MULTIMEDIA COMMUNICATIONS TECHNICAL COMMITTEE
https://mmc.committees.comsoc.org

MMTC Communications - Frontiers

Vol. 15, No. 4, July 2020

CONTENTS

Special Issue on Robust Networked Systems for Emerging Applications

Guest Editor: Chandra Bajracharya
Capitol Technology University, USA
cbajracharya@captechu.edu

This special issue of Frontiers focuses on Robust Networked Systems for Emerging Applications, which embraces robust video content delivery and blockchain based solutions for emerging applications such as internet of vehicles, vehicle-embedded smart health systems and other blockchain based systems and applications. With the advanced networking technologies and blockchain, networked systems could provide robust services for different applications, including internet of vehicles. Various research topics and projects in this area are witnessed, and the advancement can be foreseen in the future.

The first paper, by *Sadiq* et al., investigates the efficient video content transmission over vehicular networks. Authors propose a balanced video-forwarding algorithm for delivering video-based content delivery scheme where the available neighboring vehicles are ranked to the vehicle in forwarding progress before transmitting the video frames using proposed multi-score function. Forwarding progress and direction to destination, in addition to residual buffer length; the proposed algorithm can elect the best candidate to forward the video frames to the next highest ranked vehicles in a balanced way taking in account their residual buffer lengths. Simulation results demonstrate the efficiency of the proposed algorithm. In the second paper, Singh et al. propose a blockchain enabled vehicles health records (VHR) system to facilitate different entities to offer various services in a proactive, transparent, secure, reliable and in an efficient manner. Specifically, a blockchain-based decentralized secure system is proposed to manage records in an interoperable framework that leads to improved intelligent transportation system services in terms of safety, availability, reliability, e□ciency, and maintenance. Insurance based on pay-how-you-drive, and sale and purchase of used vehicles can also be made more transparent and reliable without compromising the confidentiality and security of sensitive data. The third paper focus on cyber defense remediation based on adversarial characterization in energy delivery system. Finally, the fourth paper focus on adaptive control plane load balancing in vSDN enabled 5G network

Finally, I want to thank all the contributing authors involved in this issue. I hope readers will find this special issue informative and useful.

Dr. Chandra Bajracharya is the Assistant Professor in the Department of Electrical Engineering at the Capitol Technology University, USA. Her research interests cover broad areas of cyber physical systems and cybersecurity, robotics, communications systems for emerging cyber physical systems and Internet of Things including smart grid, intelligent transportation systems. She has published over 30 peer reviewed journal articles, conference papers and book chapters and a book.

Geographical Forwarding Algorithm based Video Content Delivery Scheme for Internet of Vehicles (IoV)

Ali Safaa Sadiq[1], Kayhan Zrar Ghafoor[2], Chih-Heng-Ke[3]
[1]Monash University, Malaysia
[2]Shanghai Jiao Tong University, China
[3]National Quemoy University, Taiwan
ali.safaa@monash.edu

ABSTRACT

An evolved form of Vehicular Ad hoc Networks (VANET) has recently emerged as the Internet of Vehicles (IoV). Though, there are still some challenges that need to be addressed in support IoV applications. The objective of this research is to achieve an efficient video content transmission over vehicular networks. We propose a balanced video-forwarding algorithm for delivering video-based content delivery scheme. The available neighboring vehicles will be ranked to the vehicle in forwarding progress before transmitting the video frames using proposed multi-score function. Considering the current beacon reception rate, forwarding progress and direction to destination, in addition to residual buffer length; the proposed algorithm can elect the best candidate to forward the video frames to the next highest ranked vehicles in a balanced way taking in account their residual buffer lengths. To facilitate the proposed video content delivery scheme, an approach of H.264/SVC was improvised to divide video packets into various segments, to be delivered into three defined groups. These created segments can be encoded and decoded independently and integrated back to produce the original packet sent by source vehicle. Simulation results demonstrate the efficiency of our proposed algorithm in improving the perceived video quality compared with other approaches.

1 INTRODUCTION

Recently, further considerations were given in maintaining video streaming over vehicular ad hoc networks [1]. Utilizing Vehicle to Infrastructure (V2I) communication, a vehicle is able to download video utilizing the RSU. This was normally performed through using license-free wireless spectrum belongs to the transmission range of the RSU. In fact, it is still an open issue though RSUs are feasible to support video streaming services elaborating the license-free wireless communication technologies. This is due to the following two main challenges. Firstly, the wireless channel normally bears time-varying fading, shadowing, and interference, those consequent to high difference of link throughput and hence degrade video quality. As a second reason, the high cost that could be given in deploying RSUs to allow high coverage area in support video streaming services. Thus, it is inapplicable to install adequate RSUs to cover a complete highway. Therefore, the coverage of RSUs is irregular.

In order to address the first challenge, several approaches using the Scalable Video Coding (SVC) [2] to lighten the impact of time-varying channels that normally drawback on video Quality-of-Experience (QoE). An extension of the H.264/Advanced Video Coding (AVC) video standard, SVC encodes each video frame into layers. This was achieved by introducing a base layer and several enhancement layers. Thus, in decoding the video frames the base layer should be obtained completely. By extra enhancement layers received, a better quality of decoded video frames could be achieved. Accordingly, as an advantage of using SVC is that with some level of packets losses belong to enhancement layers are acceptable. Hence, the video receiver vehicle is able in decoding the video without obtaining all packets.

On the other hand, as a way to address the second challenge, V2V communications is a promising solution. Using V2V communications can considerably extend the coverage of RSUs along the highway. Hence, V2V allows the vehicles download video with cooperative relay vehicles. In [3] authors have organized vehicles to be into separate clusters. The way that they have used in clustering vehicles, is by managing the process of joining or leaving new vehicles. However, still there is an open issue in finding the best route to the destination or distributing the video packets among the vehicles in balanced way.

In this paper, the Quality-of-Experience (QoE) aware Geographical Forwarding Algorithm based Video Content Delivery over vehicular ad hoc networks will be considered. Certain quality metrics will be accurately measured to identify the best relay-vehicle in forwarding the video packets, which are taken in consideration the high mobility and dynamic nature of VANET. Moreover, a load balancing driven geographical forwarding for video packets is proposed to distribute them among the vehicle cooperative relay. The proposed video geographical forwarding algorithm in this study aims to minimize the video playback interruption time and maximize video playback quality with avoiding high startup delay. Thus, using our proposed video routing algorithm the users will observe an improved QoE of running video.

2 RELATED WORKS

The serious need for obtaining high QoE for the video streaming over vehicular networks has driven the research efforts towards the development of more efficient protocols. Maintain high quality of transmitted video over VANETs could enable the service of reporting fatal road accidents, which leads to obtain an improved version of IoV. Yet, this task of transmitting real-time application such as video over VANET network is a challenging. This is due to the fact that vehicles are moving in a highly dynamic and unpredictable topology, which makes the video routing protocols facing tremendous challenge. This dynamic behavior of vehicular networks topology is challenging as it consequences in frequent link disruption and a disconnection will highly occur. On the other hand, Low bandwidth, high packet loss rate, and short-lived connectivity are other concerns that need be attended in the environment of vehicular networks [20].

As an attempt to address the above-mentioned challenges, the authors in [4] have introduced a quality-aware geographical packet-forwarding algorithm from Road-Side-Unit (RSU) to Vehicles. Furthermore, when the destination vehicle (video receiver) moves from the connection link of one point of attachment to the other one, the Internet Protocol (IP) will be changed. Accordingly, the authors in [4] are also attempted IP mobility management for the seek of cultivating visual quality of transmitted video, as when the destination vehicle attend to obtain new Mobile IP address from the new visited RSU, a time will be taken to handle this process. In spite of the proposed solution in [4], further consideration should be taken of the next RSU selection as a way to avoid any possible quality, mobility and/or user preferences miscount.

On the other hand, enabling video applications for the use of traffic safety in vehicular networks using infrastructure-less setup is highly demanded. Fig 1 shows the vehicular network topology that is demonstrating this scenario. As can be seen, the radio communication range of every vehicular relay-node and multi-hop V2V would be used for packet forwarding from source vehicle V_s toward the destination vehicle V_d. Using V2V communication a free of charge video transmission can be achieved. However, this attempt yet to be widely visible due to the aforementioned reasons related to the highly dynamic topology in vehicular networks.

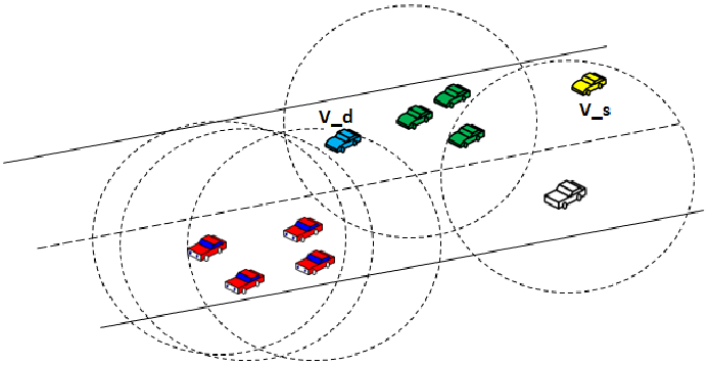


Figure 1: The highway topology of vehicular Ad-Hoc networks.

In contrast, the authors in [5] strained to improve the quality of video transmission over vehicular networks by exploring an approach to achieve a fairness of accessing the wireless channel among neighbouring vehicles. An evaluation of multi-hop video streaming from IEEE 802.11p enabled vehicular surveillance network to the traffic management center was conducted. They have employed in the evaluation phase a Scalable Video Coding (H.264/SVC) and non-standard scalable video coding three dimensional discrete wavelet transmissions (3-D DWT) [6]. As they have claimed in their study that the selection of the targeted vehicle for video transmission is crucial and it highly depends on the vehicular traffic density and location of participating vehicles. However, in their video evaluation and transmission there was no consideration of a balanced video frames routing metric considered. In other words, there should be a priority tag given for those frames (I-Frames) contributing seriously to the quality of the received video record and they should be handled view high quality relay vehicles/RSUs. While on the other side, in [7] the performance analysis of different routing protocols (AODV, DSDV, GPSR) for video transmission over realistic VANET environment is implemented. The utilized simulation tool is incorporated myEvalvid [8], NS2 [9] and VANETMobiSim [10]. The authors have concluded that DSDV is not fitting for real-time video transmission over VANET, particularly for networks with high mobility. Whilst, they have found that GPSR protocol is performing better for video transmission over VANET in comparison with AODV. They have indicated that a Pro-active type of protocols is not suitable for video transmission over VANET, and Position-based protocol is performing better for video transmission over VANET in contrast with Re-active protocol. From this claim we can also indicate that Geographical information is essential metric to be considered during the development of routing protocols for video transmission over VANET.

As another initiative to improve the video streaming over VANET, the authors in [11] have developed a method for video transmission in overlay vehicular environment. They have used joint Multi-Description Coding (MDC) [12] and spatial Flexible Macro-block Ordering (FMO) [13] as a way to save the video frames from the error-prone wireless channel. Referring to the main concept of FMO, an error resilient mechanism for H.264/AVC would be achieved. The video frames will be divided into several slices in order to cope with the lost macro-blocks of neighbor slices. Yet, this concept could not be fully on board with a scenario whereby a video frame-carrying vehicle experiencing a wireless channel quality disturbance due to some circumstances related to error rates, delay or interferences. Thus, when the essential slices of the origin video come to a relay vehicle/RSU with low offered channel characteristics, a massive distortion will be occurred on the playback video in the destined vehicle. Therefore, we could say a sensitive model/algorithm should be considered here to wisely select the next relay hope to be utilized in the video's frames forwarding process.

An attempt to study the wireless channel characteristics an evaluation based on the GloMoSim [14] simulator and additive propagation model [15] that uses a path loss model with multi-path fading was conducted in order to take into attention the signal obstruction and attenuation. The Rician fading model was considered to incorporate the multi-path interference to the vehicles communication, which comprises one line of sight and several non-lines of sight components in the received signal. The authors have interpreted from the obtained results the phenomena that different mobility models will lead to an overhead and packet loss in the vehicular networks. The main points that we want to share here are the high movement of vehicles will usually lead to for degradation with the vehicular network performance, which inquires an accurate mobility model during the evaluation of video carrier hope. Besides, when the error of the wireless channel increases, the fading factor of Rician distribution increases. As significance, the vehicular network performance is degraded, exposing the effect of multi-path fading on the performance of the network. Hence, it is important to note that during the development of a video routing algorithm, a special consideration should be given for the Geographical information (GIO) as well as the wireless channel characteristics.

Peer-to-peer (P2P) content distribution is observed to be a cutting-adage trend in vehicular networks. One of the main applications of P2P multimedia services is the vehicular Videoon-Demand (VoD), which offers edited video file to the vehicles on the road. Improvement the QoE of VoD applications is a crucial requirement. For that purpose, the authors in [1] have proposed interactive quality-aware user-centric mobile VoD mechanism for VANET (QUVoD). It is important to highlight that the QUVoD is running based on multi-homed P2P/VANET architecture and mechanisms for storing video frames, video segment retrieval, multi-path packet forwarding. Though the simulation results have shown that it performs as compared with the state-of-the-arts approaches, this kid of proposed architecture in most cases will lead for a centralized kind of solution that enables versions limitations in the large scale from.

Under other way, to develop a receiver-based packet forwarding mechanism that helps in mitigating delay of routed video packets towards destination; Rezende et al. in [17] evaluated the performance of the proposed approach for video transmission over wireless Ad Hoc networks. The authors evaluated their proposal in terms of successful delivery rate and enhancement of video transmission quality, of two erasure techniques named random linear network coding [18] and xor-based coding [19]. They have concluded that using xor-based mechanism, the bulk video file content is recovered at the receiver vehicle. From their study a recommendation was given by considering the network size, Bit rate and Mobility factors a better quality of transmitted video over wireless Ad Hoc networks.

Another efforts were given to efficiently broadcast video applications to vehicles in the urban areas. The authors in [16] have proposed Streaming Urban Video (SUV). The SUV maintains video communication based V2V. An attention was given for tuning the transmission time slot of vehicles in video forwarding progress. For attaining this objective, a graph-coloring algorithm is used to calculate the value of time slots and a group of relay vehicles that they transmitting video over a specified time slot. They have also highlighted in their proposed algorithm that considering link quality of the selected relay vehicle reflects directly to the resolution of the transmitted video over VANET.

In different attempt, in [21] a novel video source decision scheme is proposed. Cluster and Dynamic Overlay based video delivery over VANETs (CDOV) was introduced. Using CDOV scheme, nodes are clustered based on the correlation of the video requirement/supply and moving features. Though, there was a shortcoming by not take in account some effective vehicular network factors which can contribute in forward the video's frames in an optimal way to deliver them over vehicular networks.

From the given discussions in this section, we can identify there is a glaringly need for developing an efficient video forwarding algorithm in VANET environment. Therefore, in this paper we proposed a video geographical forwarding algorithm, which can maintain the video streaming among selected vehicles in balanced form to enable reporting road status for the seek of safe traffic as an application of IoV.

3 PROPOSED VIDEO GEOGRAPHICAL FORWARDING ALGORITHM (VGF) BASED VIDEO CONTENT DELIVERY SCHEME (VCD)

This study is aiming to develop a routing algorithm that can optimally forward the frames of the video file in vehicular networks. This is achieved by fairly selecting neighbour candidate vehicles to forward the packet towards the destination. The forwarding process was made based on ranking algorithm, which is performed by the video carrier vehicle. The frames are classified, based on their higher importance, as I-frames to be inserted to base layer that is denoted by tid=0, P-frames as enhancement layer 1 is identified by tid=1, and B-frames as enhancement layer 2 is classified by tid=2. Its important mentioning that in our proposed VGF algorithm a H.264/SVC method [12] was implemented in order to coding/decoding the forwarded video. Fig 2 illustrates the scenario of proposed architecture of our algorithm.

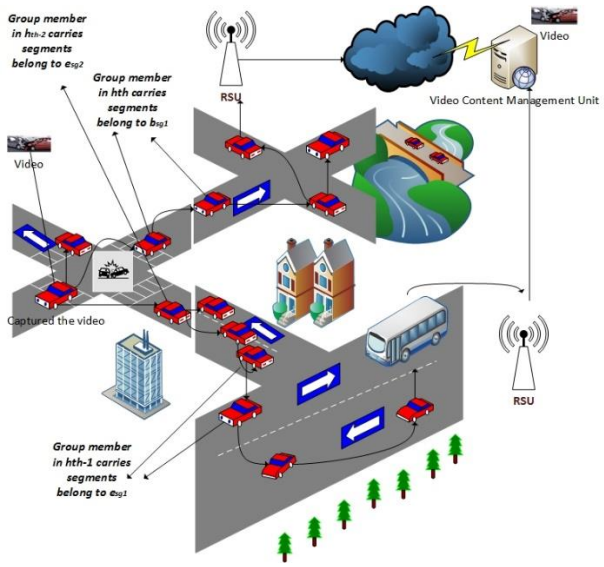


Figure 2: Proposed architecture of Geographical Forwarding Algorithm based Video Content Delivery

3.1 Enhance and Adapt Input Parameters for Reporting Video over VANET by Developing Mathematical Equations

Particularly**,** the video carrier vehicle ranks the neighbour vehicles based on several key important metrics. Afterwards, the most important layer, which is base layer, is forwarded to the highest ranked neighbour vehicle, the enhancement layer 1 is assigned to the second highest ranked neighbour vehicle and eventually the enhancement layer 2 is assigned to the third highest ranked vehicle. For example, the vehicles that ranked in the higher-level h_{th} will store the content of the first segment of base layer 1 b_{sg1}, the vehicles in the group second highest ranked h_{th-1} will obtain a second priority of storing the content of segmented video frames of enhancement layer 1 e_{sg1}, followed by the defined third highest ranked group of the vehicles in group h_{th-2}, holding segmented frames of enhancement layer 2 e_{sg2} , and so on.

Those video frames will then be assembled by the receiving vehicle/authority center, using H.264/SVC method [12] in decoding and playback the received video file. Accordingly, though the video stream could feel like a particular asset to the end user, which is in fact an integration of several packets (or video segments) as away to deliver the video content. The time taken in this process is proportional with the geographical distance between source and destination. As a way to facilitate the proposed video content delivery scheme, an approach of H.264/SVC was improvised to divide video packets into various segment, as was mentioned earlier. These created segments can be encoded and decoded independently. These segments can also be integrated back to produce the original packet sent by source vehicle. This enables video streaming more flexibility, particularly as several packets are needed to shape a video. It is important to mention that in our proposed scheme we introduced to replicate the video segments of h_{th} in the highest ranked vehicle that belongs to bsg1 to support delivering the high quality content of sent video whenever the content of that video is demanded by a neighbouring vehicle, the time of cashing this content will rely on the buffer size of vehicle i.

The ranking process of relay-vehicles was performed taking into consideration four main quality aspects. Top priority video frames that were saved in tid0 are forwarded to the vehicle achieved high rank score compared to others. Whereas, lower priorities tid1 and tid2 are forwarded to next lower ranked nearby vehicle to the top ranked vehicle accordantly. The ranking process will be made based on a developed scoring mathematical model that Considering the current beacon reception rate, forwarding progress and the geographical direction to destination, in addition to residual buffer length; the proposed algorithm can elect the best

candidate to forward the frames belong to base layer followed by enhancement layers′s video frames to the next highest ranked vehicles. Thus, the video quality over vehicular networks could be efficiently improved. The following GIO and wireless channel factors are considered in developing our proposed algorithm:

Beacon Reception Rate (BRR): As one of the main key factors that indicating the quality of neighbour vehicles is the rate of received beacons. In our proposed routing algorithm when a video carrier vehicle is in- tending to send the frames that categorized under tid0, it extracts the computed values of beacon delivery of wireless channels of the neighborhood vehicles. This can be measured by determining BRR distributed by each vehicle and then broadcast the BRR to the vehicles in the vicinity through beacon handshaking. The value of BRR is very significant as it is used in the process of neighbour selection to forward video frames towards the destination.

In fact, in order to precisely identify the accurate number of beacons that received by vehicle candidate i from source vehicle j, different factors are contributing in the determination of BRR need to be considered. For instance, BRR is normally affecting by the vehicle density in vehicular wireless network. By passing the time, the number of vehicles is fluctuating and opposite Probability of BRR (PBRR) is decreasing due to the collision phenomena, which is caused by high channel load. In the ideal channel status, the channel can go up to maximum load 1 without collisions.

A normalized vehicular wireless channel model could be formed to present the maximum or upper-bound of utilization rate of a candidate vehicle′s channel by the time of selection in our proposed video forwarding scheme. Considering the beacon generation rate γ_g by a wireless channel and the time duration of beacon to be traveled via vehicular wireless medium TD to its destination, in addition to the number of vehicles in the range of transmission V_{no}; the value of Normalized Maximum Supported Channel Utilization Rate (NMSCUR) of vehicle *i* can be calculated in Equation 1.

$$NMSCUR = V_{no} \cdot \gamma_g . T_D \qquad (1)$$

T_D can be modeled as follows:

$$T_D = T_{(PLCP_{Header}+PLCP_{Preamble}+PLCP_{data-whitener})} + \frac{Beacon-Size}{Data-Rate} \qquad (2)$$

Where $T(PLCP_{Header}+PLCP_{Preamble}+PLCP_{data-whitener})$ is time needed to transmit the Physical Layer Convergence Procedure (PLCP) header, PLCP preamble and PLCP data-whitener of a beacon frame. Moreover, the Beacon-Size measured by (bits) in addition to Data-Rate measured by (bit/second), are considered which reflected on the value of NMSCUR. The γ_g identifies how often per second a vehicle generates a beacon. This value directly influences the NMSCUR in Equation 4. The beacon frames considered to be generated at a fixed rate of 10 Hz or 10 beacon/second [69].

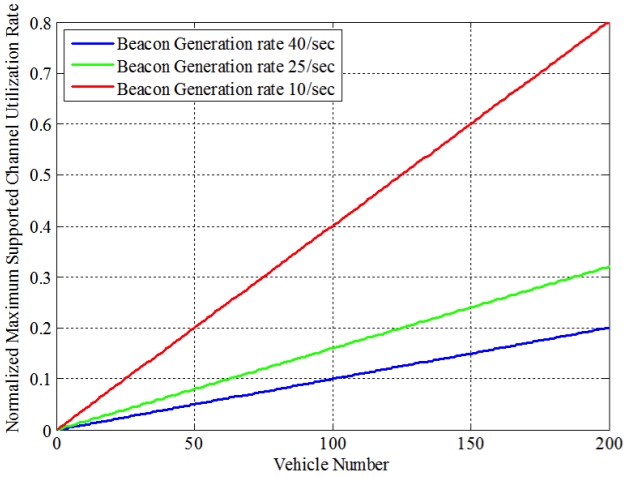


Figure 3: Normalized Maximum Supported Channel Utilization Rate with Changes in V_{no} and γ_g.

We can figure out from graphs presented in Fig 3, the behavior of NMSCUR with three different γ_g 10, 25 and 40 beacon/second rates. The highest value NMSCUR could be achieved as 0.80 with 200 vehicles when the γ_g was equal to 10 beacon/second. While it was 0.32 and 0.20 when the γg was set to 25 and 40 beacon/second respectively. The reason is that when the channel load became very high by the time of increasing the γ_g, which is leaded to drop the performance rapidly. We should note that, due to the features of radio channel, some degree of beacons might not arrive due to the high congestion rate caused by many vehicles generating

beacons with high γ_g. Thus, the vehicular wireless channel can support less utilization of recourses with high γ_g and high dense network.

On the other hand, as a way to investigate more on the factors that affecting the BRR, the number of transmission slots should be also considered [70]. During each transmission slot time, (the slot time in 802.11e is 13 Micro second), a time duration normally spent which is equivalent to the duration needed to transmit a beacon, TD. When a beacon does not reach its destination within TD, this beacon will be expired and a newly beacon will be generated. The time duration of these new regenerated beacons is calculated as:

$$T_{Newg} = 1/\gamma_g \quad (3)$$

Hence, from the previous discussion the number of transmission slots can be modeled as follows:

$$Slot_{no} = T_{Newg}/T_D \quad (4)$$

Forwarding Progress (FP): In our proposed video forwarding scheme when a video source vehicle is between intersections, it calculates the FP of the intermediate vehicles. This metric indicates the packet forwarding progress towards the destination and it is generally computed as a prediction of distance by Equation 5, where D_i is the distance of an intermediate vehicle to the destination and D_s is the distance of the source vehicle to the destination.

$$D_{predicted} = D_s / D_i \quad (5)$$

Direction (D): In vehicular environment, vehicles are traveling in the same or opposite directions; thus, the streets and intersections restrict their direction. Due to this bipolar movement of vehicles, vehicles that are traveling in the same direction have stable route as compared to the vehicles that they travel in opposite direction. Therefore, we consider this vehicular mobility characteristic to make the source vehicle to give higher priority to an intermediate vehicle that travel in the same direction with source. The relative direction between a vehicle and other coordinates is computed by determining the angle between direction vector of a vehicle and x-axes with y-axes.

The obtained angle degree value is limited in the range between -1 (when θ= 180, opposite side) to 1 (when θ= 0 same side). In other words, when vehicles are traveling on the highways most probably the angle degree between vehicles is either -1 (interconnection with opposite side) or 1 (same side connection), this is due to the highway-restricted direction as we mentioned before. On the other hand, when vehicles are moving in urban area the angle degree is more varied. Therefore, the obtained angle value is considered by our proposed VGF algorithm to insure the video frames that belong to base layer are forwarding to the most directed V_i to V_d.

The bearing angle (θ) between a Vd and Vi can be calculated as follows:

$$\cos\theta = \frac{V_{d_{x1}} \cdot V_{i_{x2}} + V_{s_{y1}} \cdot V_{i_{y2}}}{\sqrt{V_{d_{x1}}^2 + V_{d_{y1}}^2} \cdot \sqrt{V_{i_{x2}}^2 + V_{i_{y2}}^2}} \quad (6)$$

Residual Buffer Length (RBL): As a fourth ranking metric that was utilized in our VGF algorithm in forwarding the top priority video frames tid0, is the Residual Buffer Length (RBL) of vehicle candidate Vi. When a source vehicle V_s intending to elect one vehicle for forwarding the video frames, it should be aware the value RBL of intermediate vehicles, especially during the process of forwarding base layer′s frames. In case a V_i has a very low RBL, this vehicle should not be chosen for forwarding process, or a less impact frames could be sent for that vehicle such as tid1 and tid2. When tid0 packets are forwarded to this vehicle with low RBL, it might be easily dropped due to full of buffer. For this reason, the RBL was considered as one of the criteria in our developed VGF algorithm.

Based on [12], the maximum Buffer Length (BL) is set to 50 packets. Hence, we set this value to be implemented into vehicles in our simulation. By the time of V_i is utilizing in video forwarding process the value of BL is varying between 0 to 50. Accordingly, we implemented in a way to make the vehicles sharing among them the up changes happening on this value frequently elaborating beaconing services. Consequently, the value of BL is calculated by each V_i as a RBL and afterward broadcasted it every time period based on γ_g settings. Thus, V_s is aware about recent RBL values of its neighbours before make the forwarding decision of top priority video frames of base layer using our VGF algorithm.

3.2 VGF-based Multi-Score Function

The proposed VGF algorithm ranks neighbor intermediate vehicles according to the above four routing metrics. But, a score function is necessary to combine all metrics in a single one. This score function favors link quality, packet progress towards

destination, link stability and availability in buffer storage capacity instead of considering only a single metric for packet forwarding. We proposed the multi-metric scoring function to combine BRR, FP, D and RBL metrics.

Assume that a score function combines k routing metrics $j = \{j1, j2, j3, ..., jk\}$. For each jk intermediate vehicles have minimum and maximum values $[minjk\ to\ maxjk]$. Thus, a multi-score function is defined as follows:

$$f(\Gamma_{j1},\Gamma_{j2},\Gamma_{j3},\Gamma_{j4},...,\Gamma_{jk}) = X \times \Gamma_{j1}^{\sigma_1} \times \Gamma_{j2}^{\sigma_2} \times \Gamma_{j3}^{\sigma_3} \times \Gamma_{j4}^{\sigma_4} .....\Gamma_{jk}^{\sigma_i} + SP_{max} \quad (7)$$

Where SP_{max} stands for selection probability and denotes maximum value of the score function $f(j1, j2, j3, j4, ..., jk)$, X is defined as a variable that depends on the maximum value of routing metrics and weights, and $(1, 2, 3, 4...., i)$ are denoted as weights that are used to give higher priority to a specific routing metric. In the proposed VGF algorithm, four metrics have been considered for video packet forwarding decisions. Thus, the probability value of an intermediate vehicle selection is calculated as follows:

The $f(BRR_j, FP_j, D_j, RBL_j)$ value reaches maximum when their derivative equal to zero. Thus, X is expressed as follows:

$$f(BRR_j,FP_j,D_j,RBL_j) = X \times BRR_j^{\sigma_1} \times FP_j^{\sigma_2} \times D_j^{\sigma_3} \times RBL_j^{\sigma_4} + SP_{max} \quad (8)$$

$$X = \frac{-SP_{max}}{BRR_{max}^{\sigma_1} \times FP_{max}^{\sigma_2} \times D_{max}^{\sigma_3} \times RBL_{max}^{\sigma_4}} \quad (9)$$

4 PERFORMANCE EVALUATION

In this section, the performance evaluation of our propose VGF algorithm based VCD is presented and discussed. It is important to highlight, we have implemented our proposed algorithm along with the benchmarked methods (GPRS and DSDV) using NS2 simulator. The simulation area was set to 3000 * 3000 m^2, wireless channel interfaces IEEE802.11e/p, with frequencies of 5.8 and 5.9 GHz respectively, data rate was set up to maximum 11Mbps with channel sharing based CSMA/CA, transmission power up to 33dBm and transmission rage of 250m. The video format source file is set to YUV CIF (352 x 288), MPEG-4 codecs, namely the NCTU codec. The simulated vehicles are moving with an average up to 30m/s. The simulation results are collected out of an average of 10 independent runs. Fig 4 illustrates the average PSNR obtained via the numerical analysis as well as the simulated results. PSNR is one of the common objective metric that used in evaluating the level quality of transmitted video. The PSNR was measured as the difference between a reconstructed video file and the original video trace file. Each vehicle before transmitting a video, a reference PSNR value is calculated by matching the reconstructed encoded video and the original raw video. Afterwards, when the video has transmitted, the PSNR is calculated at the receiver vehicle for the reconstructed video for any feasible damaged video sequence received. The variance between the PSNR values at the sender and receiver vehicles was used to evaluate the transmission effects on video quality at the application level. As we can observe on Fig 4, the performance of our algorithm was constructively improving while the number of vehicles is increasing in the simulated scenario.

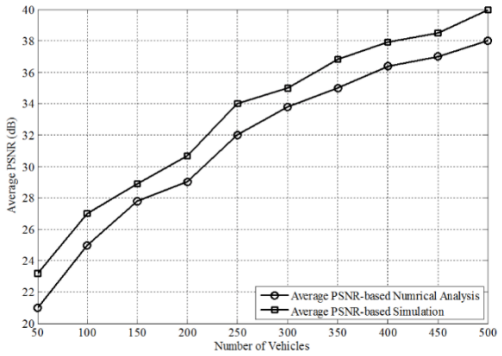


Figure 4: Average PSNR-based Simulation and Numerical Analysis with Impact of Vehicle Number.

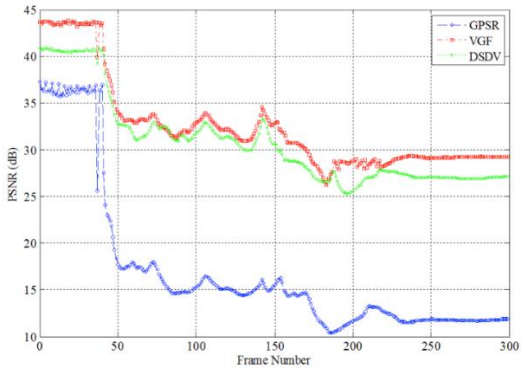


Figure 5: PSNR Comparison Obtained with Different Frame Numbers using VGF based VCD, GPSR and DSDV Routing Algorithms.

Fig 5 shows the obtained PSNR using our proposed VGF algorithm based VCD in comparison with GPSR and DSDV. It is observable that our proposed algorithm could maintain in average improved PSNR while the number of transmitted frames is increasing during the simulation time. We could relate that to the reason our proposed algorithm considering dynamically the developed evaluation metrics could improve the performance notably. Moreover, the new concept of VCD has contributed to the fact of load balancing and maintains the high priority segmented frames to get transmitted via high quality route.

4 CONCLUSIONS

In summary, we proposed Geographical Forwarding Algorithm based Video Content Delivery scheme as an initial version of an efficient video reporting approach where can assist the smart video surveillance vehicles in efficiently and instantly report road incidents and information with considering multifactor scoring function that assist in selecting relay vehicles maintain high level of QoE. In this paper the proposed architecture of our scheme was presented and discussed. Important highlighting that the video forwarding process is performed taking in account ranking the available neighboring vehicles to the vehicle in forwarding progress before transmitting the video frames using our proposed multi-score function. Considering the current beacon reception rate, forwarding progress and direction to rescuing authorities, in addition to residual buffer length; the proposed scheme could elect the best candidate to forward the video frames to the next highest ranked vehicles in a balanced way. Furthermore, a new concept was introduced in this paper that was implemented at the MAC layer of each vehicle. It helped in grouping the video frames into three categories (as was discussed in section 3) and deliver them based on the content priority to the ranked surrounding relay vehicles. Simulation results have demonstrated the efficiency of our proposed algorithm in improving the perceived video quality compared with other approaches.

REFERENCES

[1] Changqiao Xu, Futao Zhao, Jianfeng Guan, Hongke Zhang, and G-M Muntean, 2013. Qoe-driven user-centric vod services in urban multihomed p2p-based vehicular networks. Vehicular Technology, IEEE Transactions on, 62(5):2273–2289.

[2] Heiko Schwarz, Detlev Marpe, and Thomas Wiegand, 2007. Overview of the scalable video coding extension of the h. 264/avc standard. Circuits and Systems for Video Technology, IEEE Transactions on, 17(9):1103–1120.

[3] Yung-Cheng Chu and Nen-Fu Huang. Delivering of live video streaming for vehicular communication using peer-to-peer approach. In 2007 Mobile Networking for Vehicular Environments, pages 1–6, Anchorage, AK, 11-11 May 2007. IEEE.

[4] Mahdi Asefi, Sandra C´espedes, Xuemin Shen, and Jon W Mark, 2011. A seamless quality-driven multi-hop data delivery scheme for video streaming in urban vanet scenarios. In Communications (ICC), IEEE International Conference on, pages 1–5, Kyoto, 5-9 June.

[5] Boris Bellalta, Evgeniy Belyaev, Magnus Jonsson, and Alexey Vinel, 2014. Performance evaluation of ieee 802.11 p-enabled vehicular video surveillance system. IEEE, Communications Letters, 18(4):708 – 711.

[6] Evgeny Belyaev, Karen Egiazarian, and Moncef Gabbouj, 2013. A low-complexity bit-plane entropy coding and rate control for 3-d dwt based video coding. IEEE Transaction on Multimedia, 15(8):1786 – 1799, IEEE.

[7] Shouzhi Xu, Huang Zhou, Zhao Yu, and Shuibao Zhang, 2012. Simulated study on video communication over vanet. In Proceedings of the 2012 World Automation Congress (WAC), pages 221–225. Mexico: IEEE,24-28 June.

[8] Chih-Heng Ke, Cheng-Han Lin, Ce-Kuen Shieh, and Wen-Shyang Hwang, 2006. A novel realistic simulation tool for video transmission over wireless network. In Proceedings of the IEEE International Conference on Sensor Networks, Ubiquitous, and Trustworthy Computing, pages 221–228. Taiwan: IEEE, 5-7 June.

NS. Network simulator, January 2017.http://nsnam.isi.edu/nsnam/index.php/Main Page.
VANETMobiSim. Mobility model, January 2017. http://vanet.eurecom.fr.
[9] Nadia N Qadri, Martin Fleury, Muhammad Altaf, and Mohammed Ghanbari, 2010. Multi-source video streaming in a wireless vehicular ad hoc network. IET on Communications, 4(11):1300–1311. IET
[10] Chih-Heng Ke, 2012, myevalsvc: an integrated simulation framework for evaluation of h. 264/svc transmission. KSII
[11] Transactions on Internet & Information Systems, 6(1).
Cristiano Rezende, et. al, 2012. Virtus: A resilient location-aware video unicast scheme for vehicular networks. In Proceedings of the 2012 IEEE International Conference on Communications (ICC), pages 698–702. Ottawa: IEEE, 10–15
[12] June.
Azzedine Boukerche, Cristiano Rezende, and Richard W Pazzi, 2009. Improving neighbor localization in vehicular ad hoc networks to avoid overhead from periodic messages. In Proceedings of the IEEE Global Telecommunications Conference,
[13] GLOBECOM, pages 1–6. Hawaii: IEEE, 30 November–4 December.
C. Rezende, M. Almulla, and A Boukerche, 2013. The use of erasure coding for video streaming unicast over vehicular ad hoc networks. In Proceedings of the IEEE 38th Conference on Local Computer Networks (LCN), pages 715–718. Sydney: IEEE, 21-24 Oct.
[14] Fabio Soldo, Claudio Casetti, C Chiasserini, and Pedro Alonso Chaparro, 2011. Video streaming distribution in vanets. IEEE Transactions on Parallel and Distributed Systems, 22(7):1085–1091. IEEE.
Lina Zhu, Changle Li, Yun Chen, and Bingbing Li, 2015, On Dynamic Video Source Decision in VANETs: An On-Demand Clustering Approach, International Journal of Distributed Sensor Networks, http://dx.doi.org/10.1155/2015/436810
[15] Mun-Yee Lim. et al, 2016, Cognitive radio network in vehicular ad hoc network (VANET): A survey, Cogent Engineering, http://dx.doi.org/10.1080/23311916.2016.1191114
Arpana Shetty, Ashwini B, and Manasa S, 2016, Performance Analysis of Routing Protocol for Video Streaming in Vehicular Network, International Journal of Innovative Research in Computer and Communication Engineering, Vol.4, Issue 4, pp: 7399-7404
Abdelhamid Mammeri, Azzedine Boukerche, and Zhifei Fang, 2016, Video Streaming Over Vehicular Ad Hoc Networks Using Erasure Coding, IEEE SYSTEMS JOURNAL, VOL. 10, NO. 2, pp. 785-796
M. D. Felice, E. Cerqueira, A. Melo, M. Gerla, F. Cuomo, and A. Baiocchi, "A distributed beaconless routing protocol for real-time video dissemination in multimedia VANETs," Computer Communications, no. 1, pp. 1–13, 2014. [Online]. Available: http://www.sciencedirect.com/science/article/pii/S0140366414002990.

Ali Safaa Sadiq (Senior Member, IEEE) received the B.Sc., M.Sc., and Ph.D. degrees in computer science in 2004, 2011, and 2014 respectively. He is currently a Faculty Member of the Faculty of Science and Engineering, School of Mathematics and Computer Science, University of Wolverhampton, U.K. He is also an Adjunct Staff with Monash University, Malaysia. He has served as a Lecturer with the School of Information Technology, Monash University. Previously, he has also served as a Senior Lecturer with the Department of Computer Systems and Networking Department, Faculty of Computer Systems and Software Engineering, University Malaysia Pahang, Malaysia. His current research interests include wireless communications and network security.

Kayhan Zrar Ghafoor [S'10, M'15, SM'19] is currently working as a visiting researcher at the University of Wolverhampton and an associate professor at the University of Salahaddin University-Erbil. Before that, he was a postdoctoral research fellow at Shanghai Jiao Tong University and a visiting researcher at University Technology Malaysia. He received the B.Sc. degree in electrical engineering from Salahaddin University, the M.Sc. degree in remote weather monitoring from Koya University, and the Ph.D. degree in wireless networks from University Technology Malaysia in 2003, 2006, and 2011, respectively. He has published over 45 scientific/research papers in ISI/ Scopus indexed international journals and conferences. He has authored two books, Cognitive Networks: Applications and Deployments and Privacy and Cybersecurity in Smart Cities. He is the recipient of the UTM Chancellor Award at the 48th UTM convocation in 2012.

CHIH-HENG KE received the B.S. and Ph.D. degrees in electrical engineering from National Cheng-Kung University in 1999 and 2007, respectively. He is currently an Associate Professor with the Department of Computer Science and Information Engineering, National Quemoy University, Kinmen, Taiwan. His current research interests include multimedia communications, wireless networks, and software-defined networks

V-CARE: A Blockchain Based Framework for Secure Vehicle Health Record System

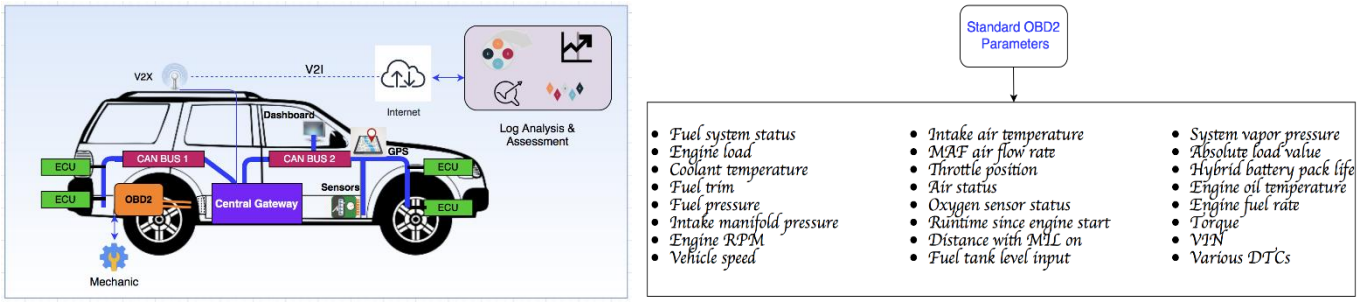
Pranav Kumar Singh, Roshan Singh, and Sukumar Nandi
Department of Computer Science and Engineering
Indian Institute of Technology Guwahati, Assam 781039, India

Abstract

One of the biggest challenges associated with connected and autonomous vehicles (CAVs) is to maintain and make use of vehicles health records (VHR). VHR can facilitate different entities to offer various services in a proactive, transparent, secure, reliable and in an efficient manner. The state-of-the-art solutions for maintaining the VHR are centralized in nature, mainly owned by manufacturer and authorized in-vehicle device developers. Owners, drivers, and other key service providers have limited accessibility and control to the VHR. We need to change the strategy from single or limited party access to multi-party access to VHR in a secured manner so that all stakeholders of intelligent transportation systems (ITS) can be benefited from this. Any unauthorized attempt to alter the data should also be prevented. Blockchain is one such potential candidate, which can facilitate the sharing of such data among diff erent participating organizations and individuals. For example, owners, manufacturers, trusted third parties, road authorities, insurance companies, charging stations, and car selling ventures can access VHR stored on the blockchain in a permissioned, secured, and with a higher level of confidence. In this paper, a blockchain-based decentralized secure system for V-CARE is proposed to manage records in an interoperable framework that leads to improved ITS services in terms of safety, availability, reliability, efficiency, and maintenance. Insurance based on pay-how-you-drive (PHYD), and sale and purchase of used vehicles can also be made more transparent and reliable without compromising the confidentiality and security of sensitive data.

I. Introduction

Modern vehicles have a complex mechatronic structure, which is not only a mechanical system of engine, brakes, gearbox, accelerator; now, it is like a networked computer on wheels (NCoW) with sophisticated control, sensing and communication layers and over millions of lines of code [1]. Fig. 1a illustrates the typical in-vehicle subsystem, which comprises sensors, actuators, Controller Area Network (CAN), Electronic Control Units (ECUs), GPS, Vehicle-to-Everything communication (V2X), On-Board Diagnostic (OBD) framework, Onboard Unit (OBU), central gateway, etc. [2].



(a) VHR from In-Vehicle Network Architecture (b) Standard OBD2 Parameters

Fig. 1: Functional Diagram of Common VHR Monitoring and standard OBD2 Parameters

There are different protocols for data exchange between inter-subsystem (ECUs) and intra-subsystem (within each subsystem) such as CAN (powertrain sensors, transmission, engine controller), CAN with Flexible Data Rate (CAN-FD), FlexRay (Airbag, chassis, steering, brake control), Local Interconnect Network (LIN) (instrument cluster, door, seat, light, climate, seat, light, climate), Media Oriented Systems Transport (MOST) (phone, audio, display, navigation),

and Ethernet. The data from different ECUs is accessible via the central gateway to authorized persons. The OBD2 protocol specified in SAE J1979 can also log a range of vehicle data. Some of the standard OBD2 parameters are listed in Fig. 1b. OBD2 provides access to data that indicates the status of the various subsystems to the vehicle owner or the mechanic cable/Bluetooth/hotspot/cloud access. The raw data collected via OBD2 and gateway data is transmitted to the cloud through the vehicle-to-infrastructure (V2I) communication and stored as VHR, which is used for intelligent analysis (diagnostics) and assessments (prognostic) using APIs. Diagnostics is analysis of current state of vehicle subsystems whereas prognostic is assessment of the future state of vehicle subsystem [3]. The owners/drivers access these details on their smartphones/dashboards via apps provided by the cloud service providers (manufacturer/trusted third party).

A. Problem Definition

The state-of-the-art solutions for VHR are centralized, which is based on cloud-based solutions. The present system is dedicated only to diagnostic and prognostic purposes i.e., finding the existing faults and predicting the future faults. Though such vehicle health monitoring systems provide clear benefits to owners/drivers for the maintenance of their vehicles, the data from vehicles ECUs can create additional opportunities in terms of safety, services , insurance, EV-charging, sales and purchasing of used vehicles, analysis of driving behavior, etc. However, these value additions require a change in the traditional deployment strategies, and there are serious issues that need to be addressed such as security, privacy, data consistency, access control, performance, availability, reliability, level of transparency, etc.

B. Related Work

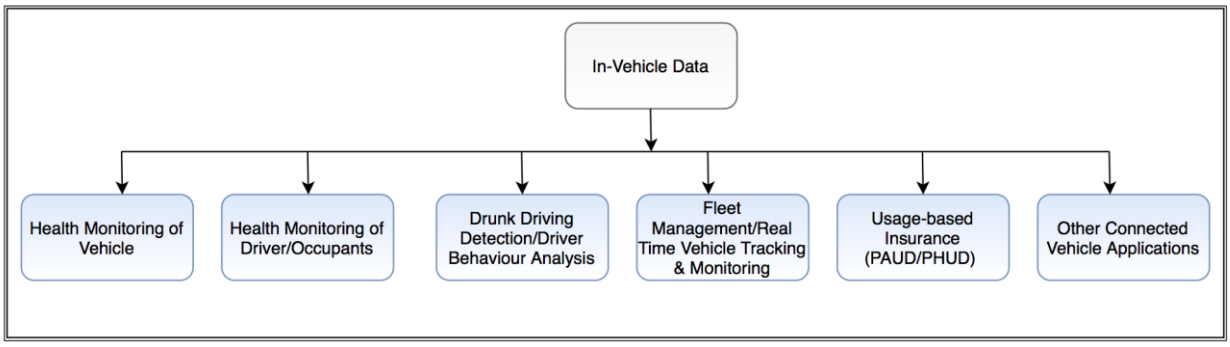


Fig. 2: In-Vehicle Data Applications

Several years of research on capitalizing the in-vehicle data (from sensors/ECUs) have resulted in various applications [3], [4], [5], [6], [7], [8], [9] as illustrated in Fig. 3. With the explosion of sensors and the revolution in telematic and radio access technologies (RATs), a normal vehicle has become a connected and autonomous vehicle. However, there is a lack of a common, decentralized and secure internet-of-vehicle (IoV) platform that can facilitate all of these applications not only for a few individuals but also for other key service providers by recording, analyzing and evaluating big data from vehicle sensors and ECUs.

C. Motivation, Contribution and Organization

Vehicle Health Records are confidential information and require a high level of security and privacy to be dealt with. The access to the VHR can be logged onto the blockchain increasing the transparency on data access made by different stakeholders of the systems. Logging the data onto the public blockchain will also make data audability easier. The VHR hashes can be encoded and stored on distributed nodes of the Blockchain. Blockchain-based VHR framework can facilitate security, privacy, immutability, and required levels of accessibility, control, and transparency. The VHR (a portion of it or full) in the Blockchain can be automatically sent to the ITS service providers, insurance companies, manufacturers, concerned mechanics, and other parties securely.

Our twofold contributions are proposing a novel blockchain-based VHR architecture to enable various useful services in IoV and provide a summary of how it can be implemented. This paper presents an approach of capitalizing

VHR not only for real-time health monitoring of the vehicle but also for various other important services that a vehicle may need in a secured manner. One can extend our framework to solve many other real-life problems of IoV and its associated services.

The rest of the paper is organized as follows: Section II contains the details of proposed system architecture. We discuss our goals in Section III and finally Section IV presents conclusion and future work.

II. Overview of the V-CARE Architecture

In this section, we discuss the system model and working principles of the proposed V-CARE architecture shown in Fig. 3. We consider the flourished stage of IoV, with RSU, fog nodes, cloud, connected and smart vehicles, and other digitally-driven services.

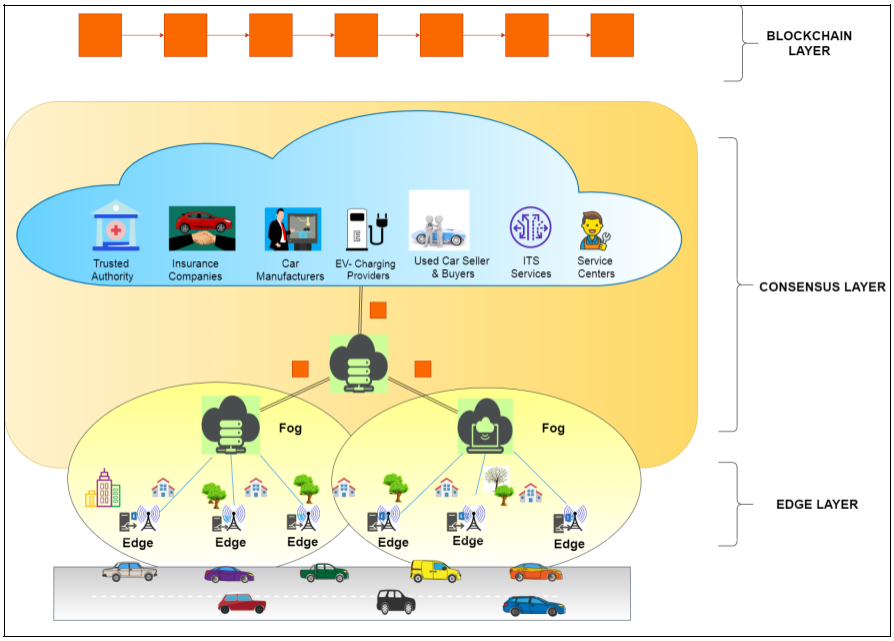


Fig. 3: Proposed V-CARE Framework

A. *Entities involved*

1) Vehicles: The vehicles are equipped with sensors, ECUs, OBUs, data loggers (CAN, OBD-II, LIN, etc.), communication (V2V and V2X), storage, and computing facilities.

2) *RSUs:* The roadside units are deployed to support V2I/I2V connectivity. The connectivity is secure and can be used for data download/upload, over-the-air updates, etc [10]. The front-haul is wireless, and the back-haul is a wired backbone network and also securely connects the fog nodes.

3) Regional Fog computing nodes: The area selected can be segregated into small regions depending on traffic loads and peak hour analysis of entering and leaving vehicles. We propose fog nodes (FNs) in those regions with connectivity to one or more RSUs.

4) Trusted Authority: The trusted authority (TA) is a central entity using a PKI-based authentication and responsible for the registration of the vehicles, RSUs, regional fog nodes, and service providers. The TA issues cryptographic materials and security mechanisms to be employed in IoV. The TA maintains a global contract, Registry Contract (RC), that maps registered identity strings to Ethereum addresses, i.e., addresses on the blockchain. The entries available in RC link each entity to their activity contract.

5) Service Providers: As we have mentioned, these entities could be manufacturers, insurers, ITS administration, and other service providers. These service providers use a cloud-based system for data storage, processing, analysis, and assessment.

B. Blockchain Related Terminologies

Blockchain has emerged as a disrupting technology over the last few years and has attracted interests from both industries as well as from the academic research community. With its inherent features of decentralization, fault-tolerance, non-reputability, high availability, high security, and reducing the need for trust, the technology is viewed as one of the contenders for solving some of the crucial challenges in the field of Finance, Supply chains, IoT and cloud computing.

1) Fundamentals of Blockchain:: Blockchain gained global attention with the introduction of Bitcoin[11], a peer-to-peer payment system based upon cryptographic primitives. A blockchain is made up of a number of blocks where each block contains one or more number of transactions that are digitally signed by the users executing them with Public Key Scheme. These blocks are chained with each other with the help of cryptographic hashes, where each block in the chain points to its previous block. A blockchain can be conceptualized as a single linked list where one can traverse through the entire historical records following the links to the date of initialization of the chain.

Blockchain being a distributed system, requires a mechanism to make the nodes in the system agree to a consistent system state at a particular instance of time [12]. This is also sometimes known as reaching a consensus. There exist three types of nodes in a blockchain network:

- Light Node: These are low-end resource-constraint devices such as a smartphone.
- Full Node: These are the devices having sufficient storage capability but may not have a well computational facility.
- Miner Nodes: These are the devices having sufficient storage capability and high computational resources.

The responsibility of maintaining the blockchain network and making the nodes in the network reach a consensus state lies with the miner nodes. Miner nodes compete among themselves in order to solve a cryptographic challenge thrown out to them by the system.

2) Smart Contracts to be used in V-CARE:

a) Registry Contract (RC): The Trusted Authority (TA) is responsible for deploying the Registry Contracts (RCs). RCs provide information such as the date of registration of a vehicle, date of expiry of the license, addresses of valid cloud service providers (CSPs), etc. Vehicle owners, as well as the CSPs, need to approach the TA for the registration. The registration details are bound to the pseudonymous identifiers or the addresses, which corresponds to the identity of the entity in the real world. The mapping details of the entities to their pseudonymous identity is only known to the TA.

b) Vehicle-Service Provider Relationship Contract (VSRC): It defines how data will be managed and accessed by various entities. It contains an array of data pointers and corresponding access permissions that identify the records available at service providers. It is issued for pairwise data interaction between the vehicle and the service providers. The interaction happens through the execution of a query string available with data pointers. After the execution, it will return a subset of vehicle data. The query string is attached to the hash of the returned data to ensure integrity. Each such string specifies a portion of the vehicle's data that any service provider is allowed to access. VSRC also defines the terms of use of the data accessed by an entity.

c) Activity Contract (AC): VSRCs are linked through references available in ACs, so that vehicle records can be unified as a whole as and when required. Thus, it maintains a list of references to VSRCs, representing the previous and current interactions among various entities of the system. The ACs also facilitate essential backup, restoring, and notification functionalities. Vehicles can leave several times; however, get back to their history by downloading the latest blockchain after rejoining the system. Thus, ACs also maintain the blockchain logs.

3) Mining and Transaction Types:: The blockchain entities in V-CARE reach the consensus by performing the mining procedure. Proof-of-Work (PoW) can be considered as the consensus mechanism in V-CARE as the network is supposed to be a public network. PoW outperforms other consensus mechanisms in terms of scalability in the number of nodes for public blockchains. Each miner participates in the mining procedure by packaging the incoming transactions in a block and solving a cryptographically hard problem that includes finding a nonce value satisfying some pre-conditions.

In V-CARE we propose to have two types of transactions:

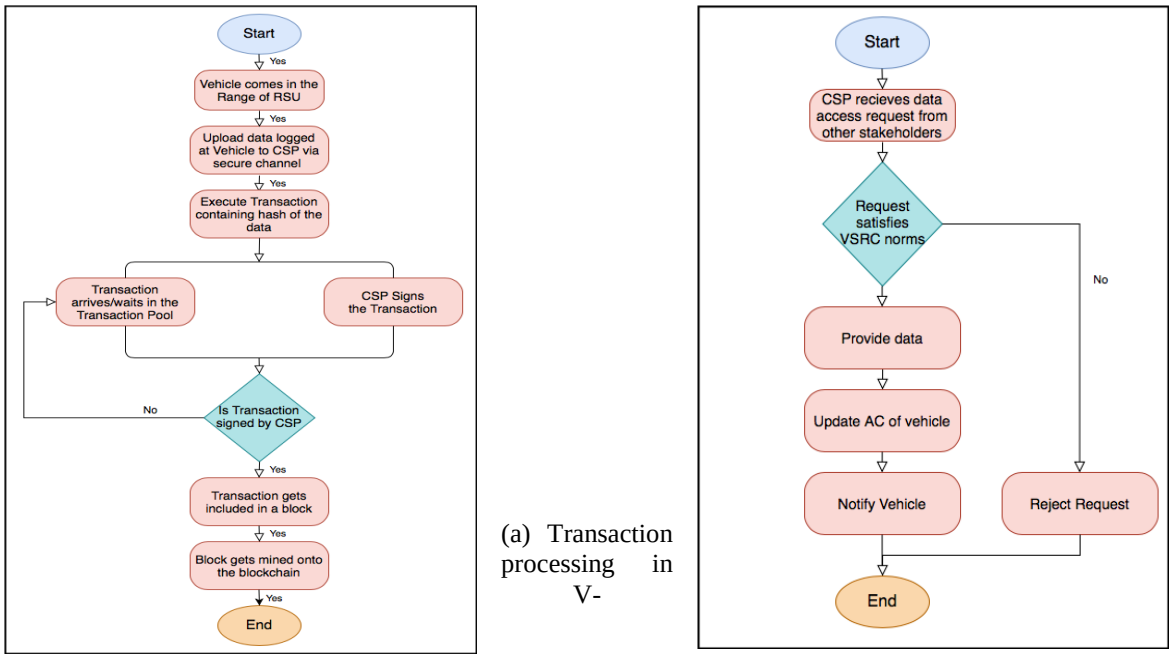
- *Single Signed Transactions:* These transactions are the general type of blockchain transactions where a transaction needs to be signed by the initiator of the transaction. In V-CARE access requests made by a stakeholder such as an insurance company to a CSP of vehicle is a single signed transaction.

• *Multi-signature Transactions:* These are the transactions that are required to be signed by multiple identities where the number of identities must be at least more than one. Multi-signature transactions are much beneficial when consent from multiple parties is required. In V-CARE transactions resulting against data upload from the vehicle to the CSP is a multi-signature transaction which requires signatures from both the vehicle as well as the CSP to be valid.

C. Working Principles

1) Phase I: Registration: All the vehicles (V1...Vn) first register themselves to the RC via the TA in order to join the blockchain-based VHR network. All service providers also need to register themselves in RC. Upon successful registration the entity is provided with an address and a private key corresponding to the address. The entity is uniquely identified on the blockchain network with the assigned address identifier.

2) Phase II: Data Logging, and Record at Vehicle: The raw data generated from various ECUs, and OBD-II of the vehicle are logged (lossless logging) locally in the SDcard of onboard storage of the vehicle.



(a) Transaction processing in V-CARE

(b) Access management in V-CARE

Fig. 4: Transaction Management and Access Management in V-CARE.

3) Phase III: Data Transfer to Fog node via RSUs: The data recorded and stored on the vehicles are uploaded to the fog nodes via the RSU when the vehicles are in the RSU range. Once the backup is taken at the edge nodes, that data from vehicle storage can be purged to utilize the storage for local recording. The deeper analysis of the data is done at the cloud level by the various service providers and stakeholders of the system.

4) Phase IV: System Initiation: The V-CARE is initialized by the TA with the deployment of infrastructures such as the RSU (Edge nodes) and the fog nodes. The TA sets up the blockchain network and does the deployment of smart contracts onto the chain.

5) Phase V: Consensus and Processing: Once a vehicle comes under the range of an RSU, it initiates its data upload mechanism to the cloud via the Fog Nodes. The data upload is made through a secure channel. For each block of data being uploaded, the vehicle also initiates a multi-signature blockchain transaction corresponding to the data upload containing details such as a hash of the data block, timestamp, address of the intended cloud service provider.

Each cloud service provider which also acts as a miner node responsible for maintaining the blockchain. Upon receiving a transaction, they check the credibility of the transaction first; then, they check whether any data block is present in their system with the corresponding transaction data hash. If yes, the CSP also signs the transaction. Once, both the signatures are acquired the miners bundle the transaction into a block and compete among themselves in order to get the block onto the blockchain. The transaction processing and access management flow chart is shown in Fig. 4 (a) and Fig. 4 (b), respectively.

In V-CARE, the fog nodes deployed by the TA and the CSPs primarily act as the miner nodes, however other stakeholders of the ecosystem can also join the mining procedure by deploying their own mining equipment to make the blockchain much more decentralized.

6) Phase VI: Access Control: Once, a CSP receives a data access request from another stakeholder for a vehicle whose data management is associated with the CSP, the CSP checks for the satisfaction of conditions laid down by the VSRC of the vehicle. If the request satisfies the VSRC norms, access to the data is provided to the requester, and the vehicle's AC is also updated, marking a successful data access attempt.

7) Phase VII: Service Delivery: Service providers perform different analyses on the data that they receive from the CSP, such as the manufacturer of the vehicle analyzing the OBD-II and ECUs specific data. In contrast, the insurance company might be more interested in analyzing the driving behavior data. Based on the analysis, the critical information will be forwarded immediately to drivers as alerts, and warnings. The other important information can be offloaded to the regional fog, which will be pushed to the visiting edge nodes for better service delivery.

III. Discussion

We proposed a blockchain-based VHR system called V-CARE that leverages a flourished multi-tier [13], [14] IoV framework (Cloud, Fog, and Edge nodes) for better service delivery to vehicles. Our main concern was how to utilize the power of blockchain to design a secure VHR that fulfill the security requirements such as integrity, authenticity, non-repudiation, availability, access control, etc. Our focus was on how the scope of VHR can be broadened to facilitate a wide variety of services in IoV. With the use of contracts, various activities by all the entities can be logged and recorded in a consistent manner in the blockchain. The data, once recorded, can't be altered by any parties. Vehicles are highly dynamic and frequently leave and join the network. Once they rejoin the system, the proposed architecture can help them upload data, access results, and other activities in a secure and fast manner. The proposed framework also facilitates backup, restore, and warning systems through activity contracts.

IV. Conclusion and Future Work

In this paper, we presented a concept of a novel decentralized VHR system that leverages blockchain technology for maintaining vehicle health records, which can enable various types of services in IoV. We discussed how such a decentralized approach could help to handle VHRs securely and provide a wide range of services by accessing them. In the near future, we look forward to implementing the system on available blockchain platforms to demonstrate the feasibility. We will try to integrate quantum resilience multi-factor authentication and attribute-based access control for data access and sharing across different entities. We will provide details of VHR data update policies, such as how data will be added and deleted. Our work can be extended to integrate more services and solve other challenges of IoV.

References

[1] Z. El-Rewini, K. Sadatsharan, D. F. Selvaraj, S. J. Plathottam, and P. Ranganathan, "Cybersecurity challenges in vehicular communications," *Vehicular Communications*, p. 100214, 2019.

[2] P. K. Singh, S. K. Nandi, and S. Nandi, "A tutorial survey on vehicular communication state of the art, and future research directions," *Vehicular Communications*, vol. 18, p. 100164, 2019.

[3] U. Shafi, A. Safi, A. R. Shahid, S. Ziauddin, and M. Q. Saleem, "Vehicle remote health monitoring and prognostic maintenance system," *Journal of Advanced Transportation*, vol. 2018, 2018.

[4] H. Kargupta, R. Bhargava, K. Liu, M. Powers, P. Blair, S. Bushra, J. Dull, K. Sarkar, M. Klein, M. Vasa *et al.*, "Vedas: A mobile and distributed data stream mining system for real-time vehicle monitoring," in *Proceedings of the 2004 SIAM International Conference on Data Mining*. SIAM, 2004, pp. 300–311.

[5] D. I. Tselentis, G. Yannis, and E. I. Vlahogianni, "Innovative insurance schemes: pay as/how you drive," *Transportation Research Procedia*, vol. 14, pp. 362–371, 2016.

[6] T. Toledo, O. Musicant, and T. Lotan, "In-vehicle data recorders for monitoring and feedback on drivers' behavior," *Transportation Research Part C: Emerging Technologies*, vol. 16, no. 3, pp. 320–331, 2008.
[7] P. M. Forsman, B. J. Vila, R. A. Short, C. G. Mott, and H. P. Van Dongen, "Efficient driver drowsiness detection at moderate levels of drowsiness," *Accident Analysis & Prevention*, vol. 50, pp. 341–350, 2013.
[8] P. K. Singh, R. Singh, G. Muchahary, M. Lahon, and S. Nandi, "A blockchain-based approach for usage based insurance and incentive in its," in *IEEE Region 10 Conference (TENCON)*. IEEE, 2019, pp. 1202–1207.
[9] M. Jensen, J. Wagner, and K. Alexander, "Analysis of in-vehicle driver behaviour data for improved safety," *International journal of vehicle safety*, vol. 5, no. 3, pp. 197–212, 2011.
[10] P. K. Singh, R. Singh, S. K. Nandi, K. Z. Ghafoor, and S. Nandi, "Seamless v2i communication in hetnet: State-of-the-art and future research directions," in *Connected Vehicles in the Internet of Things*. Springer, 2020, pp. 37–83.
[11] S. Nakamoto, "Bitcoin: A peer-to-peer electronic cash system," Manubot, Tech. Rep., 2019.
[12] P. K. Singh, R. Singh, S. K. Nandi, and S. Nandi, "Smart contract based decentralized parking management in its," in *International Conference on Innovations for Community Services*. Springer, 2019, pp. 66–77.
[13] D. B. Rawat, "Fusion of software defined networking, edge computing, and blockchain technology for wireless network virtualization," *IEEE Communications Magazine*, vol. 57, no. 10, pp. 50–55, 2019.
[14] D. B. Rawat and A. Alshaikhi, "Leveraging distributed blockchain-based scheme for wireless network virtualization with security and qos constraints," in *2018 International Conference on Computing, Networking and Communications (ICNC)*. IEEE, 2018, pp. 332–336.

Pranav Kumar Singh is working as an Assistant Professor in the Department of Computer Science and Engineering, Central Institute of Technology Kokrajhar, India. He is having more than 12 years of Teaching Experience. He has also served as Nodal officer NKN and IPv6 Road Map of CITK, an initiative by the Government of India. He received the B.Tech and M.Tech Degree in Computer Science and Engineering. He is pursuing his Ph.D. in the Department of Computer Science and Engineering, Indian Institute of Technology Guwahati, India. His research interests include Vehicular Communications, Security and Privacy, Software-Defined Vehicular Networking, QoS and QoE in Wireless Communication, Intelligent Transportation System, Blockchain, and IoT.

Roshan Singh received his Diploma in Computer Engineering from Central Institute of Technology, Kokrajhar, India in 2016, and a B. Tech degree in Computer Science and Engineering in the year 2019. He is an Assistant Project Engineer in the Open Source Intelligence Lab at the Indian Institute of Technology, Guwahati, India. His research interests are in Blockchain Technology, IoT, and Social Network Analytics.

Sukumar Nandi is a senior professor with the Department of Computer Science & Engineering, Indian Institute of Technology Guwahati, India. He was a visiting senior fellow at NTU, Singapore, during 2002-2003. He is co-author of a book entitled Theory and Application of Cellular Automata (IEEE Computer Society) and four book chapters on sensor/vehicular networks. He has published around 400 journals/conference papers. His research interests include traffic engineering, wireless networks, network security, distributed computing, VLSI Design, and Data Mining. Dr. Nandi is a Senior Member of IEEE, a Senior Member of Association for Computing Machinery, a Fellow of The Institution of Engineers (India), and a Fellow of The Institution of Electronics and Telecommunication Engineers (India), a Fellow of Indian National Academy of Engineering (INAE).

Towards Cyber Defense Remediation based on Adversarial Characterization in Energy Delivery System

Sharif Ullah∗, Kamrul Hasan∗, Sachin Shetty∗†
∗Old Dominion University, Norfolk, VA, USA
†Virginia Modeling, Analysis, and Simulation Center, Suffolk, VA, USA

I. INTRODUCTION

Industrial Control System (ICS) such as Energy Delivery System (EDS) has been targeted by sophisticated attacks Black- Energy [1], Shamoon attack on oil & gas system [2], and Triton attack on safety instrumented system [3]. Even though critical targets are often segregated and deployed far from the perimeter complying with IEC 62443 reference architecture [4], recent campaigns expose diverse strategies a threat could undertake in this environment. These sophisticated attacks have shown a multi-step multi-domain attack life cycle, organized and focused on specific targets to reach their objectives. Moreover, a low and slow process usually taken by the adversary. As such, individual attack footprint seems insignificant in an isolated manner since it is generally part of a broader campaign.

One of the benefits of a layered architecture is that these well-rehearsed and coordinated single step attacks need to propagate a long span of attack surface to fulfill their goal. A larger attack surface indicates a higher cyber threat landscape and an increased risk of compromise. On the other hand, defenders have more opportunity to learn adversarial propagation, thus have more time to inflict further penetration. Prior work only considers attack surface analytics by acquiring different hosts' information, exploitable vulnerabilities, and how they affect the probability of attack success. Toady's network architecture is more heterogeneous based on the implementation and integration of devices with diverse operating systems, vendors, firmware, and service operations. In this work, we investigate the attack surface as a static and dynamic indicator of adversary propagation and shows how the cumulative analytics could help security controller to design their remediation plan. We argued that an attack surface shouldn't just demonstrate the systems resource, which can be potentially used to launch an attack but also exhibit the attack life cycle in the system. We investigate multi-stage attack propagation within three different aspects, such as *opportunity*, *capability*, and *intent* to characterize an attack successfully. We focus on the adversary strategy that involves lateral spread throughout the EDS infrastructure that culminates in launching an integrity or availability attack on the physical component. This goal of this analysis is to characterize adversary phases in the attack surface, which will be leveraged then to devise a remediation scheme for a particular EDS system. Our project proposed an optimal resource allocation given the criticality of the adversary phase at the operational level to optimize the EDS network risk.

II. SYSTEM MODEL

Figure 1 presents our system model showing the pipeline of our methodology from getting network information to adversarial characterization, eventually leading to our cyber defense scheme. The attack graph (AG) uses to examine the attack surface efficiently for a while from quantifying the vulnerability impact to optimize the prioritize defense in security modeling and analysis [5]–[7]. Our analysis starts with getting ICS testbed network information as a part of EDS by scanning the cyber topology along with firewall rules to generate the network connecting accessibility among different hosts automatically. This information is then utilized to create AG to show how a network and system configurations result in unauthorized actions to specific targets.

While AG shows all potential attack propagation in a given system, without understanding the patterns, it is not possible to impose a response decision. Moreover, for the real network, the graph gets exponential in size, making the analytics computationally intractable. To resolve this issue, the next phase of the model involves inferring the causal relationship between stepping stones. A stepping stone in an AG represents a threat action or respective consequences which doesn't make any values while analyzed separately but could unfold a behavior within a chain of stepping stones. The modus operandi of every threat can be traced back to the stepping stones along the attack path. We extract the logical dependencies between these stepping stones that provide adversaries the opportunity to propagate laterally. We also track the attacker's capability and intent to estimate the complexity of penetration and probability of actions, respectively. We incorporate different information from multiple threat intelligence sources to enrich each context in the attack surface. The extracted attack behavior is augmented to AG to understand different

phases of the attack life cycle. Then it is carefully examined within our response plan to see which step is more critical as well as recurrent periods; thus, blocking it might shrink the attack surface to a considerable extent. The response/remediation algorithm also considers the different legs of cost (money, equipment, and time) to get optimized remedial measures at the operational level and policies at the business level.

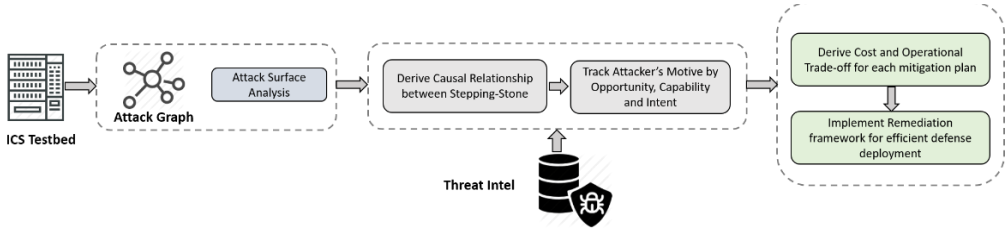


Fig. 1: System model depicting the pipeline of our methodology

III. ADVERSARIAL CHARACTERIZATION

Our adversary behavior analysis is modeled to enable response mechanisms proactively and reactively. The indicator of compromise (IoC) plays a vital role in inferring the behavior in each stage of the attack graph. We initiated the efficient use of threat intelligence by connecting it to the resources from the attack surface. The IoC is divided into two categories: technical indicator and strategic indicator. We employed both types of IoC in our analysis. We intend to capture and analyze the dynamic behavior of the attacker throughout the propagation path. First, we model the attacker's opportunity by investigating the influence of each node in successful penetration in AG [8]. To measure such influence, we have taken account of technical indicators embedded in the attack graph. The AG includes several system artifacts such as system/network configuration, running services, open ports, associated vulnerabilities, and security control, etc. These technical indicators were correlated by adjacent stepping stones to estimate the corresponding effort the attacker encounters through their penetration. We denote this correlation with similarity index $S_{index(p_k, x)}$ for technical indicator x for attack path p_k, which is part of the path set $P=\{p_1, p_2, \ldots\ldots, p_k\}$. The opportunity of node j is formulated as an exploitation score [9]-

$$ES_j = D^t \sum_{t \epsilon T} \sum_{p_k \epsilon P} \left(\frac{1}{\varepsilon^t_{p_k j}} \times \frac{c^t_{p_k j}}{C^t_{p_k}} \times \prod_x \frac{1}{1 - S_{index(p_k, x)}}\right) \quad (1)$$

Here $c^t_{p_k j}$ and $C^t_{p_k}$ denoted the cost of the node j and target t (e.g., PLC, RTU, etc.), respectively. The damage potential D^t indicates the highest direct operational capacity of target node t. Some of the nodes in the network are interconnected by functional dependency between them possessed a significant risk in the system. The persistent attackers can take advantage of this scenario and initiate a stealthy malicious link, which could trigger a cascading impact if exploited. We model the functional dependency between assets through object interaction, where we take three types of objects such as process, files, sockets, and specific system calls responsible for information flow dependency. The model has been built by leveraging Bayesian Network (BN) to specify the interaction between objects. The functional dependency is dynamic because of time-variable socket communication and cascading dependency between the target with various hosts in the network.

The opportunity analytics gives a proactive estimate of the potential path criticality in the system. But the attacker's motivation cannot be generalized as some attackers prefer the shortest path to reach the target. Some might go for stealthy penetration that might take weeks or months. The uncertainty of attacker behavior obstructs the response decision-making process. We model the attacker's intent by analyzing the security state of the network devised from intrusion alert in the system. The local alert information corresponds to a compromised node that helps the defender to understand the underlying strategy of the attacker. We intend to capture two apparent behavior of the attacker: diverse capability and aggressiveness. The different capacity is estimated by the uniqueness of technical indicator in the compromised path. The aggressiveness is determined by the temporal information associated with the alert. We make a hypothesis that aggressive attackers take less time slot per penetration in their path. Each estimation comes up with different weights, which is plugged into the opportunity analytics shown above to filter the options the attacker under investigation likely to follow.

So far, our analysis is confined with low-level technical indicators, which is static for a particular network, doesn't present attackers skills, which is only captured by performed action in the compromised path. We incorporate MITRE ATT&CK [10] framework, a rich knowledge base from a real cyber-attack campaign to capture the latent behavior of threat in the system. A tactic refers to attackers' motive behind an action, where technique defines the particular operation and procedure provides fine-grained granular information corresponds to an action. We integrated each state of the attack surface to the distinct, high-level category defined by the ATT&CK model [11]. Thus, each attack path could be representative of a sequence of cyber kill chain phases.

We proposed multiple analytics to reveal meaningful insight into the attack phase in terms of the local and global threat landscape. We devise a unique vulnerability score by fusing the default Common Vulnerability Scoring System (CVSS) and attempted vulnerabilities from real-world exploitation. To do so, we distinguish the state of an exploit into three different categories [11]. *Unproven* refers to the unavailability of potential full-fledged exploit code for the vulnerability. *Proof-of-concept* exploitation happens to be part of penetration testing, and vulnerability disclosure process can be acquired from the exploit database. *Exploit in the wild* refers to the vulnerability extensively practiced in real threat campaigns, can get from security reports, and various attack signature databases. We also formulated a score for each technique in the MITRE ATT&CK database. Two factors have been considered to determine the score: adaptability and exploitation. A technique's resilience depends on the environment and conditions which allow it to be exercised. Exploitation depends on the technique manifestation in the real world. Incorporating these parameters, we define the hardness of path to show the attacker's capability as follows [11]-

$$H_{p^k_{j,j'}} = \sum_{i \epsilon AS_{p^k_{j,j'}}} \left(\alpha_i^{-1} + TSc(ta_t)^{-1}\right) e^{-\sum_{q=AS_{p^k_{j,j'}}}^{i} (0) \frac{CC_{iq}}{\gamma}} \quad (2)$$

Here we denote $AS_{p^k_{j,j'}} = \{as_1, as_2, \ldots\ldots, as_n\}$ as the set comprised of n states for the path p^k from node j to node j'. The correlation between state i and q are denoted with correlation coefficient (CC_{iq}), while for similar states, a decay factor γ is introduced representing the effort reduction in similar actions. $\left(\alpha_i^{-1} + TSc(ta_t)^{-1}\right)$ is defined as the criticality of the state where $TSc(ta_t)$ is the technique score assuming state i is mapped with technique t and α_i is the vulnerability score of this state. The technique score reflects the defender's priority parameter alternatively means less hard for the attacker.

IV. CYBER DEFENSE REMEDIATION

Suppose we have a resource budget, B_D, and the cost to eliminate all vulnerabilities and exploits from node i is $maxA_i$, where A_i is the actual cost invested. In which the goal is to reduce the number of pre-conditions, vulnerabilities and exploits, denoted as V_i, to zero. So, the number of remaining vulnerabilities is a function of budget allocation A_i that represents actions performed on a node to remove and remediate such vulnerabilities, for every node in AG. The target function is to allocate correct A_i to each node such that the overall risk is minimized. Namely:

$$\min \{R\} = \sum_{i=1}^{n} V_i(A_i)C_i \qquad (3)$$
$$\text{Subject to,} \quad \sum_{i=1}^{N} A_i \le B_D;\ \sum_{i=1}^{N} \max A_i > B_D;\ A_i \ge 0$$

There are two types of cost models, namely: linear cost model and exponential cost model. The linear cost model is unrealistic because it assumes that the vulnerability will be zero with the increased budget allocation. But in reality, the vulnerability attached to a node cannot be zero since the vulnerability landscape evolves and continuously generates new threats. In other words, vulnerability reduction may suffer from diminishing returns. For this reason, researchers prefer the exponential cost model [12]. The exponential cost model is precisely the same as the linear cost model except for the relationship between budget allocation and vulnerability reduction. Moreover, the allocation strategy is the same; the higher-ranked node receives more resources than lower-ranked nodes.

The exponential cost model differs from the linear model in two important ways: (1) the actual resource allocations A_i are different, and (2) network risk is typically higher because an infinite investment is required to eliminate the vulnerability. A simple exponential function for vulnerability reduction is [12]:

$$(A_i) = e^{-\sigma_i A_i};\ 0 \le A_i \le 1; \text{ where, } \sigma_i = \frac{1}{maxA_i} \qquad (4)$$

This function asymptotically declines to zero when an infinite budget allocation is assigned to this node. Unlike the linear strategy, the exponential cost allocation never completely removes the vulnerability. Allocation of budget B_D to nodes is optimized when objective function R is minimized, with budgetary constraints. The optimized function is [13] [14]:

$$R(A_i) = \sum_{i=1}^{N} e^{-\sigma_i A_i} C_i - \lambda[\sum_{i=1}^{N} A_i - B_D] \qquad (5)$$
$$where,\ A_i = \frac{\ln(\sigma_i C_i) - \ln(\lambda)}{\sigma_i} \quad \text{and } \ln(\lambda) = \frac{\sum_{i=1}^{N} \frac{\ln(\sigma_i C_i)}{\sigma_i} - B_D}{\sum_{i=1}^{N} \frac{1}{\sigma_i}}$$

In this work, we kept maximum budget allocations for every node was as same as the maximum allocation for the most critical the node, which was ($maxA_{i1}$).

The risk reduction by the exponential cost model is slightly lower than the linear cost model because the exponential model never reduces vulnerability to zero. However, for both linear and exponential cost models the optimal allocation is ensured when the budget is distributed according to the rank of nodes. Figure. 2 shows budget allocation amongst nodes for linear cost and exponential cost allocation. In both cases, the limited budget (15 units) is allocated after ranking their criticality from highest to lowest: SCADA1, RTU1, SCADA2, RTU2, WebS, and node WS.

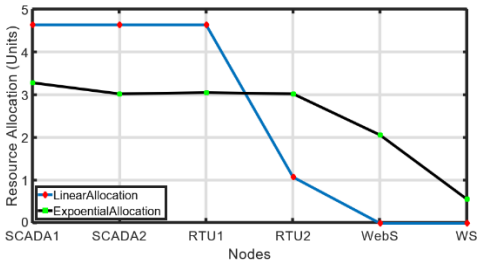


Fig. 2: Linear and exponential resource allocation

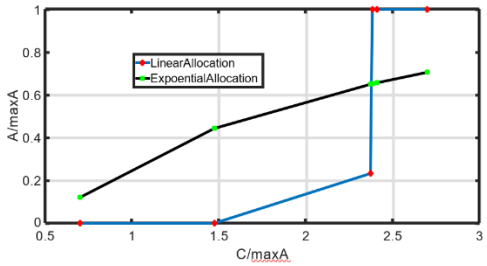


Fig. 3: Linear and exponential cost allocation vs. criticality

Figure. 3 depicts the allocation priority- from highest to lowest. Linear and exponential allocation obey the rank-order established by the product of $\frac{C_i}{maxA_i}$. This property is observed in allocation strategies regardless of whether the relationship between allocation and vulnerability reduction is linear, exponential, or a power law. This establishes a hierarchy among nodes; the most critical nodes of a network are those with the highest $\frac{C}{maxA}$ value.

V. CONCLUSION

In this work, we enumerate the complexity of each state of attack surface based on technical and strategic threat indicator in an EDS. The transition of the state is defined by the attacker's evolving capability, opportunity, and intent by their potential choice of actions and respective consequences. Attack surface augmented with contextual information from threat intelligence allows investigating the possible attack pattern based on a real-world threat campaign. After knowing those characteristics of an attacker by a defender, the prioritized mitigation plan mostly depends on the criticality index of assets. This work also examines the relationship between cost models of budget allocation for the removal of vulnerabilities on critical nodes and its impact on gradual readiness.

REFERENCES

[1] M. J. A. Robert M. Lee and T. Conway. (2018, Aug.) Analysis of the cyber attack on the ukrainian power grid. [Online]. Available: https://ics.sans.org/media/E-ISAC˙SANS˙Ukraine˙DUC˙5.pdf

[2] C. Bronk and E. Tikk-Ringas, "The cyber attack on saudi aramco," *Survival*, vol. 55, no. 2, pp. 81–96, apr 2013.

[3] A. Carcano. (2018, Aug.) Understanding triton, the first sis cyber-attack. [Online]. Available: http://www.nozominetworks.com/blog/black-hat-understanding-triton-the-first-sis-cyber-attack

[4] K. Stouffer, V. Pillitteri, S. Lightman, M. Abrams, and A. Hahn. (2015, May) Guide to industrial control systems (ics) security. NIST Special Publication 800-82. [Online]. Available: http://dx.doi.org/10.6028/NIST.SP.800-82r2

[5] V. Shandilya, C. B. Simmons, and S. Shiva, "Use of attack graphs in security systems," *Journal of Computer Networks and Communications*, vol. 2014, 2014.

[6] N. Idika and B. Bhargava, "Extending attack graph-based security metrics and aggregating their application," *IEEE Transactions on Dependable and Secure Computing*, vol. 9, pp. 75–85, Jan. 2012.

[7] J. Homer, S. Zhang, X. Ou, D. Schmidt, Y. Du, S. R. Rajagopalan, and A. Singhal, "Aggregating vulnerability metrics in enterprise networks using attack graphs," *Journal of Computer Security*, vol. 21, no. 4, pp. 561–597, 2013.

[8] S. Ullah, S. Shetty, and A. Hassanzadeh, "Towards modeling attacker's opportunity for improving cyber resilience in energy delivery systems," in *2018 Resilience Week (RWS)*. IEEE, Aug. 2018.

[9] S. Ullah, S. Shelly, A. Hassanzadeh, A. Nayak, and K. Hasan, "On the effectiveness of intrusion response systems against persistent threats," in *2020 International Conference on Computing, Networking and Communications (ICNC)*. IEEE, 2020, pp. 415–421.

[10] "Mitre adversarial tactics, techniues, and common knowledge," Aug. 2018. [Online]. Available: https://attack.mitre.org/techniques/enterprise

[11] S. Ullah, S. Shetty, A. Nayak, A. Hassanzadeh, and K. Hasan, "Cyber threat analysis based on characterizing adversarial behavior for energy delivery system," in *International Conference on Security and Privacy in Communication Systems*. Springer, 2019, pp. 146–160.

[12] K. Hasan, S. Shetty, S. Ullah, A. Hassanzadeh, and E. Hadar, "Towards optimal cyber defense remediation in energy delivery systems," in *2019 IEEE Global Communications Conference (GLOBECOM)*. IEEE, 2019, pp. 1–7.

[13] K. Hasan, S. Shetty, A. Hassanzadeh, and S. Ullah, "Towards optimal cyber defense remediation in cyber physical systems by balancing operational resilience and strategic risk," in *MILCOM 2019-2019 IEEE Military Communications Conference*. IEEE, 2019, pp. 1–8.

[14] K. Hasan, S. Shetty, A. Hassanzadeh, M. B. Salem, and J. Chen, "Modeling cost of countermeasures in software defined networking-enabled energy delivery systems," in *2018 IEEE Conference on Communications and Network Security (CNS)*. IEEE, 2018, pp. 1–9.

Sharif Ullah is a Ph.D. candidate in Electrical and Computer Engineering department at Old Dominion University (ODU), Norfolk, Virginia. He received the BSc. and MSc. degrees in Applied Physics, Electronics and Communication Engineering from University of Dhaka, Bangladesh. His current research is focusing on cybersecurity risk and resiliency analytics for critical infrastructure (CI). His research interest includes cyber-physical system (CPS) security, adversarial behavior analytics, malware analysis and anomaly detection, and industrial internet of things (IIoT).

Kamrul Hasan awarded a B.S. degree in Electrical and Electronics Engineering from Bangladesh University of Engineering and Technology (BUET), Dhaka, Bangladesh. He also graduated as M.S. in Computer Information and Systems Engineering from Tennessee State University, Nashville, Tennessee. Currently, he is pursuing his Ph.D. in Computational Modeling and Simulation Engineering at Old Dominion University, Norfolk, Virginia. His research interests lie in ICS/CPS Security, SDN-enabled Cyber resilience, AI/ML-enabled cyber threat modeling and remediation, and wireless network security.

Sachin Shetty received the Ph.D. degree in modeling and simulation from Old Dominion University in 2007. He was an Associate Professor with the Electrical and Computer Engineering Department, Tennessee State University, USA. He is currently an Associate Professor with the Virginia Modeling, Analysis and Simulation Center, Old Dominion University. He holds a joint appointment with the Department of Modeling, Simulation and Visualization Engineering and the Center for Cybersecurity Education and Research. He has authored and co-authored over 125 research articles in journals and conference proceedings and two books. His research interests lie at the intersection of computer networking, network security, and machine learning. He was a recipient of the DHS Scientific Leadership Award. He has served on the Technical Program Committee of ACM CCS, IEEE INFOCOM, IEEE ICDCN, and IEEE ICCCN.

IEEE COMSOC MMTC Communications - Frontiers

Adaptive Control Plane Load Balancing in vSDN Enabled 5G Network

Deborsi Basu*, Uttam Ghosh† and Raja Datta‡

**G.S. Sanyal School of Telecommunication, Indian Institute of Technology, India.*

†Dept. of Electronics and Electrical Comm Engineering, Indian Institute of Technology, India.

‡Dept. of Electrical Engineering and Computer Science, Vanderbilt University, Nashville, TN, USA.

deborsi.basu@iitkgp.ac.in, ghosh.uttam@ieee.org, rajadatta@ece.iitkgp.ac.in

I. INTRODUCTION

Standardization of the future 5G networks are still under construction and researchers are intensively working into this field [1], [2]. However, the evolution of the cellular technology is ever expanding and will flow beyond 5G as well, soon after the standardization has been made successfully. The speculations based on 6G networks are already in the market and people have already started thinking beyond 5G network architectures and technological developments. The fundamental aim of all such developments always remains the same, which is to satisfy the end user demands in all possible way. Everyday network servers are being loaded with hundreds of new applications and services & maximum of them are redundant in nature, creating unnecessary load overhead on the network. Keeping demand threshold restriction in mind the TSPs (Telecomm. Service Providers) are giving intensive care to server load distribution for handling heavy network functions without any service disruption. The integration of SDN & NFV give the tenants an upgraded open platform to manage these complex issues by providing a virtualized network service plane with dynamic and programmable network slicing architectures. The openness of networks brings major network scalability problems like CPP & HPP (Controller Placement Problem & Hypervisor Placement Problem). Network Hypervisors are virtual entities to be placed in between Control Plane and Data Plane to allow multiple tenants to use the network resources and update systems simultaneously [3–5]. Due to centralized architecture SDN faces huge traffic load at the control plane which degrades network performances [6], [7]. Through our work we have proposed an intelligent solution of Control Plane load balancing of Joint CPP-HPP using vSDN concept, that transforms non-virtualized networks to virtualized networks. We have used real network topology to validate our approach by defining four latency objectives and finding out the potential Controller-Hypervisor (C-H) positions that generates minimal load on C-H planes. This approach can also be applied in solving similar other critical localization problems like service chain mapping in 5G-NR, baseband unit deployment in 5G C-RAN etc.

II. RELATED WORKS & MOTIVATION

The CPP was first framed by Heller *et al.* in [8] where they have tried to find out the number and potential positions of the controller inside a given 100 possible WAN (Wide Area Network) topology. The introduction of Hypervisor plane or H-plane has been done inside the CPP by Blenk *et al.* in [9]. They formulated a Hypervisor Placement Problem (HPP) in a vSDN network while fixing the controller positions at each vSDN. Furthermore, Killi *et al.* in [10] have shown that reduction of worst-case latency can be done by fixing the hypervisor location at H-plane and optimizing the controller location at C-plane. Furthermore, it is shown that the Joint HPP-CPP models at physical networks and virtual networks respectively are even more efficient in latency reduction. The flow-paths which are terminated at H-plane via C-plane makes unnecessary load at H-plane. They are responsible for higher network processing delay. If the path-flow can be reverted back to C-plane only then the load at H-plane can be reduced significantly. The flow signals which reach the C-plane first through the shortest paths are being processed at C-plane itself. This conceptualization motivates us to contribute further in this Joint HPP-CPP load balancing model & our major contributions have been explained next.

Contributions: In this work we have initiated the process of adaptive load balancing by solving Joint HPP-CPP in the context of future 5G networks. More precisely the contributions have been explained below:

- We have started the Joint C-plane and H-place controller and hypervisor placement using a real network topology & the flexibility to select both their positioning in the planes. We have defined an MILP based analytical modeling on graphical mapping to solve the problems based on four latency objectives.
- After getting the proper positions of the physical entities at both the C and H planes based on the latency objectives, we have found out the optimum propagation paths from the user end to the controller using a bottom up approach. Our proposed RPF (Reverse Path-Flow) algorithm suitably found out the optimal paths from the Data Plane physical nodes to the controller through which the PACKET-IN messages flow. It can be seen that all the paths reaching to the C-plane are not necessarily routed through the H-plane. We restrict the unnecessary in flow of the

messages at the H-plane.

- Finally, we discarded the extra paths to reduce the load at the H-plane and C-plane overheads as well. As H-plane has been used by multiple tenants to bring their network services, it is extremely necessary to keep the load at the H-plane as low as possible to give high processing efficiency to the service messages. The C-H plane load & propagation delay reduction of Service Requests are the key enablers to experience ULL network services to which the future 5G & 6G networks are aiming [11].

III. SYSTEM MODEL & PROBLEM FORMULATION

A. System Model

We have considered a real network topology instance of AT&T North America and apply an analytical graphical modeling to make the Load and Latency aware Joint HPP-CPP formulation. We have compared our simulation results with the existing CPP-HPP models [9], [10] to show the efficiency of our proposed approach. For simplicity we have considered two terminologies where Joint CPP-HPP is represented by **JHCPP** and Load and Latency aware model has been represented by **opJHCPP** (Open JHCPP- Open Joint Hypervisor-Controller Placement Problem) and the same terms have been maintained throughout the paper.

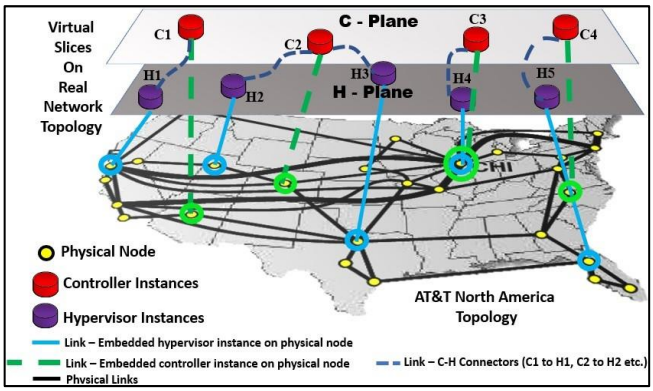


Fig. 1: The controller and hypervisor positions based on latency matrix optimization - A Generalized Case [13]

The network has been considered as a graph denoted by $\mathcal{G} = V_p \rightarrow physical\ node \cup E_{link} \rightarrow bi-directional\ links$. Physical Nodes $p_{node} \in V$ can consist zero, one or multiple virtual hypervisor or controller instances ($h_{node} \in H_{node}$ & $c_{node} \in C_{node} \subseteq V_p$). H_{node} & C_{node} are the potential positions of the hypervisors and controller nodes respectively. The maximum number of hypervisor and controller instances for a single virtual network is H_{inst} and C_{inst} respectively. The cost of the min. distance path from a physical vSDN node to the controller through hypervisor for a particular service demand towards the controller is given by $\psi_{v_n,\ d,\ h_{node},\ c_{node}}$. The path with source, intermediate and destination at same node costs zero.

B. Problem Formulation

Now the following **opJHCPP** Latency matrices are explained below which are evaluated and compared with other existing cases mentioned in [9], [10] to show the effectiveness of our proposed approach.

1) Worst Case Latency: This is used to minimize the longest path delay among all vSDNs.

$$min\,(\mathbb{W}) \qquad (1)$$

Given the following: The worst-case latency or Maximum latency case can be incorporated in our model by adding a continuous variable constraint in the equation (2) given by $\mathbb{W}$.

$$L_{worst} = \left(\max_{v_n \in V_{net}, d \in D_{v_n}}\right)\left(\sum_{h_{node} \in H_{node},\ c_{node} \in C_{node}}\left(Y_{v_n,\ d,\ h_{node},\ c_{node}} \times \psi_{v_n,\ d,\ h_{node},\ c_{node}}\right)\right) \qquad (2)$$

Where,

$$\sum_{h_{node} \in H_{node},\ c_{node} \in C_{node}}\left(Y_{v_n,\ d,\ h_{node},\ c_{node}} \times \psi_{v_n,\ d,\ h_{node},\ c_{node}}\right) \leq \mathbb{W}\ \forall\ v_n \in V_{net}, \forall\ d \in D_{v_n} \qquad (3)$$

2) Minimum of Average Latency: The minimum overall average latency demands among all vSDNs.

$$min\ (L_{avg}) \qquad (4)$$

Given the following:

$$\frac{1}{\sum_{v_n \in V_{net}} |D_{v_n}|} \sum_{v_n \in V_{net}} \sum_{d \in D_{v_n}} \sum_{h_{node} \in H_{node},\ c_{node} \in C_{node}} \left(Y_{v_n,\ d,\ h_{node},\ c_{node}} \times \psi_{v_n,\ d,\ h_{node},\ c_{node}}\right) \quad (5)$$

3) Avg-Maximum Latency: It selects all the worst-case latencies from each vSDN and then try to minimize the average value of the respective latencies.

$$min\left(\frac{1}{|V_{net}|} \sum_{v_n \in V_{net}} \mathbb{W}_{v_n}\right) \quad (6)$$

Given the following: Here the continuous variable $\mathbb{W}_{v_n}$ represents the worst-case latencies of individual virtual networks v_n given by equation (2).

$$L_{avg-max} = \frac{1}{|V_{net}|} \left(\max_{d \in D_{v_n}}\right) \sum_{h_{node} \in H_{node},\ c_{node} \in C_{node}} \left(Y_{v_n,\ d,\ h_{node},\ c_{node}} \times \psi_{v_n,\ d,\ h_{node},\ c_{node}}\right) \quad (7)$$

Where,

$$\sum_{h_{node} \in H_{node},\ c_{node} \in C_{node}} \left(Y_{v_n,\ d,\ h_{node},\ c_{node}} \times \psi_{v_n,\ d,\ h_{node},\ c_{node}}\right) \leq \mathbb{W}\ \forall\ v_n \in V_{net}, \forall\ d \in D_{v_n} \quad (8)$$

4) Max-Average Latency: It takes all the average values from each vSDN and then aim to find the minimum among all maximums.

$$min\,(\mathbb{W}) \quad (9)$$

Given the following: Similarly, here also $\mathbb{W}$ is a continuous variable for max-avg latency of individual vSDNs.

$$L_{max-avg} = \left(\max_{v_n \in V_{net}}\right) \frac{1}{|D_{v_n}|} \sum_{d \in D_{v_n}} \sum_{h_{node} \in H_{node},\ c_{node} \in C_{node}} \left(Y_{v_n,\ d,\ h_{node},\ c_{node}} \times \psi_{v_n,\ d,\ h_{node},\ c_{node}}\right) \quad (10)$$

Where,

$$\frac{1}{|D_{v_n}|} \sum_{d \in D_{v_n}} \sum_{h_{node} \in H_{node},\ c_{node} \in C_{node}} \left(Y_{v_n,\ d,\ h_{node},\ c_{node}} \times \psi_{v_n,\ d,\ h_{node},\ c_{node}}\right) \leq \mathbb{W}\ \forall\ v_n \in V_{net} \quad (11)$$

IV. SOLUTION & RESULT ANALYSIS

A. Algorithmic Solution

We have used a Greedy Algorithmic approach to solve the above opJHCPP problem using the Reverse path-flow concept.

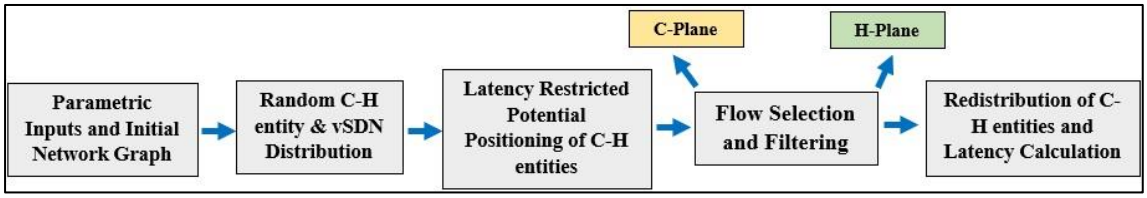
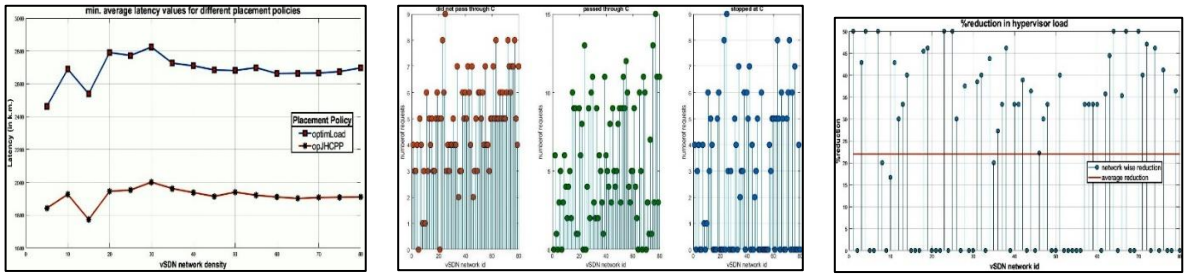


Fig. 2: The Sequence Flow Diagram of Algorithmic Solution

B. Result Evaluation



(a) min. avg. latency comparison (b) test case signals-block and pass (c) test case H-plane load reduction

Fig. 3: Comparative load reduction using opJHCPP with latency trade-off

For calculating the percentage reduction in hypervisor load it is necessary to compute the distribution pattern of requests based on whether they were blocked by the controller, passed through the controller or did not pass through the controller in an attempt to reach the network hypervisor. For a particular c_{node}-h_{node} pair let's denote the number of requests which did not pass through the controller in order to reach the hypervisor by *dptc*, number of requests which were forwarded from the controller to the hypervisor by *cp* and the number of requests which were blocked at the controller by *cs*. Then the reduction $r_{c_{node},\, h_{node}}$ is given by:

$$r_{c_{node},h_{node}} = \frac{cs}{cs + cp + dptc} \qquad (12)$$

The distributions of requests for different controller and hypervisor combinations for |M| = 80 (no. of vSDN networks) with respect to the vSDN network ids are obtained. (i,j) refers to controller position C(i) and hypervisor position H(j). Here C = 3,7,10,23 and H = 2,5,15,19 are converging potential positions we get after 100 iterations. It can be seen clearly that the controller and hypervisor positions best suited for maximum hypervisor load reduction are not favorable for achieving optimum latency benefits for the latency objectives. Hence, there is a trade-off between minimizing hypervisor load and minimizing network latency. It can be explained from the fact that minimum hypervisor load in case of a single controller and single hypervisor system (as considered in this case) means that most of the requests are blocked by the controller and do not reach the hypervisor which itself means that such controller and hypervisor positions are far apart, so for those requests which do reach the hypervisor, the latencies of propagation are maximum. One important fact to be noted is that, the heavy messages are processed at the Controller itself and restricted for further transmission to H-plane only if their *C-plane processing time ≤ (2 * (C plane to H plane propagation delay) + H-plane processing time)*. The trade-off in latencies can be minimized by placing multiple hypervisors and controllers in the networks which we may consider in our future works.

IV. CONCLUSION & FUTURE WORKS

Our work provides a comprehensive adaptive load balancing approach by properly positioning the controller and hypervisor entities at H-C planes according to their potential locations. Here, we have kept the network service latency under suitable tolerance limit. Apart from our topology (AT&T North America), the proposed approach can be applied to other network topologies as well by changing the parametric values according to the system requirements. We have illustrated the effect of different evaluation setups on the outcome of all four latency metrics. A C++ algorithm-based framework has been implemented using MATLAB R2020a to simulate, & solve the problem, and also analyze the results. In future, we will be targeting some interesting facts like AI (Artificial Intelligence) driven task offloading in between Hypervisor plane and Control plane for optimal resource utilization. We will be focusing towards network slicing based edge computing approach to allocate the additional network functions for optimum QoE for end-users.

REFERENCES

[1] R. A. Addad, D. L. C. Dutra, M. Bagaa, T. Taleb, and H. Flinck, "Fast service migration in 5g trends and scenarios," *IEEE Network*, vol. 34, no. 2, pp. 92–98, 2020.

[2] M. Taheribakhsh, A. Jafari, M. M. Peiro, and N. Kazemifard, "5g implementation: Major issues and challenges," in *2020 25th International Computer Conference, Computer Society of Iran (CSICC)*. IEEE, 2020, pp. 1–5.

[3] A. Blenk, A. Basta, M. Reisslein, and W. Kellerer, "Survey on network virtualization hypervisors for software defined networking," *IEEE Communications Surveys & Tutorials*, vol. 18, no. 1, pp. 655–685, 2015.

[4] H. Huang, B. Niu, S. Tang, S. Li, S. Zhao, K. Han, and Z. Zhu, "Realizing highly-available, scalable, and protocol-independent vsdn slicing with a distributed network hypervisor system," *IEEE Access*, vol. 6, pp. 13 513–13 522, 2018.

[5] G. Yang, B.-Y. Yu, S.-M. Kim, and C. Yoo, "Litevisor: A network hypervisor to support flow aggregation and seamless network reconfiguration for vm migration in virtualized software-defined networks," *IEEE Access*, vol. 6, pp. 65 945–65 959, 2018.

[6] D. Basu, R. Datta, U. Ghosh, and A. S. Rao, "Load and latency aware cost optimal controller placement in 5g network using snfv," in *Proceedings of the 21st International Workshop on Mobile Computing Systems and Applications*, 2020, pp. 106–106.

[7] Basu, D., Jain, A., Datta, R., & Ghosh, U. (2020, April). Optimized Controller Placement for Soft Handover in Virtualized 5G Network. In *2020 IEEE Wireless Communications and Networking Conference Workshops (WCNCW)* (pp. 1-8). IEEE.

[8] B. Heller, R. Sherwood, and N. McKeown, "The controller placement problem," *SIGCOMM Comput. Commun. Rev.*, vol. 42, no. 4, p. 473–478, Sep. 2012. [Online]. Available: https://doi.org/10.1145/2377677.2377767

[9] A. Blenk, A. Basta, J. Zerwas, and W. Kellerer, "Pairing sdn with network virtualization: The network hypervisor placement problem," in *2015 IEEE Conference on Network Function Virtualization and Software Defined Network (NFV-SDN)*, 2015, pp. 198–204.

[10] B. P. R. Killi and S. V. Rao, "On placement of hypervisors and controllers in virtualized software defined network," *IEEE Transactions on Network and Service Management*, vol. 15, no. 2, pp. 840–853, 2018.

[11] U. C. Kozat, A. Xiang, T. Saboorian, and J. Kaippallimalil, "The requirements and architectural advances to support urllc verticals," *5G Verticals: Customizing Applications, Technologies and Deployment Techniques*, pp. 137–167, 2020.
[12] A. Blenk, A. Basta, J. Zerwas, M. Reisslein, and W. Kellerer, "Control plane latency with sdn network hypervisors: The cost of virtualization," *IEEE Transactions on Network and Service Management*, vol. 13, no. 3, pp. 366–380, 2016.
[13] U. o. A. The Internet Topology Zoo, "http://www.topology-zoo.org/dataset.html," 2011.

AUTHORS' BIO

Deborsi Basu is pursuing his Ph.D from G.S Sanyal School of Telecommunication, Indian Institute of Technology, Kharagpur, India with the joint collaboration of Dept. of Electrical Engineering and Computer Science, University of Vanderbilt, Nashville, Tennessee, USA. He has completed his M.Tech from Kalyani Government Engineering College, Kalyani, West Bengal, India in Dept. of ECE in 2018 and B.Tech from Heritage Institute of Technology, Kolkata, West Bengal, India in Dept. of ECE in 2016. He is a Graduate Student Member of IEEE. His current research areas are Software Defined Networking, Network Function Virtualization, Network Slicing in 5G & NextGen Wireless Communication Networks, OpenFlow etc.

Uttam Ghosh joined as an Assistant Professor of the Practice in the Dept. of Electrical Engineering and Computer Science in January 2018 at Vanderbilt University. Dr. Ghosh obtained his PhD in Electronics and Electrical Engineering from Indian Institute of Technology Kharagpur, India in 2013, and has Post-doctoral experience at the University of Illinois in Urbana-Champaign, Fordham University, and Tennessee State University. His main research interests include Cybersecurity, Computer Networks, Wireless Networks, Information Centric Networking and Software-Defined Networking. He has been awarded the 2018-2019 Junior Faculty Teaching Fellow (JFTF) at Vanderbilt University. He is a Senior Member of the IEEE and a member of AAAS, ASEE, ACM, and Sigma Xi.

Raja Datta is the Head of the department at G.S Sanyal School of Telecommunications at Indian Institute of Technology (IIT) Kharagpur. He also is the Professor In-charge of Technology Telecom Center. Prof. Datta is a senior member of IEEE. He has produced a number of PhD and MS students in area of Communication Networks. His research areas include computer communication networks, mobile ad-hoc and sensor networks, optical WDM networks, inter planetary networks, computer architecture, distributed systems etc.

Securing Vehicular Communications in Shared Networks

Abubakar U. Makarfi1, Khaled Rabie1, Rupak Kharel1
1Manchester Metropolitan University, UK
r.kharel@mmu.ac.uk

1. Introduction

Vehicular networks have recently been undergoing huge transformations towards the realisation of the evolving concept of intelligent transportation systems (ITS) [1]. Several existing and emerging technologies are today converging towards the achievement of the ultimate goal of improved safety, reliability and efficiency in transportation. Thus, over the years, existing configurations like vehicular ad-hoc networks (VANETs) are rapidly enhanced with new technologies, such as internet of things (IoT) devices, towards improving communications between vehicle-to-vehicle (V2V) and vehicles to "everything" (V2X).

This sudden growth of connected vehicles comes with practical costs and challenges [2]. Firstly, the information exchange in such large shared networks are increasing exponentially, thus increasing the likelihood of interference from different sources. Secondly, the vehicular density is growing rapidly and the types of connected devices with different connectivity and compatibility standards and requirements are also growing, which brings about an urgent need for securing the networks. Moreover, the security of these networks remains crucial in order to minimise the risk of security attacks and maintain safety of users [3].

Securing vehicular networks can be implemented via different approaches or across several layers of the system. In this study, we adopt a physical layer approach to securing the wireless network. This approach is known as physical layer security (PLS) and involves employing the intrinsic features of the wireless channel, through signal processing and design to realise [4]. The fundamental characteristics of the propagation channel exploited in PLS techniques include noise, fading and interference. The advantages of the PLS approach include less computational complexity compared to computation-based cryptography techniques as well as keyless secure communications, which reduces challenges in distribution and management of secret keys, especially in decentralized systems [5].

As we move into the 5G and beyond realm, novel promising technologies are emerging to provide radio technology designers with even greater control of the wireless channel physical layer, in order to improve signal quality and coverage [6]. One of such technologies are reconfigurable intelligent surfaces (RISs), otherwise known as Large Intelligent Surfaces. RISs are man-made surfaces are composed of arrays of passive elements with specially designed physical structures, where each scattering element can be controlled in a software-defined way to alter the phase shift and other signal characteristics, of the incident signals on the scattering elements [7]. The benefits of RISs to traditional wireless communications are numerous. Specifically, RISs can be regarded as valuable technologies to minimise the challenges of security and interference within shared/connected vehicular networks, due to the flexibility of simultaneously enhancing or suppressing signal beams to different users allows easy implementation of PLS [8],[9].

2. Related Work

The PLS of vehicular communications have been studied within the literature. For instance, PLS was studied for relay-assisted mobile networks were studied in [10]. The secrecy performance for an amplify-and-forward (AF)-based vehicle to infrastructure network was studied in [11], the secrecy performance for a decode-and-forward (DF)-based V2V network in [12], while cooperative AF relaying in V2Vs was investigated in [13]. Additionally, the effects of interference on PLS was demonstrated in [14], [15], and shown to adversely affect the secrecy performance, while, from a vehicular network standpoint, the effect of interference on the PLS, was investigated in [16].

From a RIS perspective, a few studies have investigated non-vehicular RIS-assisted systems in shared wireless networks. For example, the authors in [17] investigated RIS-based cognitive radio networks, the authors in [18] examined RIS-enabled IoT networks in composite fading and shadowing, while the authors in [19] studied the PLS of a RIS-assisted IoT network in Fisher-Snedecor composite fading. Particularly, the authors in [20], provided a first look at the PLS of RIS-assisted vehicular networks, for different configurations of the RIS technology.

3. Contributions

From the aforementioned works, [10] – [13] have studied PLS in vehicular networks without the use of RISs, the authors in [16] studied the effect of interference on the PLS of vehicular networks, while [20] considered the PLS of RIS-assisted vehicular networks. However, none of these works considered the more realistic scenario of interference effect on PLS within a shared vehicular network or the additional interference suppression achieved by RIS-based PLS system.
Motivated by the potential of RIS-based PLS for vehicular networks, the main contribution of this study is two-fold: Firstly, we consider the PLS of a V2V network and the effect of interference from the co-existing users. Next, we consider the PLS of a RIS-enabled vehicular network and finally, we consider the effect of interference from co-existing users on the RIS-based vehicular network.

4. System Model and Problem Formulation

The system model consists of vehicular nodes in a shared network. There are three nodes of interest, namely, the information source (*S*), the legitimate destination vehicle (*D*) and a passive eavesdropper vehicle (*E*). A wiretap model is assumed, such that *S* initiates a transmission to *D*, while *E* intercepts the confidential information. *S* is assumed to be a vehicular node or a stationary base station. Furthermore, *S* employs a RIS-based scheme as a relay or reflector for vehicular nodes in the network, as illustrated in Fig. 1. The RIS is deployed on a building or other large surface, and used as a relay to *D*. It is assumed that the signal from *S*, can only reach *D* or *E* through the RIS. However, the presence of other vehicles within the shared space and band, leads to cochannel interference to *D* and/or *E*. The received signals at *D* and *E* are respectively represented as:

$$y_D = \sum_{n=1}^{N} h_{D,n} x e^{-j\emptyset_n} + \sum_{k=1}^{K} h_{D,k} x_k + w_D \quad (1)$$

$$y_E = \sum_{n=1}^{N} h_{E,n} x e^{-j\emptyset_n} + \sum_{l=1}^{L} h_{E,l} x_l + w_E \quad (2)$$

where, *N* is the number of RIS elements. *K* and *L* denote the number of interference nodes at *D* and *E*, respectively. x, x_k and x_l are the transmitted signals by *S*, the *k*-th interferer and the *l*-th interferer, while the terms w_D and w_E denote the additive white Gaussian noise (AWGN) at *D* and *E*, respectively. h_D and h_E are the channel coefficients from S to *D* and *E*, respectively. The term $\emptyset_n$ is the reconfigurable phase induced by the RIS's *n*th element. It is worth noting that, in the first terms of (1) and (2), N=1 represents the case when no RIS is deployed. The average secrecy capacity (ASC) can therefore be computed as

$$C_s = \begin{cases} \mathbb{E}[\log_2(1+\gamma_D) - \log_2(1+\gamma_E)], & \gamma_D > \gamma_E \\ 0, & \gamma_D < \gamma_E \end{cases} \quad (3)$$

where $\mathbb{E}[.]$ is the expectation operator, while γ_D and γ_E are the SINR terms at *D* and *E*, respectively.

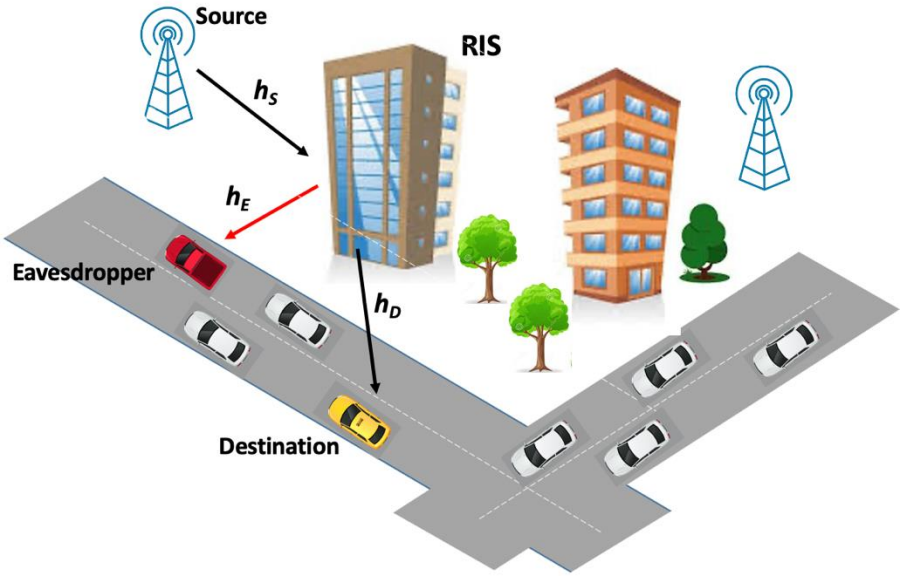


Figure 1: System model for a vehicular network scenario. Source base station using large surface mounted RIS as relay for vehicular communication. RIS with N elements,

5. Results and Discussion

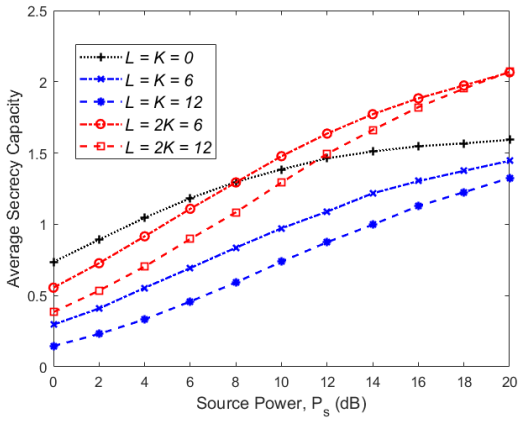


Figure 2: ASC against source power for shared vehicular network interference-limited channel.

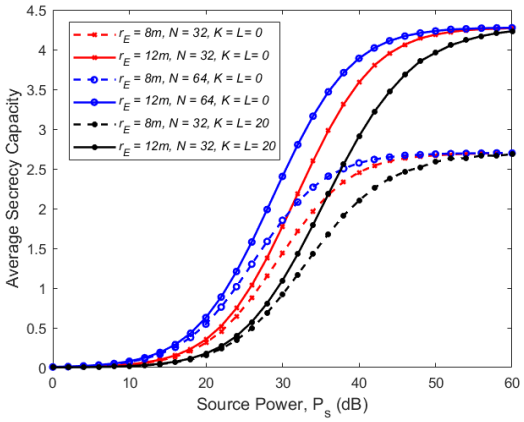


Figure 3: ASC against source power for a) RIS-based VANET and b) RIS-based interference limited network.

In this section, we present and discuss some simulation results from the models discussed earlier. The results illustrate the effect of the main system parameters on the ASC, using Monte Carlo simulations conducted on MATLAB software package.

In Fig. 2, the ASC is examined with respect to the source transmit power at different interference levels. In general, it can be observed that the ASC increases with higher source power, due to greater received SINR. For completeness, we compare the case when there is no interference effect on the legitimate and eavesdropper nodes, i.e. $K = L = 0$. We further observe that, when the number of interferers increase, the ASC degrades, for

example, when interferers increase from $K = 6$ to 12. However, when the effect of interference on the eavesdropper is higher than at the legitimate destination, i.e. $L = 2K$, we observe that the ASC increases above the case with no interfering nodes, beyond SINR of about 10dB. This shows that both legitimate and eavesdropper nodes are affected by interference, but the higher interference at the eavesdropper allows for greater secrecy.

In Fig. 3, we present the ASC analysis for the RIS-assisted networks. We consider the worst case scenario, when the eavesdropper receives equal SINR to the legitimate node. It should be noted that, in every other scenario, the RIS-based system should perform better, since the RIS has the capability of beamforming to direct the desired signal to the legitimate node, depending on the relative unknown position of the eavesdropper. In the first instance, we consider a scenario where the legitimate and eavesdropper nodes receive information through the RIS-relay only, such that $K = L = 0$. We observe that the ASC improves with better source transmit power, increased number of RIS elements or when the distance of the eavesdropper is increased. It can be further noted that within the region considered, the eavesdropper distance has a greater effect on the secrecy capacity than doubling the number of RIS elements. Additionally, we compare with a new scenario, when the legitimate and eavesdropper nodes receive interference from other nodes in the network, or when the source power has other lines of sight apart form the RIS-relay. In this scenario, we observe that, even in the presence of the maximised SNR from the RIS-relay, the interference has an observable effect on the secrecy capacity.

6. Conclusion

In this work, we examined the security of vehicular networks in shared networks from a physical layer approach. Firstly, we considered the effect of interference generated within the shared network on the PLS. Secondly, we investigated the use of a RIS-based scheme to enhance the PLS and followed this with an examination of the interference on this enhanced vehicular network. The secrecy capacity was presented as a metric for measuring the PLS performance. The results indicated that interference adversely affects the secrecy performance with or without the RIS. However, the number of RIS elements greatly enhances secrecy, although the proximity of the eavesdropper was a more important factor on secrecy within the region observed, due to the interference degrading the SINR at the receiving vehicles.

References

[1] C. Chen, J. Hu, T. Qiu, M. Atiquzzaman, and Z. Ren, "CVCG: Cooperative V2V-Aided Transmission Scheme Based on Coalitional Game for Popular Content Distribution in Vehicular Ad-Hoc Networks," *IEEE Trans. Mobile Comput.*, vol. 18, no. 12, pp. 2811–2828, Dec. 2019.

[2] L. Farhan, R. Kharel, O. Kaiwartya, M. Hammoudeh, and B. Adebisi, "Towards green computing for Internet of things: Energy oriented path and message scheduling approach," *Sustainable Cities and Society*,
vol. 38, pp. 195 – 204, 2018.

[3] O. Kaiwartya, Y. Cao, J. Lloret, S. Kumar, N. Aslam, R. Kharel, A. H. Abdullah and R. R. Shah, "Geometry-Based Localization for GPS Outage in Vehicular Cyber Physical Systems," *IEEE Trans. Veh. Tech.*, vol. 67, no. 5, pp. 3800–3812, May 2018.

[4] Y. Wu, A. Khisti, C. Xiao, G. Caire, K. Wong, and X. Gao, "A Survey of Physical Layer Security Techniques for 5G Wireless Networks and Challenges Ahead," *IEEE J. Sel. Areas Commun.*, vol. 36, no. 4, pp. 679–695, Apr. 2018.

[5] L. Sun and Q. Du, "Physical layer security with its applications in 5G networks: A review," *China Commun.*, vol. 14, no. 12, pp. 1–14, Dec. 2017.

[6] M. D. Renzo, M. Debbah, D.-T. Phan-Huy, A. Zappone, M.-S. Alouini, C. Yuen, V. Sciancalepore, G. C. Alexandropoulos, J. Hoydis, H. Gacanin, J. d. Rosny, A. Bounceur, G. Lerosey, and M. Fink, "Smart
radio environments empowered by reconfigurable AI meta-surfaces: An idea whose time has come," *EURASIP J. Wireless Commun. Netw.*, vol. 2019, no. 1, pp. 129, May 2019.

[7] S. Gong, X. Lu, D. T. Hoang, D. Niyato, L. Shu, D. I. Kim, and Y.-C. Liang, "Towards smart radio environment for wireless communications via intelligent reflecting surfaces: A comprehensive survey," arXiv:1912.07794, Dec. 2019. [online]. Available: https://arxiv.org/abs/1912.07794.

[8] M. Cui, G. Zhang, and R. Zhang, "Secure wireless communication via intelligent reflecting surface," *IEEE Wireless Commun. Lett.*, vol. 8, no. 5, pp. 1410-1414, Oct. 2019.

[9] J. Chen, Y.-C. Liang, Y. Pei, and H. Guo, "Intelligent Reflecting Surface: A Programmable Wireless Environment for Physical Layer Security," *IEEE Access*, vol. 7, pp. 82 599–82 612, 2019.

[10] I. Dey, R. Nagraj, G. G. Messier, and S. Magierowski, "Performance analysis of relay-assisted mobile-to-mobile communication in double or cascaded Rayleigh fading," in *IEEE Pacific Rim Conf. Commun. Comput. Sign. Process.*, Aug. 2011, pp. 631–636.

[11] L. Sun, P. Ren, and Q. Du, "Distributed source-relay selection scheme for vehicular relaying networks under eavesdropping attacks," *EURASIP J. Wireless Commun. Netw.*, vol. 2014, no. 1, p. 109, Jul 2014.

[12] J. Zhang and G. Pan, "Secrecy outage analysis with kth best relay selection in dual-hop inter-vehicle communication systems," *AEU – Int J. Electron. Commun.*, vol. 71, pp. 139–144, 2017.

[13] A. Pandey and S. Yadav, "Physical Layer Security in Cooperative AF Relaying Networks with Direct Links Over Mixed Rayleigh and Double-Rayleigh Fading Channels," *IEEE Trans. Veh. Tech.*, vol. 67, no. 11, pp. 10 615–10 630, Nov. 2018.
[14] Z. Shu, Y. Yang, Y. Qian, and R. Q. Hu, "Impact of interference on secrecy capacity in a cognitive radio network," in *Proc. IEEE Global Commun. (GLOBECOM)*, Dec. 2011, pp. 1–6.
[15] D. S. Karas, A. A. Boulogeorgos, G. K. Karagiannidis, and A. Nallanathan, "Physical layer security in the presence of interference," *IEEE Wireless Commun. Lett.*, vol. 6, no. 6, pp. 802–805, Dec. 2017.
[16] A. U. Makarfi, K. M. Rabie, O. Kaiwartya, K. Adhikari, G. Nauryzbayev, X. Li, R. Kharel, "Towards Physical Layer Security for Internet of Vehicles: Interference Aware Modelling," in *IEEE Internet of Things Journal*, (accepted), doi: 10.1109/JIOT.2020.3006527.
[17] A. U. Makarfi, R. Kharel, K. M. Rabie, O. Kaiwartya, X. Li and D. Do, "Reconfigurable Intelligent Surfaces based Cognitive Radio Networks," arXiv: 1912.12197, May. 2020. [online]. Available: https://arxiv.org/abs/2004.11288.
[18] A. U. Makarfi, K. M. Rabie, O. Kaiwartya, O. S. Badarneh, X. Li and R. Kharel, "Reconfigurable Intelligent Surface Enabled IoT Networks in Generalized Fading Channels," arXiv:1912.06250, Dec. 2019. [online]. Available: https://arxiv.org/abs/1912.06250.
[19] A. U. Makarfi, K. M. Rabie, O. Kaiwartya, O. S. Badarneh and R. Kharel, "Physical Layer Security in Reconfigurable Intelligent Surfaces-Assisted Networks in Fisher-Snedecor Composite Fading," in Proc. *12th IEEE/IET International Symposium on Communication Systems, Networks and Digital Signal Processing- (CSNDSP)*, Jul. 2020.
[20] A. U. Makarfi, K. M. Rabie, O. Kaiwartya, K. Adhikari, X. Li, M. Quiroz-Castellanos and R. Kharel, "Reconfigurable Intelligent Surfaces-Enabled Vehicular Networks: A Physical Layer Security Perspective," arXiv: 1912.12183, Apr. 2020. [online]. Available: https://arxiv.org/abs/2004.11288.

MMTC OFFICERS (Term 2018 — 2020)

CHAIR

Honggang Wang
UMass Dartmouth, USA

STEERING COMMITTEE CHAIR

Sanjeev Mehrotra
Microsoft, USA

VICE CHAIRS

Pradeep K Atrey (North America)
Univ. at Albany, State Univ. of New York
USA

Wanqing Li (Asia)
University of Wollongong
Australia

Lingfen Sun (Europe)
University of Plymouth
UK

Jun Wu (Letters&Member Communications)
Tongji University
China

SECRETARY

Shaoen Wu
Ball State University
USA

STANDARDS LIAISON

Guosen Yue
Huawei
USA

MMTC Communication-Frontier BOARD MEMBERS (Term 2018 — 2020)

Dalei Wu	Director	University of Tennessee at Chattanooga	USA
Danda Rawat	Co-Director	Howard University	USA
Melike Erol-Kantarci	Co-Director	University of Ottawa	Canada
Kan Zheng	Co-Director	Beijing University of Posts & Telecommunications	China
Rui Wang	Co-Director	Tongji University	China
Lei Chen	Editor	Georgia Southern University	USA
Tasos Dagiuklas	Editor	London South Bank University	UK
ShuaiShuai Guo	Editor	King Abdullah University of Science and Technology	Saudi Arabia
Kejie Lu	Editor	University of Puerto Rico at Mayagüez	Puerto Rico
Nathalie Mitton	Editor	Inria Lille-Nord Europe	France
Zheng Chang	Editor	University of Jyväskylä	Finland
Dapeng Wu	Editor	Chongqing University of Posts & Telecommunications	China
Luca Foschini	Editor	University of Bologna	Italy
Mohamed Faten Zhani	Editor	l'École de Technologie Supérieure (ÉTS)	Canada
Armir Bujari	Editor	University of Padua	Italy
Kuan Zhang	Editor	University of Nebraska-Lincoln	USA