Indian Journal of Science and Technology, *Vol 10(10), DOI: 10.17485/ijst/2017/v10i10/108251, March 2017*
ISSN (Print) : 0974-6846
ISSN (Online) : 0974-5645

Intelligent Transportation Architecture for Enhanced Security and Integrity in Vehicles Integrated Internet of Things

Surbhi Gill, Pooja Sahni, Paras Chawla, Sukhdeep Kaur

Department of Electronics and Communication Engineering, Chandigarh Engineering College, Landran, Sector 112, Greater Mohali – 140307, Punjab, India; gillsurbhi@gmail.com, pooja.ece@cgc.edu.in, dr.paraschawla@cgc.edu.in, sukhdeep.ece@cgc.edu.in

Abstract

Objectives: To devise and simulate an effective and novel approach for intelligent transportation architecture with higher security and integrity in vehicles integrated Internet of things. **Methods/Statistical Analysis**: Dynamic Clustering Enabled Secured IoT method is used to enhance the security and integrity in vehicles integrated IoT. The dynamic formation of a simulated environment is implemented so that the movement of vehicles on road can be monitored. **Findings:** The proposed intelligent transportation architecture is effective in terms of higher security and integrity with very less complexity and cost factors. The overall vehicular network is secured using proposed novel architecture. **Application/Improvements:** The integration of satellite and base station based real time monitoring in association with road side units are making the overall network more secured which reduces the collisions.

Keywords: Intelligent Transportation Architecture, Internet of Things, Pervasive Computing, Security and Integrity in Vehicles

1. Introduction

Internet of Things (IoT)[1] is one of the growing classical and prominent domains in advance wireless and sensor based environments for multiple applications. Intelligent traffic based systems are prominently used for the tracking, capturing and monitoring of running objects on road. Generally, this implementation was done under the umbrella of VANET[2], but now it transformed to intelligent VANETs with effective global positioning protocols as in Figure 1 depicting the GPS based diagrammatic approach for IoT enabled highway traffic control. The sniffer detectors and collision monitoring with intelligent sensors are now part of the vehicular ad hoc networks and then it became one of the key components in IoT based applications.

The implementations under IoT are covered in Pervasive Computing (PC) or Ubiquitous Computing (UbiqC) and lots of research initiatives are going on.
Some of the key implementations under IoT are

- Smart Cities
- Smart Offices
- Intelligent Home Appliances
- Smart medical ambulances
- Patient Porting Containers
- Intelligent Vehicular Tracking Systems
- Automated on road toll collections
- Automated traffic controlling devicesand many others

2. Attacks on Vehicular Ad Hoc Networks

A number of attacks and sniffers are prevalent on the cyber space as well as cracking communities on which the security experts are working. Following are classical attacks which are implemented in vehicular based systems

- Denial of service (DOS) Attack[3]
- Distributed Denial of service (DDOS) Attack[4]

**Author for correspondence*

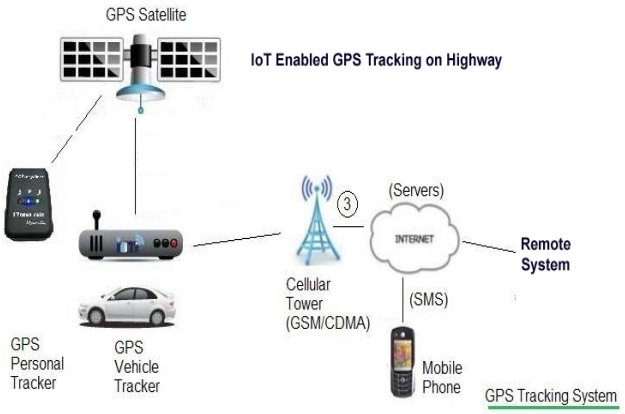

Figure 1. Classical Diagrammatic Approach for GPS Tracking.

- Timing Attack[5,7]
- Wireless Node Sybil Attack[6]
- Node ImitationAttack[8]
- Node Tampering Assault[9]
- Packet Alteration Assault[10]
- Node Illusion[11]
- Sniffers and Packet Capturing[12]
- Application Level Attack[13]

3. Projected Effective System for Intelligent and Secured Traffic

The proposed as well as effective intelligent transportation system is depicted in Figure 2 with assorted wireless technologies in association for higher degree of performance and accuracy.

Following are the steps and modules integrated for the development of smart and effective intelligent system.

a. Initialize and Active the Sensor Based Vehicle (SBV) system integrated.
b. SBV communicate in parallel to global positioning system along with the base station and that directly communicates with the satellite.
c. Sensor Object integrated with an intelligent firewall and observation panel so that real time tracking can be done.
d. A secured dynamic security key transmitted for higher security, integrity and overall trust of the network environment.
e. Following operation shall be carried by the integrated firewall.

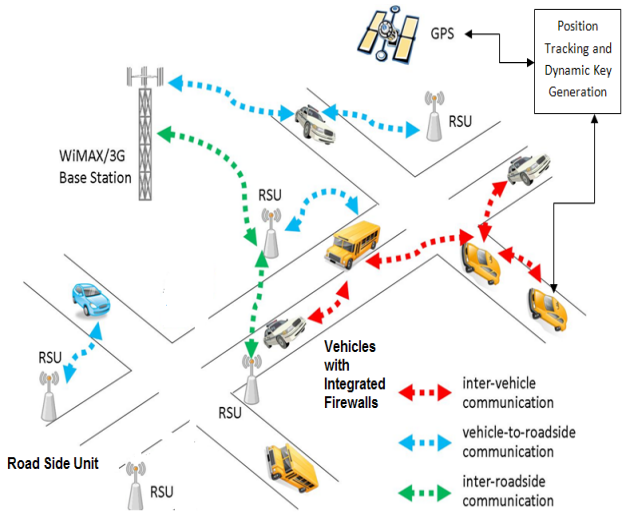

Figure 2. Proposed Intelligent Transportation System.

i. Analysis of Raw PCAP (Packet Capturing).
ii. Blocking of the Data Packets based on the specific Signature containing malware.
iii. Online Firmware updating so that current attacks as well as the signatures of malicious packets can be updated instantly in the system.

f. The legitimate signals directly communicate and get authenticated at regular intervals with satellite.
g. Sensor Based RSU transmit the data to base station, satellite and collaborate the vehicular embedded objects

4. Architecture of Smart Firewall

Figure 3 illustrates the constituents of smart firewall and road side units which are effectual and performance aware components in the proposed approach.

5. System Model

In this research work, the clustering integrated approach is used in which the minimum distance is maintained and the avoidance of collision is implemented. Figure 4 Further, the possibility of upcoming intrusion or obstacle is identified so that overall performance and integrity of road can be done as shown in Figure 5.

6. Implementation

- Deployment of the Sensor Nodes (SN) and Formation of Wireless Sensor Network (WSN) on the Highway.

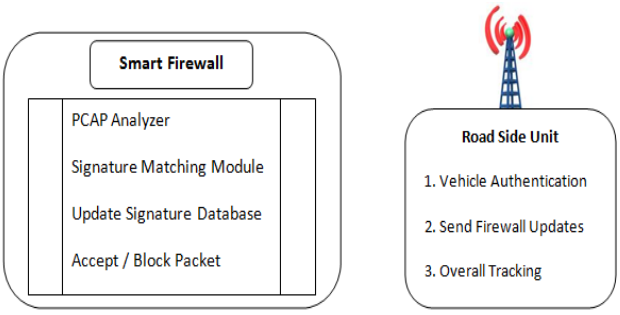

Figure 3. Proposed Layered Approach for Smart Traffic Implementation.

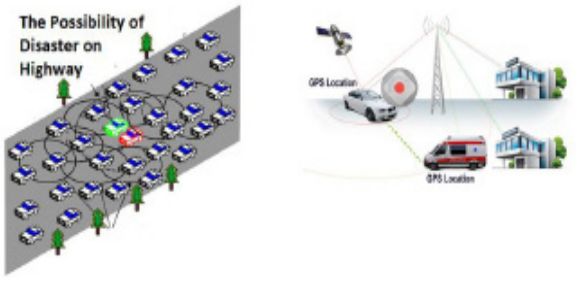

Figure 4. Distance Aware Vehicular and Security Optimization.

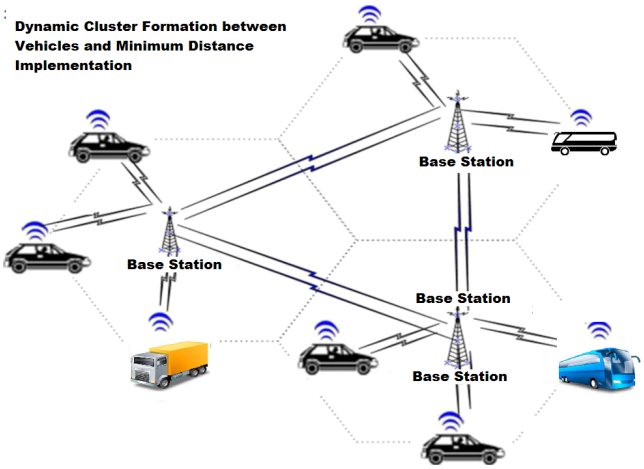

Figure 5. Proposed System Model with the Base Station and Controlling Points for Vehicles.

- WSN Node / Chip Based direct communication based on the IoT based secured environment so that real time tracking can be done
- The monitoring protocol and station keep track of each vehicle on road including remote vehicles so that any possibility of collision or congestion can be reported as well avoided.
- Overall performance and lifetime of the network will improve with the integration of sensor based devices
- The base tower, satellite and GPS tracking protocols and algorithm keep on tracking and communicating with each other so that higher degree of integrity and overall security can be escalated.

7. Proposed Algorithm - DCESI (Dynamic Clustering Enabled Secured IoT)

1. Initialized and Activate the Road for IoV(RI)
2. Set Wireless Sensor Nodes with Max. Limit N Nodes
3. Set Threshold Factor (Th) as Distance Measure. Threshold is used for the identification of minimum distance and avoidance of collisions
4. Activation of Network Environment in which the nodes work
5. Activation of each Wireless Sensor Node with Cluster (CH)
6. Investigation and Calculation of the Obstacle Vector
7. Activation of Base Station (BS). Base Stations keep track the distance and GPS location of each vehicle
8. If (dist (RI_i, RI_j) >Th)
   Signal [i]=Base Station (BS) [i]
   (V_i, V_j -> Vehicles)
9. If Distance Vector greater than Threshold Level
   (i) Signal from RI to be sent to Base Station (BS) and Satellite (S)
   (ii) Clustering of Highway with Sensors with Repeated Distance Threshold Checking
10. Detailed Analytics and Reports Generation

Figure 6 illustrates the data flow diagram with number of modules working at programming level so that all the

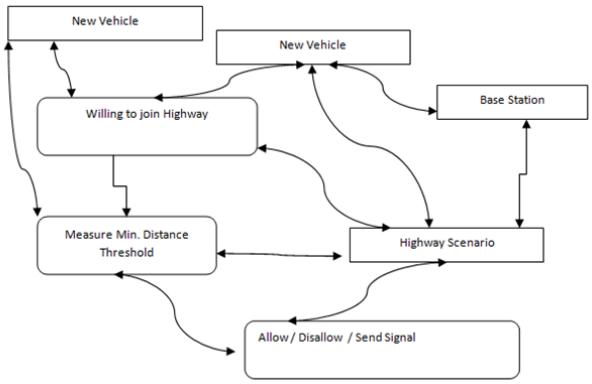

Figure 6. DFD of the Proposed Approach.

segments of proposed architecture and systems can be integrated in effectual perspectives.

Figure 7 depicts the line graph with the performance of classical and proposed approach in terms of data transfer and shows that the proposed approach is improved as compared to the existing approach.

Figure 8 depicts the simulation of proposed IoT based architecture with the vehicle moving on highway. The road side units and stations are controlling as well as monitoring the activities including distance and movements.

Figure 9 depicts the formation of cluster on road so that the distance matrix can be analysed at different phases.

Figure 10 illustrates the line graph with the incurred-packets loss during the simulations of existing and proposed approach and shows that the proposed approach is having less number of packet losses as compared to the existing approach.

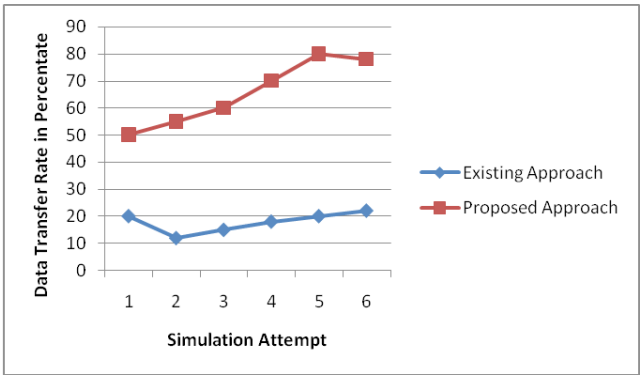

Figure 7. Comparison between Existing and Proposed in terms of Data Transfer.

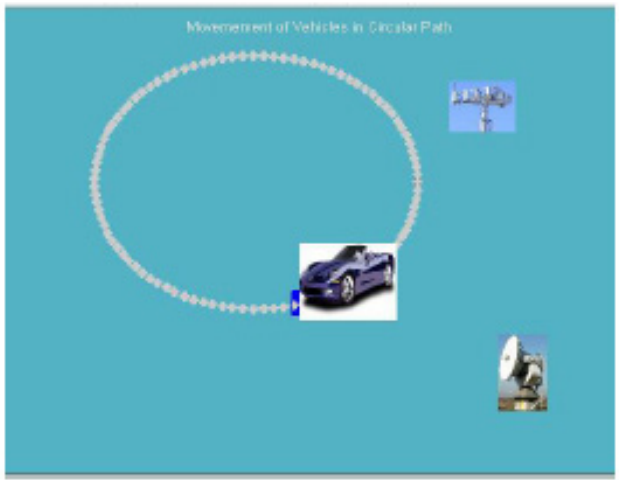

Figure 8. Network Simulation Scenario.

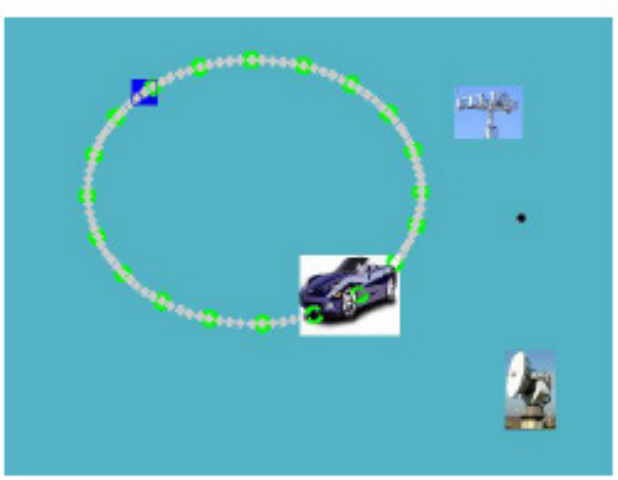

Figure 9. Clusters Formation in Road Side Units with Signal to Base Stations.

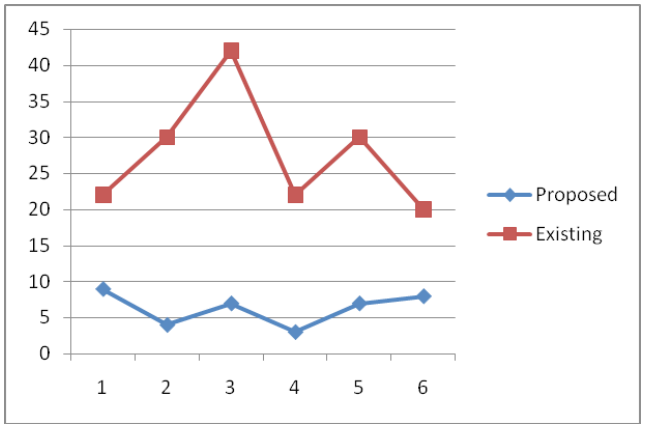

Figure 10. Comparison between Existing and Proposed in terms of Packet Loss.

Table 1. Performance Level of Existing and Proposed Approach

Simulation Attempt	Performance (Existing)	Performance (Proposed)
1	78	90
2	68	87
3	60	89
4	50	91
5	89	98

Table 1 presents the values during simulation associated with the performance of classical and proposed approach and shows that the proposed approach is enhanced and effective as compared to the existing approach.

The line graph in Figure 11 depicts the performance level of classical and proposed approach and illustrates

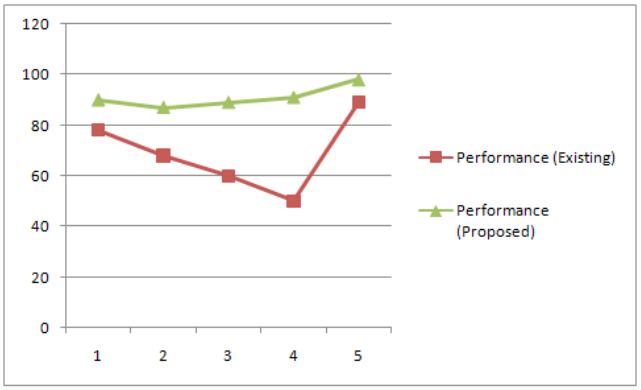

Figure 11. Comparison between Existing and Proposed in terms of Overall Algorithmic Effectiveness.

that the proposed approach is enhanced and effective as compared to the existing approach.

8. Conclusion

The research on wireless based secured transportation systems is still going on and being integrated by assorted automobile companies. Still, there is colossal span for the development of novel, unique and effective algorithms. In this research manuscript, the real time tracking, collision detection and avoidance protocol is proposed and executed so that the entire IoT based ecosystem can be secured. This proposed algorithm is an improvement in assorted parameters with better performance cumulatively.

9. References

1. Xia F, Yang LT, Wang L, Vinel A. Internet of things. International Journal of Communication Systems. 2012; 25(9):1101. Available from: Crossref
2. Elsadig MA, Fadlalla YA. VANETs security issues and challenges: A survey. Indian Journal of Science and Technology. 2016 Jul 26; 9(28):1-8.
3. Hofmann-Wellenhof B, Lichtenegger H, Collins J. Springer Science & Business Media: Global positioning system: theory and practice. 2012; p. 1-229.
4. Sharifi AM, Amirgholipour SK, Alirezanejad M, Aski BS, Ghiami M. Availability challenge of cloud system under DDOS attack. Indian Journal of Science and Technology. 2012 Jun; 5(6):2933-37.
5. Rafeh R, Khodadadi M. Detecting Sybil Nodes in Wireless Sensor Networks Using Two-hop Messages. Indian Journal of Science and Technology. 2014 Sep 30;7(9):1359-68.
6. Velmurugan S, Logashanmugam E. Detecting and Replacing Beacon Node Failure and Secure Communication in WSNs (DRBF). Indian Journal of Science and Technology. 2016 Oct; 9(39):1-7. Available from: Crossref
7. Conti M, Di Pietro R, Mancini LV, Mei A. A randomized, efficient, and distributed protocol for the detection of node replication attacks in wireless sensor networks. Proceedings of the 8th ACM international symposium on Mobile ad hoc networking and computing. 2007 Sep; p. 80-89.Available from: Crossref
8. Rama A, Masthan M. Quick Detection Involving Cellular Duplicate Node Assaults in Cellular Sensor Networks Using SPRT. Middle-East Journal of Scientific Research.2014; 17(12):1883-86.
9. Kumar MD, Rao AN. Defending Towards Falsification and Packet Descent Attacks in Wireless Sensor Networks. 2017 Jan; p. 1-9.
10. Eriksson J, Krishnamurthy SV, Faloutsos M. TrueLink: A practical countermeasure to the wormhole attack in wireless networks. Network Protocols, 2006. ICNP'06. Proceedings of the 2006 14th IEEE International Conference. 2006 Nov; p. 75-84. Available from: Crossref.
11. Qadeer MA, Iqbal A, Zahid M, Siddiqui MR. Network traffic analysis and intrusion detection using packet sniffer. In Communication Software and Networks, 2010. ICCSN'10. Second International Conference. 2010 Feb; p. 313-17. Available from: Crossref
12. Xu W, Trappe W, Zhang Y, Wood T. The feasibility of launching and detecting jamming attacks in wireless networks. In Proceedings of the 6th ACM international symposium on Mobile ad hoc networking and computing. 2005 May; p. 46-57.Available from: Crossref.