Traffic congestion worldwide has led to loss of human lives due to failure in transporting accident victims, critical patients, medical, equipments and medicines on time. With the unending growth in vehicular traffic everywhere, the fusion of Internet of Things (IoT) and Vehicular Ad Hoc Network (VANET) has embarked as a promising platform for an Intelligent Traffic Management System (ITMS). In the literature, researchers have suggested various solutions, but without taking into consideration how to prioritize emergency vehicles when traffic system is collapsed due to hacking. This paper proposes a novel intelligent traffic management system for a smart city after considering the research gaps which are yet to be explored in the current scenario. Our proposed solution, not only navigates ambulances to find the shortest possible paths till their destination, but also presents a counter measure to get rid the problem of the traffic light system when it is hacked during its operation. To show the advantages of our proposed solution over already proposed solutions, a simulated environment (CupCarbon simulator) is used to model various scenarios which shows the actual roads and vehicle movements in the implementation. The observed results exhibit the superiority of our proposed solution over state-of-the-art solutions.

organizing both the green light duration and green light sequence on the basis of distance measured with less delay and response time. At the outset, we propose an ITMS based on the type of an incident and hacking of traffic signals. It is inspired by the principles of VANET and IoT where every vehicle in a VANET system share information with one another within a certain range through wireless technology and every device (such as vehicles, Road Side Units (RSUs), users, mobile, traffic control server, etc.) are interconnected to exchange information among themselves.

The remainder of the paper is structured as follows: section 2 presents a brief review of related works. Section 3 introduces our proposed methodology with its algorithm. The performance and evaluation of the proposed work are discussed in section 4. Finally, section 5 concludes the paper and gives future work.

2. RELATED WORKS

Shekher et al. [3] introduced an efficient navigation system based on VANET for ambulances that addresses the problem of ascertaining the shortest path to the destination to get rid of unexpected congestions based on real time traffic information updates and historical data. A dynamic routing system was suggested by integrating real time traffic scenario and Global Positioning System (GPS). The system also includes a metro rail network with road transport system to guide ambulances in real time scenarios. Similarly, Djahel et al. [4] also presented an adaptive framework for an efficient traffic management of emergency vehicles that not only adjusts the traffic signals dynamically, but also recommend drivers required behavior changes, driving policy changes and exercise necessary security controls. Sundar et al. [5] proposed a smart way of controlling traffic for clearing ambulances, detect stolen vehicles and control congestions. This is done by attaching Radio Frequency Identification (RFID) tags on vehicles that assists it to count the number of vehicles passing on a particular path, detect stolen vehicle and broadcast message to the police control room. Additionally, it communicates with traffic controller to prioritize ambulances with the help of ZigBee modules.

The author in reference [6] initiated an intelligent traffic management system which prioritizes emergency vehicles using a different approach, i.e. by categorizing them based on priority levels and incident type occurred. They also proposed a secure method to detect and respond hacking of traffic signals. An ITS has been introduced based on Green Wave system in reference [7] that allows a traffic signal system to turn green whenever it encounters an emergency vehicle, thereby allowing it to acquire all green signals in its pathway. The traffic signal system in this project also identifies stolen vehicle that bypasses the green signal. The main drawback of the Green Wave is that it can create a heavy traffic jam when the synchronization of the signals is disturbed.

Although several researchers have projected many approaches to offer clear pathways to emergency vehicles after assuming a single emergency vehicle coming from a single direction. So far, very few of the existing ITMS considered the case of possible attacks that a traffic signal system may be vulnerable too. Some researchers investigated the possible cyber-attacks on autonomous vehicle and listed the type of attack(s) that can be performed on these vehicles. Autonomous vehicles are capable of identifying its environment using multiple sensors [8].

Significant researches focused on reducing collision or accidents on roads [9, 10] and managing traffic congestions using various concepts like Machine-to-Machine (M2M), IoT and VANET [11, 12]. Optimal route planning for providing shortest traveling time were presented in [13, 14], while transmitting traffic information such as traffic statistics, vehicle density and weather conditions, etc. were proposed in references [11, 15]. Therefore, it is pertinent to say that several works have been done for traffic management system, but not many concentrated on prioritizing emergency vehicles.

3. PROPOSED METHODOLOGY

3.1. Architecture of the Proposed Solution

This section presents our proposed architecture for an ITMS inspired by the fused concepts of VANET and IoT that prioritizes the emergency vehicles on roads. The system firstly measures the gap between an intersection and the emergency vehicle, then dispatched EV from that particular intersection with the consideration that either the traffic signals are hacked or non-hacked, the type of incident and emergency car type. Our main motivation is to allow the emergency cars to bypass heavy traffic and reach their destinations on time as well as ensuring minimum transmission delay for emergency messages. Figure 1 demonstrates our proposed model comprising of Traffic Management Server (TMS), vehicles, RSUs, sensors deployed at strategic locations, all interconnected in a VANET system exchanging with one another. Every emergency vehicle has a unique identity that distinguishes it from the rest of the vehicles on the road. As depicted in Figure 1, the TMS maintains the database of the traffic conditions globally. Once the information of emergency vehicles is obtained from sensors, it estimates the distance of emergency vehicles from an intersection and delivers access to the emergency vehicle on that particular road segment immediately. An RSU of the
The current intersection (RSU-A) informs the RSU of neighboring intersections (RSU-B) with the details of velocity of emergency car and number of vehicles which is moving towards the same intersection-B. On receipt of information from RSU-A, RSU-B will estimate its arrival time at the intersection-B. RSU-B will then regulate both the green light sequence and duration on the basis of expected time of arrival of the same and the received vehicle details from RSU-A. Additionally, the TMS also keeps a check on the response time of emergency vehicles for both normal and hacked traffic signals. If it observes that the traffic signals are hacked or some malicious entities are trying to impersonate emergency car to gain road clearance, it will immediately terminate its access. As soon as the emergency vehicles clear the road, the traffic system continues to function normally. Hence, with no or little delay, emergency vehicles can bypass through the intersections and save lives and property.

The primary objective of the proposed work is to deliver importance emergency messages quickly and lessen the broadcast delay. Four different types of vehicles are considered in our paper: ambulance, police car, fire brigade and ordinary cars. The following subsections show the flow of our proposed solution:

3. 1. 1. Determination of Incident Type

Emergency situations can be broadly classified into three categories:

i. Life-threatening issues such as situations requiring medical assistance during a road accident.

ii. Fire threats such as burning houses.

iii. Crowd control problems such as fights or other criminal activities requiring the presence of police.

The incident type can be quickly analyzed and determined through video surveillances.

3. 1. 2. Determination of Priority Level

Determination of priority levels based on the urgency of the situation is necessary. The priority levels assigned to different types of vehicle on the basis of an incident are given in Table 1. In order to appropriately determine the priority levels of emergency vehicles on the basis of incidents, three cases have been considered:

In case 1, an ambulance is given the topmost priority for a situation when medical assistance is more important, for instance, road accidents or transporting critical patients.

Fire brigades and police can follow after ambulances as they have little or no role to play. In case of fire accidents, fire brigades will be given the priority as paramedics cannot rescue people from fire. Here, case 2 will be considered. Ambulance and police cars will be assigned priorities consequently. In the case 3, Police cars will be given the priority for situations like riots or, fights or crowd controlling situations.

3. 2. Algorithm for Prioritizing Emergency Vehicles

In Table 2, the symbols and descriptions, used in our proposed solution, are shown. When an EV plying on the road send out emergency notifications for priority, its $V_{id}$ will be checked in the database to find out if the vehicle is an authentic EV. On finding the matched id, TMS will schedule EVs on the basis of incident type and priority levels. When more than one EVs are plying on the same road simultaneously, they will be given priority on the basis of their classified cases (case 1, 2, 3) in sequence.

Now, when an RSU is hacked (for instance, DDOS attack) or is compromised by some malicious entity, the entire traffic of the attacked RSU will be shifted to a handler (i.e., another uncompromised RSU). To address such an issue, the handler tries to find the source of packet from which the malicious traffic is disseminated. If the number of packets coming from one source has exceeded the threshold (Th) or the set limit of a normal traffic system, then it will be considered as malicious and the source $S$ of the incoming malicious packets will be immediately blocked by the handler.

![Figure 1. An architecture of an Intelligent Traffic Management System Prioritizing Emergency Vehicles](image-url)
TABLE 2. Symbols and their descriptions

<table>
<thead>
<tr>
<th>Symbols</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>$V_{id}$</td>
<td>Vehicle id</td>
</tr>
<tr>
<td>$V_{Ai}$</td>
<td>Ambulance id of vehicle $i$</td>
</tr>
<tr>
<td>$P_r$</td>
<td>Priority</td>
</tr>
<tr>
<td>$P_{Ai}$</td>
<td>Priority of ambulance $i$</td>
</tr>
<tr>
<td>$D$</td>
<td>Distance of vehicle from RSU</td>
</tr>
<tr>
<td>Th</td>
<td>Threshold for normal traffic</td>
</tr>
<tr>
<td>Handler</td>
<td>RSU which handles attack</td>
</tr>
<tr>
<td>C</td>
<td>Cases, where $c=1,2,3$</td>
</tr>
<tr>
<td>$I_s$</td>
<td>Counter for each source $S$</td>
</tr>
<tr>
<td>$p_s$</td>
<td>Packet from source $S$</td>
</tr>
</tbody>
</table>

Once the situation is handled, the traffic resumes to its normal way of functioning. A flowchart of the proposed step is shown in Figure 2.

3. Identification of Hacking and its Countering

Hacking of traffic signals can interrupt the entire normal functioning of the traffic system. There is a typical pattern of signals in a traffic system during peak and off-peak hours. Any form of intrusion in the system can be deduced as hacking. Once hacking is confirmed, the compromised RSU’s traffic is handled by a handler (by another RSU). The malicious source of the packet is traced and blocked from communicating further with the traffic system. Thus, hacking is handled efficiently. This is depicted in Figure 3 of the proposed solution.

**Figure 2.** Flowchart for Prioritizing Emergency Vehicles

**Figure 3.** Identification of hacking and its countering

**Algorithm 1.** ITMS for Prioritizing Emergency Vehicle algorithm

1. When an EV and normal vehicles are present
2. for each vehicle $i$ passing through RSU in $D$ distance
3. if ($V_{id}==V_{EV}$)
4. if ($N(V_{EV})>1$)
5. Switch($c$)
6. Case 1: $P_{max}=P_r$
7. Allow $V_{EV_{A}}$ to pass ($P_{A} > P_{P}$)
8. Allow $V_{EV_{F}}$ to pass
9. Allow $V_{EV_{P}}$ to pass
10. Case 2: $P_{max}=P_{P}$
11. Allow $V_{EV_{F}}$ to pass ($P_{A} > P_{P}$)
12. Allow $V_{EV_{A}}$ to pass
13. Allow $V_{EV_{P}}$ to pass
14. Case 3: $P_{max}=P_{P}$
15. Allow $V_{EV_{A}}$ to pass ($P_{A} > P_{P}$)
16. Allow $V_{EV_{F}}$ to pass
17. Allow $V_{EV_{P}}$ to pass
18. End if
19. End if
20. End if
21. End

To detect attacks on RSU:

1. if (bitrate $>$ Th)
2. Attack Detected
3. Divert attack traffic to Handler
4. In Handler
5. for each packet $p_s$
6. $I_s++$
7. if $I_s > \text{lim}$
8. Block $S$
9. End if
10. End if
4. PERFORMANCE AND EVALUATION

For simulation, we have implemented our proposed solution on CupCarbon U-One simulator, which is an open source and free network simulator for the simulation of smart city and IoT applications. In this section, performance of our system is evaluated by comparison with previous proposed works, i.e., EPCS [6] and Green Wave [7] system. A total of 20 vehicles and eight intersections between each RSUs have been considered. We have taken 10 vehicles between the starting point of EV and the incident location (destination) during simulations. The average speed of the vehicle is set at 15 km/hr and distance between two successive vehicles is taken at 1 meter. The simulation results, in Figure 4, show that Green Wave, EPCS and our proposed system require 17.5 minutes, 12.7 and 11.2 minutes, respectively to meet the set target. In order to examine the proficiency of handling hacking in the system, we have considered that 10% of hacked traffic signals are hacked. When traffic systems are compromised, Green Wave and EPCS show 19.2 minutes and 14 minutes respectively, while our proposed work shows 11.8 minutes to meet the target even in a hacked scenario. This shows the superiority of our proposed solution over Green Wave method and EPCS. At the outset our proposed solution shows 12% improvement over EPCS system and 17% over Green Wave.

Figure 5 shows bit rate of packets of traffic signals per seconds.

It is observed from the plotted graph that during a normal working of RSUs, the average bit rate is 12.5 Mbps. When an attack begins at 4th sec after a few seconds, the bit rate rises to 20 Mbps leading to heavy congestion in a few minutes and eventually collapses the traffic system. The traffic is then shifted to a handler to handle and normalize the flow of bit rates. We witness here that there is a drop in bit rates of 12.5-13 Mbps on the compromised road.

5. CONCLUSION AND FUTURE SCOPE

Several researches have been carried out on intelligent traffic monitoring system, but a secure and efficient solution for emergency vehicles is yet to discuss. Therefore, an ITMS has been proposed to prioritize emergency vehicle by fusing the concept of VANET and IoT with an effort to ease the flow for ambulances in urban areas. It also presents a method to detect and counter hacking of traffic signals which is a very common problem nowadays. The distance between intersections and emergency cars were estimated to achieve the target travel time of emergency vehicles with minimal delay time, considering both hacked and non-hacked traffic signals. The proposed model not only distinguishes emergency messages with several priorities, but also prevents false warnings from malicious entities. The experimental results show that our system outperformed others in terms of time constraints, thereby achieving the goal of allowing emergency services to be met at the shortest possible time. The proposed system eliminates the time delay in medical assistance for accident victims, transporting critical patients and medicines.

For future directions, different priority levels for multiple incidents and scenarios can be considered. The main issue with IoT is that the security of the entire system have to be concentrated on and not a particular IoT layer, device or software. Hence, integrating the entire traffic management system with multiple layer security for various data generated from various sources can be another subject of future scope.

6. REFERENCES

Intelligent Traffic Management System for Prioritizing Emergency Vehicles in a Smart City

L Sumia, V Ranga

Department of Computer Engineering, National Institute of Technology, Kurukshetra, India

Paper Info

Keywords: Intelligent Traffic Management System
Emergency Vehicles
Road Side Units
Smart Cities


