Current Trends in Biomedical Engineering & Biosciences
ISSN: 2572-1151

Juniper PUBLISHERS key to the Researchers

Research Article
Volume 6 Issue 1 - July 2017
DOI: 10.19080/CTBEB.2017.06.555678

Curr Trends Biomedical Eng & Biosci

Improvised Autonomous Car for a Safe Travel

Bhagyalakshmi A[1]*, Jashwanthi A[2], Asha S[2] and Roshni P[2]

[1]*Assistant Professor, Velammal Engineering College, India*

[2]*BE Computer Science and Engineering, Velammal Engineering College, India*

Submission: March 08, 2017; **Published:** July 26, 2017

***Corresponding author:** Bhagyalakshmi A, Assistant Professor, Velammal Engineering College, India,Email: kirubhagya@gmail.com

Abstract

An autonomous car is a self driving car that can operate itself without a human interaction. The current developed autonomous car that uses V2V protocol for communication lacks secured data transmission between vehicles. In this paper, we implement V2V protocol along with AES encryption algorithm and zigbee cryptographic key.AES along with zigbee provides privacy in data sharing and also enhances vehicular communication. ZigBee provides secured communication, transportation of cryptographic key and helps in controlling the devices. It is developed using the basic security framework defined in IEEE 802.15.4.Advanced Encryption Standard is used to encrypt sensitive data.

Keywords: V2V; Security; AES; Zigbee

Introduction

An autonomous car is also called self-driving car or robotic car is an innovative technology which need to be improvised. The idea for autonomous car was laid by THE ELECTRIC UTILITY COMPANY. In 1980's, the first autonomous cars were built. The main feature of using autonomous car is that it reduces traffic collision. This robotic car has several features like RADAR, Lidar, computer vision, GPS, odometry. It decreases the pollution in terms of car sharing. Due to its self governance it gives best performance in uncertain environment and compensates the system failure. Google is the leading company which performs vast research on autonomous cars. Its current version is WAYMO which stands for new way mobility [1,2].

The centralized base station used to govern the communication by providing public key and digital certificate for security. The central base station is also called as central authority. The certificate provided here does not provide any privacy. The major bane of this protocol is that it shares a particular autonomous car's information with all the other cars. Due to this, it increases the traffic in information sharing, pollution and we lose our privacy.

Current Methodology

V2V protocol is a vehicle to vehicle communication protocol that is used for communicating information among autonomous cars. Information that is shared are location, direction of travel, braking and loss of stability. Dedicated short range communication (DSRC) and mesh topology is used. It is a type of MANET [3,4].

The centralized base station used to govern the communication by providing public key and digital certificate for security. The central base station is also called as central authority. The certificate provided here does not provide any privacy. The major bane of this protocol is that it shares a particular autonomous car's information with all the other cars. Due to this, it increases the traffic in information sharing, pollution and we lose our privacy.

Modified Implementation

ZigBee is a wireless mesh network specification for low-power wireless local area networks (WLANs) that cover a large area. ZigBee was designed to provide high data throughput in applications because it provides low power consumption. ZigBee network has a special feature of Self Organizing. Since a node in the network can relay the data to its neighbor, the range can be extended much longer than 50 meters.

The Advanced Encryption Standard or AES is a symmetric block cipher implemented in software and hardware throughout the world to encrypt sensitive data .This new encryption algorithm is easy to implement in restricted environments (for example, in a smart card) and offer good defenses against various attack techniques. It is found that AES IS at least six time faster than triple DES .It is based on 'substitution–permutation network. The AES algorithm is based on number of substitutions, permutations and linear transformations, each of which is executed on data blocks of 16 byte – therefore it is termed as block cipher. These operations are repeated several times, called "rounds". During each round, a unique round key is calculated out of the encryption key, and incorporated in the calculations. Till now, no practical cryptanalytic attacks against AES have been found. In addition, AES has built-in flexibility of key length .It allows a degree of 'future-proofing' against progress to perform exhaustive key searches [5,6].

System Architecture (Figure 1 & 2)

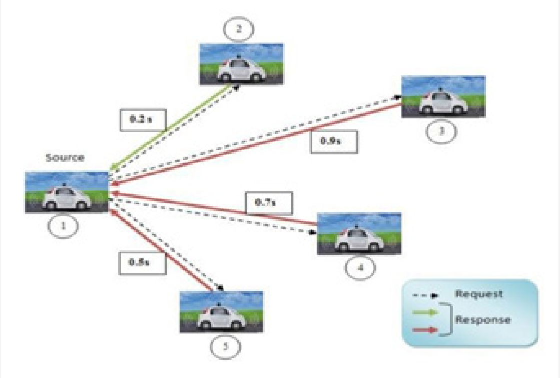


Figure 1

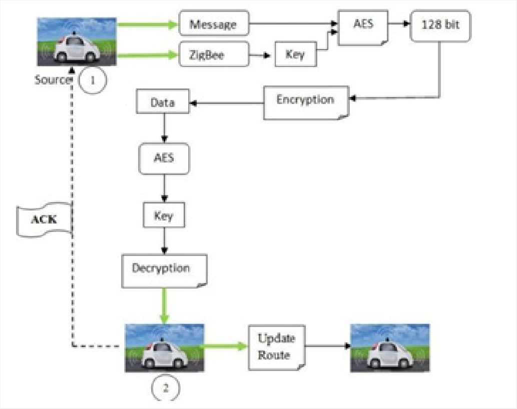


Figure 2: Communication between source and its nearest neighbours.

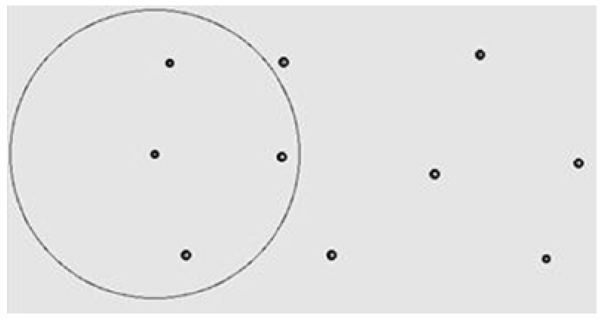
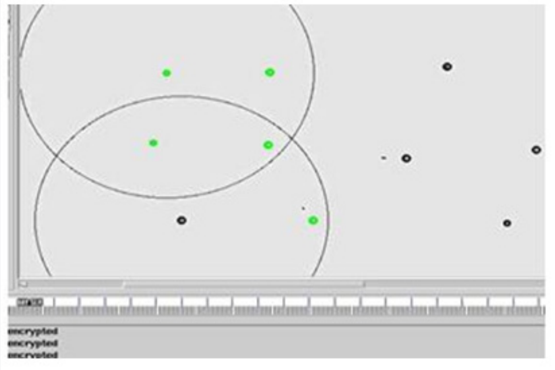


Figure 3

Module Description

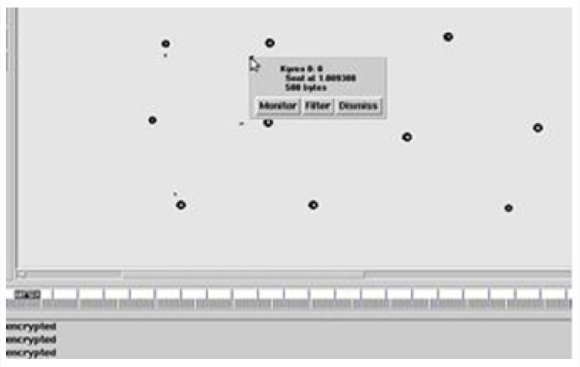
Identifying Vehicular Network: Senses the nearby vehicles using V2V protocol and detects the vehicular network. After identifying a network the source node sends beacon (request) messages to all the nodes in that network (Figure 3 & 4).



encrypted
encrypted
encrypted

Figure 4

Replying to Baecon Message: The destination vehicle accepts the request for data sharing. Nearest neighbor is identified from the response that first reaches the source node (Figure 5).

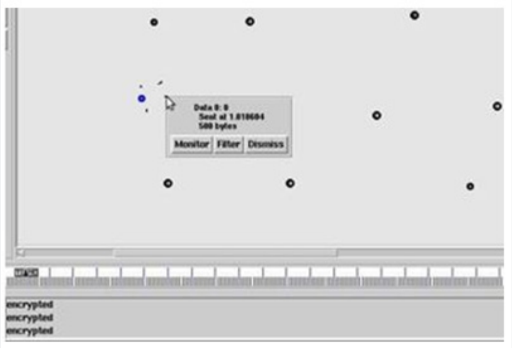


Kyes 0: 0
Seal at 1.809388
500 bytes

encrypted
encrypted
encrypted

Figure 5

Encrypted Data Sharing: The source vehicle encrypts its data using AES algorithm along with zigbee which provides cryptographic key. The encryption key used in AES is 128 bits, which generates a single key for all data transmission and hence not secured. Zigbee is an (Figure 6).



Data 0: 0
Sent at 1.818684
500 bytes

encrypted
encrypted
encrypted

Figure 6

How to cite this article: Bhagyalakshmi A, Jashwanthi A, Asha S, Roshni P. Improvised Autonomous Car for a Safe Travel. Curr Trends Biomedical Eng & Biosci. 2017; 6(1): 555678. DOI: 10.19080/CTBEB.2017.06.555678.

Rebroadcasting by neighbouring nodes: After receiving the data, destination vehicle acknowledges the source vehicle saying that it successfully transmitted the encrypted data. Further it rebroadcasts the network in the similar way so that data traffic doesn't occur (Figure7).

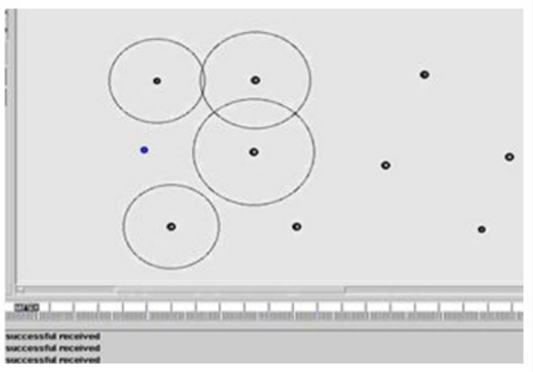

successful received
successful received
successful received

Figure7

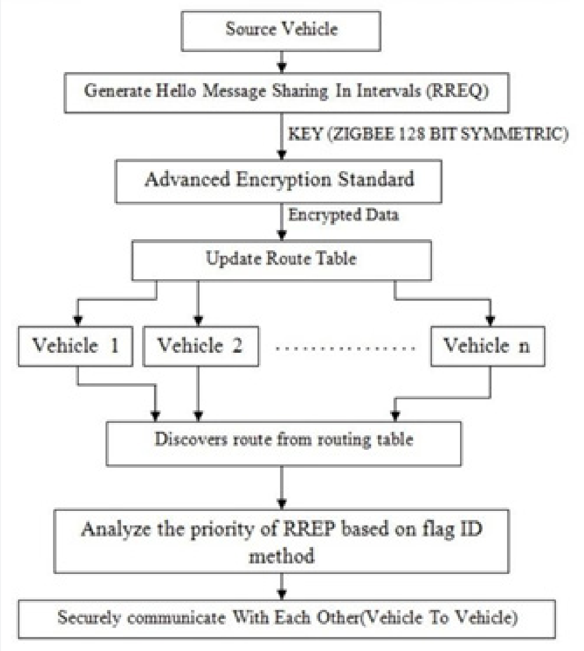

Source Vehicle
Generate Hello Message Sharing In Intervals (RREQ)
KEY (ZIGBEE 128 BIT SYMMETRIC)
Advanced Encryption Standard
Encrypted Data
Update Route Table
Vehicle 1
Vehicle 2
....
Vehicle n
Discovers route from routing table
Analyze the priority of RREP based on flag ID method
Securely communicate With Each Other(Vehicle To Vehicle)

Figure 8

System Flow (Figure 8)

STEP 1: The source vehicle forms the vehicular network.

STEP 2: It detects the nearby vehicles and sends the request.

STEP 3: The detected nearby nodes sends the response to the source.

STEP 4: The source node then shares the data with the nearby vehicles i.e., encrypted with AES algorithm using zigbee, a cryptographic key. The encrypted data consists of only the vehicular movements.

Conclusion

The advancement in technologies has brought many changes in the field of computing and communication. Recent announcements states that many manufacturers are aspire to soon sell such vehicles in the market. Autonomous cars will soon be widely available giving a solution for the transportation problems. Thus, the proposed system will add many benefits to the predicted features as it overcomes two main biggest disadvantages: privacy (security) and safety.

By using Zigbee and AES algorithm with V2V protocol we can ensure that there is privacy between the vehicles and data hiding can be achieved. We believe that the evolution of the advancement in the technology will cause a greater change in the automotive value chain.

References

1. http://www.ijettjournal.org/volume-3/issue-3/IJETT- V3I3P205.pdf
2. Bielsa A, Gascón D (2010) Triple Security in ZigBee: Link, Network and Application layer Encryptions.
3. https://en.wikipedia.org/wiki/Autonomous_car
4. http://www.intel.in/content/www/in/en/automotive/driving-safety-advanced-driver-assistance-systems-self-driving-technology-paper.html. 5.
5. http://ieeexplore.ieee.org/xpl/login.jsp?tp=&arnumber=4531925&url=http%3A%2F%2Fieeexplore.ieee.org%2Fiel5%2F4531847%2F4531848%2F04531925.pdf%3Farnumber%3D4531925
6. http://dl.acm.org/citation.cfm?id=2555192

DOI: 10.19080/CTBEB.2017.06.555678

How to cite this article: Bhagyalakshmi A, Jashwanthi A, Asha S, Roshni P. Improvised Autonomous Car for a Safe Travel. Curr Trends Biomedical Eng & Biosci. 2017; 6(1): 555678. DOI: 10.19080/CTBEB.2017.06.555678.