related video streaming in vanet using network coding. In: Proc VANET'06 USA, ACM (2006) 102–103
20. Gerla, M., et al: Vehicular networks and the future of the mobile internet. Comput Netw **6** (2011) 127–142
21. Rezende, C., el al: A reactive and scalable unicast solution for video streaming over vanets. IEEE Trans Vehicular Technol **64** (2015) 614–626

22. Adimoolam, M., John, A., Balamurugan, N. M., & Kumar, T. A. (2020). Green ICT Communication, Networking and Data Processing. In Green Computing in Smart Cities: Simulation and Techniques (pp. 95-124). Springer, Cham.
23. Gulati, M.K. el al: Performance comparison of mobile adhoc network routing protocols. Int J Comp Netw Commun **6** (2014) 127–142.
24. Aleksandr Ometov, et al: Positioning Information Privacy in Intelligent Transportation Systems: An Overview and Future Perspective, Sensors 9 (2019) 1-23.