A Secure Data Transmission in VANETs using HC12

Kalkundri Ravi, Rajashri Khanai, Kalkundri Praveen

***Abstract:** Vehicular ad hoc networks (VANETs) is an Intelligent Transportation System and a part of MANETS. VANETs communication is wireless between vehicles and different nodes along the road to increase efficiency and human safety. VANETs embedded all the features of MANETs and almost any Ad Hoc Network. We have discussed various features of VANET and different types of attacks, since the VANET communication is open in nature; they are prone to various types of attacks. Although various attractive features, VANETs also face some challenges like communication with different types of nodes and sensors and gather information or data. Our major focus is on securing this data or information sent by the sender node before transmitting on the network to another node in the network. We intend to solve this by using a wireless LoRa module and cryptography algorithm like ECDH for secure data transmission and solve the security risks and privacy problems. Our work discusses VANET communication method and structure. We provide a simple communication method using P2P topology method and ECDH cryptographic algorithm for keeping the data secure.*

***Keywords :** VANET, Security, HC12, RSA, ECDH*

I. INTRODUCTION

Vehicles are playing a very role in our human life. Vehicles are used to transport goods or passengers. The major concern with vehicles world-wide is the safety issues. Another issue that we intend to address is the increasing traffic and the congestion caused by the huge traffic. To provide all the information which is required for the vehicular network, Vehicular Ad Hoc Network (VANET) came into existence. VANET infrastructure is subgroup of Mobile Ad Hoc Network (MANET). All the properties of MANETs are applied to VANET's. All the features are used to improve the efficiency and consistency of the system. Further VANET's are vital component of Intelligent Transport System (IET). The advancement of technology, VANETs or vehicles is equipped with GPS or Wi-Fi for communication. VANET infrastructure is created to provide information for the people who are travelling in vehicles. The various types of information's are like safety information, weather prediction, warning the driver about upcoming dangers as early as possible, recognition the traffic status and help the driver to take proper decision and other related issues which can help the driver. The other information is like to provide infotainment for the commuters, toll payment, fuel payment, parking ticket, etc [1].

Communication in VANET takes place between Vehicles to Vehicles called V2V and Vehicle to the Infrastructure (V2I) network called as Road Side Units (RSU). There are various topologies that are involved in the communication in VANETs. According to the situation and the type of message to be dissipated the type of topology is used for communication dynamically.

II. VANET BACKGROUNG

A. VANET Architecture

The nodes in VANETs are the vehicles that are mobile in nature and hence VANET network is an infrastructure less network. Since the vehicles movement is not uniform, the entire infrastructure is very dynamic in nature. Thus the network hoes not have fixed topology. The topology also changes dynamically. The vehicles are smart enough as all the vehicles are operational with a special device called On Board Unit (OBU). The OBU's consists of processor, memory and antennae for communication. Each vehicle is equipped with a unique OBU's. Vehicles communicate within themselves, via the OBU's only. The vehicles communicate to the infrastructure via the Road Side Unit (RSU). The RSU's are interconnected via cables. The vehicles communicate through its OBU with other vehicles OBU or RSU's.

Manuscript received on February 10, 2020.
Revised Manuscript received on February 20, 2020.
Manuscript published on March 30, 2020.
* Correspondence Author

Kalkundri Ravi*, Asst. Professor, Dept. of Computer Science and Engineering, K.L.S's Gogte Institute of Technology, Belagavi, Karnataka, India. Email: kalkundri.ravi05@gmail.com

Dr. Rajashri Khanai, Professor and HOD, Dept. of Electronic & Communication Engineering, KLE Society's College of Engineering & Technology Belgaum, Karnataka, India. Email:rajashri.khanai@gmail.com

Kalkundri Praveen, Asst. Professor, Dept. of Electronic & Communication Engineering, K.L.S's Gogte Institute of Technology, Belagavi, Karnataka, India. Email: kalkundri.praveen@gmail.com

Retrieval Number: F8874038620/2020©BEIESP
DOI:10.35940/ijrte.F8874.038620
Journal Website: www.ijrte.org

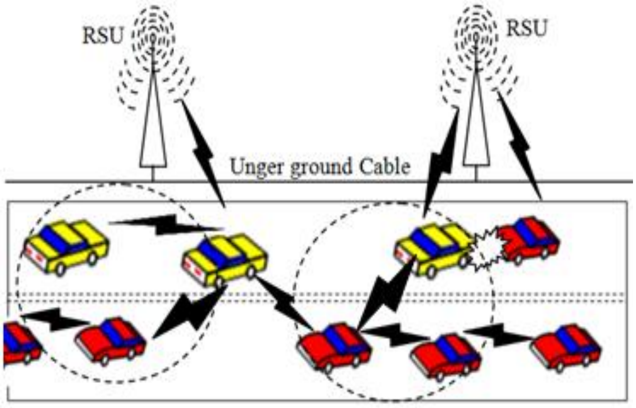


Fig. 1: A typical VANET Infrastructure.

In the Fig. 1 shown above, we can see that there are RSU located along the roadside. The vehicles communicate among themselves and with the RSU's for transfer of information. As shown in Fig. 1, there are two vehicles that have meet with an accident, then the vehicles that have meet with accident, sends the message to the nearby RSU or neighbouring vehicles. Further the RSU's send the messages to the other vehicles that are travelling in the same path and towards the accident zone. By this the upcoming vehicles are alerted and more accidents can be avoided.

Further, as shown in the Fig. 1, the vehicles also communicate to either the RSU that is in the range or the vehicle that are in the range. The vehicles that cannot communicate the RSU's, communicate with other vehicles. As soon there is accident occurred between vehicles, those vehicles send a warning message to other upcoming vehicles coming in that direction. The message is sent via the RSU's or other vehicles. The vehicles act as intermediate nodes if not the destination node. If the vehicle is not in the radius of the RSU, the only way for communication is through other vehicles.

B. Features of VANETs

VANETs are subset of Mobile Ad Hoc Networks (MANETs) and a part of ITS systems. Though, VANETs are considered as separate domain and a distinct research field for many researchers. VANETs includes many characters of MANETS and also it has additional distinct characteristics that make it little different from MANETs. Some of the characteristics of VANETs that are unique are as follows [5]:

- **High Mobility:** The nodes (vehicles) are very dynamic in nature, and are in constant motion. The speed of every vehicle differs, where the speed may be slow or fast. The continuous motion of the node is one of constrains for the topology and layout for communication.
- **Rapidly Changing Network Topology:** Since the nodes are dynamic in nature, the network topology changes frequently in VANETs. Another reason is that all nodes do not travel; at the same speed, hence the topology must be dynamically adaptive.
- **Boundless Network Size:** VANETs is one of the networks where the number of nodes is not fixed. VANET involves vehicles of all types and also includes vehicles which are within city limit or the vehicles that are on highways. Hence, VANETs network are not limited to the limited size of network, but any number of vehicles can be a part of the network at a time.
- **Identification Secrecy:** VAENTs communicate via the network id, but there are certain applications that require the actual identification like vehicle ID at the toll booth. In such cased the original must be hidden and should be kept secure and a protection measure have to be taken if any attack occurs.
- **Delay-sensitive Data Exchange:** Messages should be transmitted without any delay in VANET network. The reason for delay can be like, security concern, more intermediate nodes, etc... Applications that require less delay, care must be taken for such applications.
- **Self sustaining Network:** Like MANETs, VANETs are also self sustaining network. The network keeps on working in case of any failure or any issues like link failure or node failure.
- **Rich Resources:** As the nodes or vehicles have ample energy, hence power is not an issue for computation. Having enough power, additional computation or routing decision or calculate best suitable topology etc., which can be helpful for VANETs. We can have addition schemes such as usage of cryptographic algorithms like ECDSA, RSA, etc., which may require more energy for computation.
- **Better Security:** VANET nodes have better security, as the nodes are in constant motion and change their topology frequently, it becomes difficult compromise

C. Security requirements in VANETs

VANET technology used wireless communication which is vulnerable for any type of attack that is possible for any ad hoc network. Since humans are involved with vehicles, some security measures have to taken. Important information like presidential convoy, ATM cash van, etc., can be some critical information that has kept hidden from the common public. For any security to be applied it should satisfy the following requirements [2] [3][4].

- **Authentication:** This ensures that both the sender and the receiver nodes are authentic and genuine. The security algorithm should take care of authenticity for the sender and receiver.
- **Accessibility:** This ensures that the sender and receiver can read or modify the data. Any other node that acts as an intermediate is to be permitted to only read the message and not modify. If any attack takes place, the system must either detect and remove such message or simply terminate the connection between the nodes.
- **Message verification:** The system should be capable to handle malicious messages that are received by the nodes. The system must be able to detect and kill such messages.
- **Privacy:** Privacy must be maintained between the authenticated used and should be avoided from unauthorized users.
- **Emergency message:** If any vehicles have meet with accidents, then that information has to be broadcasted to other vehicles that are coming towards the accident zone or which are in the same path.

Retrieval Number: F8874038620/2020©BEIESP
DOI:10.35940/ijrte.F8874.038620
Journal Website: www.ijrte.org

Published By:
Blue Eyes Intelligence Engineering
& Sciences Publication

- **Reliability:** This is one of the major concerns. Here the system has to ensure that the message must be delivered to the intended receiver within the required time and via a trustworthy transmission.
- **Scalability:** Since vehicles travel at various speeds, but places like tool plaza, lot of vehicles get accumulated during peak hours. Hence the system must be capable to increase or decrease the nodes rapidly, but also take care that it should not degrade the overall performance of network.

D. P2P combined with VANET

Communication between V2V or between V2I can be one to one communication; hence we can also use Peer-to-Peer (P2P) communication in VANET.

P2P communication is one of the simplest ways of communication in any MANET. The properties of P2P are very suitable for VANET. Further integration of P2P and VANETs, as the properties of P2P network provides better features and connectivity to the physical structure of VANET which best suitable to VANET like dynamic network [6]. The similarity factor between P2P and VANET is that, both are self organizing, self sustainable to failures and also work in a distributed network. Further like P2P nodes, VANET nodes are also independent, decentralized and very high mobile in nature. A P2P2 based VANET scenario is shown in Fig. 2.

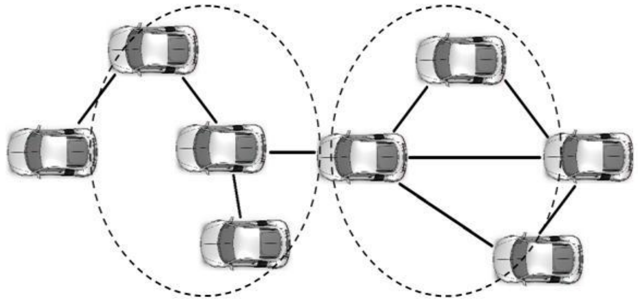


Fig.2: P2P implementation on VANET

The highlighting feature is that in P2P network large files can be sent effectively and efficiently, hence in similar concern, large files like multimedia files, audio files, images or pictures or even a huge text files. As the features between VANET and P2P are same, the issues are also common between them, like frequently changing topology, vehicles are continuously travelling and hence they always come in range and go out of range continuously due to various reasons [7]. The attributes of P2P are very suitable to VANET and its related applications like fuel payment, toll payment, video-on-demand, Internet surfing, live streaming, etc... All these applications can be easy implemented and provide a powerful platform for VANET.

III. ECC SECURITY FOR VANETS

Hence we need some type of security, and the best and easy possible method is to use cryptographic algorithm, for hiding the messages that are transmitted. As Public Key Cryptography (PKC) consume high resources like power and computation power, hence it was believed that PKC is not researchers believe that PKC is impractical for WSN, as WSN's have high limitation in terms of resources and battery power. As the advancement in the PKC took place, PKC gained its popularity, and PKC was used in technologies like MANET and VANET [5][8].

Elliptical Curve Cryptography (ECC) was proposed by Neal Koblitz and Victor Miller in 1985. ECC functionality is very much similar to that of RSA. Both algorithms use public-key mechanism, use prime number technique for generation of keys, etc... ECC is an asymmetric cryptographic algorithm [9][10], as shown in Fig. 3. The working of ECC uses the point formation by the line passing through the curve. There are various methods how to use the points on the curve, like points addition, point multiplication, etc… Message encoding is possible using the combination of points on curve that have been randomly selected which are formed on the cure. These provide a powerful security for message delivery [9][10].

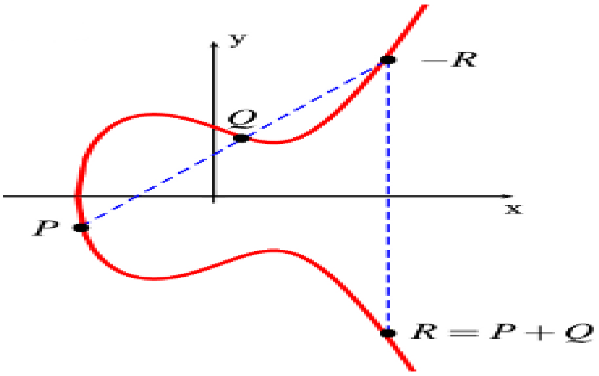


Fig.3: Sample of ECC curve [10]

As ECC is more robust in terms of security, ECC has gained popularity for securing data in various fields. Compared with traditional algorithms like RSA, ECC performs better in terms of smaller key. The key size of ECC is smaller than RSA, but provides equivalent level of security. Thus ECC has become an eye-catching alternative cryptosystem for many algorithms in various domains. Due to the popularity, many ideas have been proposed about the usage of ECC in various fields.

As shown in Table 1, ECC has smaller key size than RSA, but ECC has advantage both in terms of performance and strength. Though ECC has smaller key size, it provides the same security level as of RSA. Table 1 also shows the various key sizes comparison between traditional RSA and ECC [11] provided by NIST to US federal government for use in their defence sector.

Table- I: NIST recommended field size to US federal government [11].

Symmetric Cipher Key Length	RSA (n bits)	ECC	
		Fp (p bits)	*F2m (m bits)*
80	1024	160	163
96	1536	192	193
112	2048	224	233
128	3072	256	283
192	7680	384	409
256	15360	521	571

Further, Table 1 also demonstrates that ECC is feasible for WSN. ECC is a PKC algorithm; it will be the best choice, because of its better security, smaller key size and fast computation. For example, as seen in Table 1, we can see that the security level of 1024-bit RSA offer the same degree of security with 160-bit ECC.

A. Comparison between RSA and ECC

Key generation of any algorithm is one of the major criteria for comparison. Here we compare the key generation between the traditional RSA and ECC.

Both the algorithms work on the principle of PKC. Both the algorithms are similar in performance; by differ in key sizes [12]. As we can see in Table 2, ECC outperforms RSA in terms of Key generation and at all key lengths. The feature of ECC is that no resources are allocated for the generation of prime number, which is used for Key generation. The public key and private keys are generated by ECC at faster rate than the RSA. Key generation time in ECC are at linear rate, while the key generation time in RSA increases exponentially, the difference can be seen in Table 2 [12][13][14].

Table- II: Key generation performance of RSA and ECC [13][14].

Key Length		Time in seconds	
RSA	***ECC***	***RSA***	***ECC***
1024	163	0.16	0.08
2240	233	7.47	0.18
3072	283	9.80	0.27
7680	409	133.90	0.64
15360	571	679.06	1.44

Table 3 shows the time spent in cracking the key of both ECC and RSA. We can also see the number or computation required for breaking the key and the memory space required to break that key. Here also we can see that with smaller key size, ECC security level is equivalent to larger key compared to ECC. Table 3 also shows the various key sizes compared to RSA to break or decode the data by an attacker [13][14].

Table- III: The time spent on cracking all size Keys [13][14].

ECC Key (bit)	RSA Key (bit)	Time	Number of computation/key	Memory
112	430	<5 min	105	Very small
160	760	50years	4300	4 GB
192	1020	3 million years	114	170 GB
256	1620	1016 years	0.16	120TB

B. Elliptic Curve Diffie-Hellman (ECDH) Key Exchange

ECC has better performance and security, but only ECC cannot provide better security alone. When combined with some other algorithm, the combination provides extremely better security. Generally ECC can be combined with some other algorithms like, ECAES, ECDSA and ECDH. We intended to use ECC with Diffie Hellman Algorithm for key distribution in VANET between two nodes. Elliptic Curve Diffie Hellman (ECDH) is a variant of the Diffie-Hellman algorithm using elliptic curves [15][16]. ECDH in an encryption algorithm, but more than this it is basically a key-agreement protocol algorithm. Thus ECDH is also used for key distribution between two or more parties. ECDH generates a pair of keys for each node, and using the shared secret another key may be generated or the shared key only be used as the key. Thus the new key or the shared key is used to encrypt or decrypt the data and transmitted between parties [17]. Further ECDH is also very useful for providing can be used to provide group key management in a cluster or group of nodes. In securing the communication between a cluster or group of nodes, group key management plays an important role in VANETs. Thus to protect the network from the unauthorized or any attacked, ECDH cryptographic techniques is used [17][18].

As said above, ECDH can also be used to provide a secure environment for the drivers and the passengers, and also provide an authentication system during travel on the roads. This scheme provides the following features for VANET: 1) Reliability of VANET model 2) Privacy of the vehicles 3) Authentication of message delivery to adjacent nodes. Further the proposed scheme also ensures the privacy concern of every node in the network, and also detect legitimate or malicious node vehicle [19].

IV. Wireless Modules

A. HC-12 Wireless Serial Port Communication Module

HC-12 module is a wireless serial port communication module, which consists of new-generation multichannel embedded wireless data transmission technique. HC-12 works with the frequency band between 433.4-473.0MHz, and by stepping 400 KHz multiple channels can be set. Further HC-12 consists of totally 100 channels. HC-12 transmission power is 100mW and receiving power is -117 dBm, with 5,000 bps as the baud rate in air and distance of communication is 1,000m in line of sight. HC12 is as shown in Fig. 4.

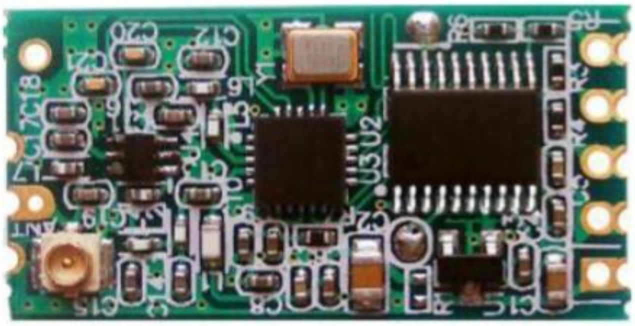


Fig.4: HC-12 Wireless Serial Port Communication Module

There are three serial ports for transparent transmission known as FU1, FU2 and FU3 modes. The responsibility of all the serial ports is to receive and send data rather than just using wireless transmission.

Among the three ports, FU3 is default working mode at full-speed mode, and according to the modes, the baud rate in air is automatically adjusted. The baud rate will be low if the communication distance is farthest. The only issue is that the modes cannot communicate with each other as they work at different baud rate. According to the application requirement, the user can select the suitable and optimal modes according to practical conditions [20].

As the communication is half duplex, usually a pair of modes is used, i.e. one mode at a time.

Meanwhile, the transparent transmission mode is set same as the serial port baud rate and two paired modules wireless communication channel. The default setting is FU3 at 9,600 bps and 433.4MHz [20].

B. Zigbee

There were some wireless applications where low-cost and low-power consuming devices were required. To address the need of such module, an open global standard wireless technology called Zigbee was developed which is of low-cost and low-power wireless IoT module. Zigbee standard operates at IEEE 802.15.4 wireless physical radio specification and operates at bands including 2.4 GHz, 900 MHz and 868 MHz. Zigbee is suitable for high-level communication protocols which can be used to create personal area networks , such as for home or office automation, medical health care, and other low-power low-bandwidth needs, like agriculture designed for limited area and to collect limited data. A simple Zigbee is shown in the Fig. 5 [21].

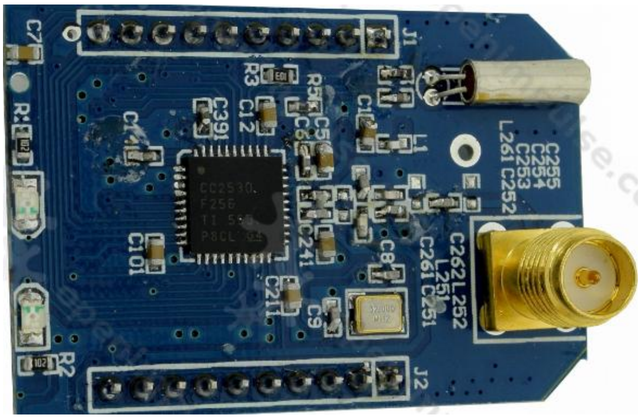


Fig.5: A simple Zigbee Module

Zigbee is similar to Wireless Personal Area Networks (WPAN's), but it is intended to be simpler and less expensive WPANs. One of the simplest applications of Zigbee is Bluetooth or Wi-Fi, which is general wireless networking application. Other applications are such as home energy monitors, traffic monitoring and control systems, industrial management system, etc… All the applications require short-range and low-rate wireless data transfer [22].

The main advantage of Zigbee is that it consumes low power and the range of communication is better than WiFI and Bluetooth. But one of the drawbacks is that its data transmission distance is restricted to 10–100 meters in the line-of-sight, depending on environmental condition. In case for applications where data is to be transmitted over long distance, then a mesh network of Zigbee can be created, where the network consists of more than one Zigbee devices and other intermediate devices. In most application, the Zigbee nodes are situated at places where maintenance is difficult, and hence such nodes must have secure networking transmission and long battery life [22].

C. DASH 7

DASH7 is a new generation wireless communication protocol that operates in globally available used for active RFID. DASH7 is an ultra-low power, low data-rate, long range, and low latency WSN technology [23]. DASH7 operates at three frequencies, i.e. at 433 MHz, 868 MHz and 915 MHz unlicensed ISM band/SRD band. The most stunning features of DASH7 is that has multi-year battery life, transmission range is up to 2 km, has low latency for connection with moving nodes, security that used AES 128-bit shared key encryption support, and finally a data transmission up to 167 kbit/s [23].

DASH7 is reliable and an open source protocol, that uses limited battery or a coin like power storage or thin battery with no requirement of using external power supply, but have a limited life span. On the other hand, RFID requires continuous external power supply and also the overall lifetime is about 10 years, which also depends on the type of application and its power consumption. The main advantage of DASH7 is that it operates at low frequency, which enables it for communication in the range of 1000-10000 meters outdoor with the data rate between 28 kbps and 200 kbps. DASH7 range is 6 times bigger than Zigbee of frequency of 2.4 GHz and 2 times bigger than 960 MHz based wireless communication modules/protocols, also 10-100 times better in indoor communication [24].

D. Performance Analysis of HC12 vs other

We can see the comparison between HC12, Zigbee and DASH 7 in Table 4 for End-to-End delay for various numbers of nodes [25]. From the comparison, we can see that HC12 performs better than Zigbee, DASH-7, when the number of node gets increased.

Table- IV: End-to-End delay verses Number of nodes [25].

Nodes	HC12	Zigbee	DASH 7
20	1.65	2.22	1.68
30	1.35	2.2	1.6
40	1.3	1.12	1.5
50	1.25	1.9	1.45
60	1.28	1.84	1.36
70	1.15	1.7	1.52
80	1.25	1.75	1.35
90	1.2	1.6	1.3
100	1.1	1.62	1.17

Similarly, Table 5 shows the Lifetime of each module for various numbers of nodes. The lifetime of HC12 is better than Zigbee and DASH-7, even the number of nodes increases.

Table- V: Lifetime verses number of nodes [25].

Nodes	HC12	Zigbee	DASH 7
20	34.28	32.60	33.46
30	34.33	32.56	33.52
40	34.38	32.7	33.4
50	34.26	32.8	33.34
60	34.32	32.7	33.68
70	34.34	32.3	33.72
80	34.36	32.3	33.38
90	34.39	32.8	33.23
100	34.66	32.69	33.46

V. PROPOSED SCHEME

A. Proposed Topology

We have used a P2P communication topology between the nodes, as shown in the Fig. 6 below, where we assume that each node communicates with other in a P2P mode. The nodes transmit various data to within each other, where the data are like encryption/decryption keys and actual data. As we depict a VANET scenario, the data exchange may occur at a very high rate, since the vehicles which are communicating may not be at the same speed.

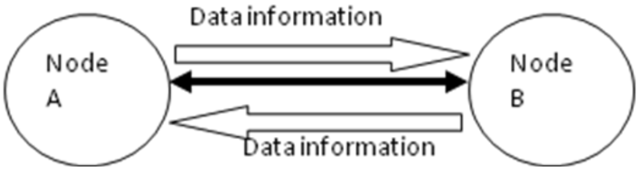


Fig.6: Proposed Scheme P2P VANET topology.

B. Implementation

Our goal is to come up with a simple method that can be used for communication between the vehicles and the VANET infrastructure. We have designed a portable yet an efficient way for communication using the long Range (LoRa) communication module. We intend to use HC12 (LoRa) for wireless communications in VANET's. Our aim is to transfer data between the two nodes that are using HC12 for communication. We cannot attach HC12 directly to a laptop, so we have used TTL-USB converter that is used to convert the parallel data obtained from the laptop and send it to the HC12 for wireless communication, as shown in the Fig. 7.

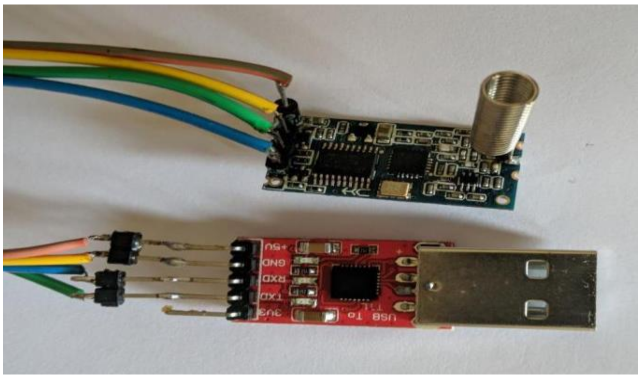


Fig.7: HC21 and TTL-USB converter connected together.

A TTL-USB converter is as shown in Fig. 8. A USB adapter is a type of protocol converter which is used for converting USB data signals to and from other communications standards. Generally to convert USB data to standard serial port data and vice versa. USB adaptors are used.

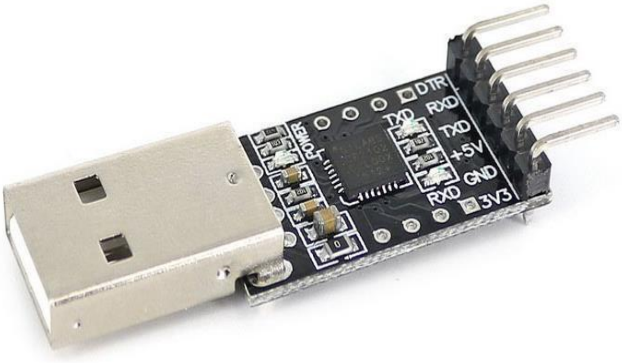
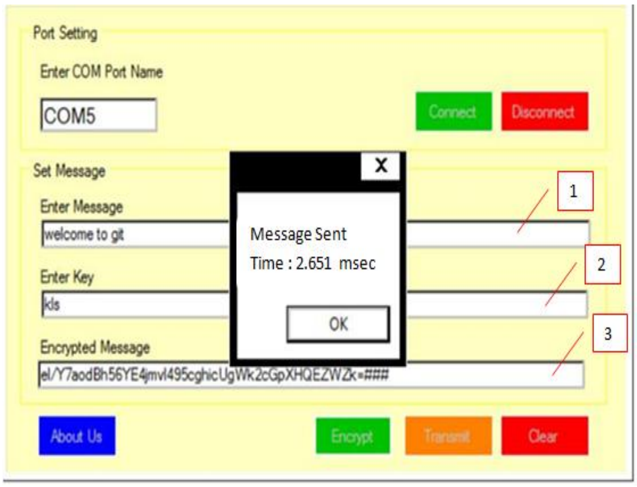


Fig.8: TTL-USB Convetor

A user interface has been built through which the user can send and receive the data. We have used ECDH for encryption at the sender and at the receiver side decryption of data takes place. Basically for communication, we assume that the key distribution has taken place and both, the sender and the intended receiver know the encryption and decryption keys. So when the sender wishes to send data to some receiver, the sender enters the message in the first box. Then the sender inserts that particular agreed Encryption key, to that intended receiver, in the second box. Then the sender clicks on the "Encrypt" button, which uses the specified key for encryption of the message, and the encrypted message is displayed in the third box. The Message box (1), Key box (2) and the Encrypted Message box (3) are Sender Side interface as shown in Fig. 9.



Port Setting

Enter COM Port Name: COM5

Set Message

Enter Message: welcome to git

Enter Key: kls

Encrypted Message: el/Y7aodBh56YE4jmvl495cghicUgWk2cGpXHQEZWZk=###

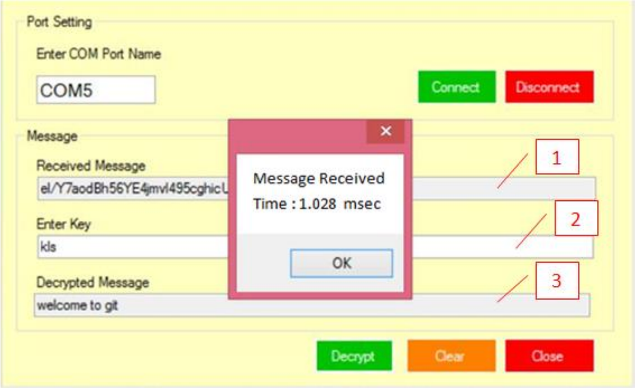
Message Sent

Time : 2.651 msec

Fig.9: Sender Side User Interface

Once the sender clicks the "Transmit" button, the message is encrypted and the message sent to the receiver.

Once the message is sent, we get a popup window, indicating that the message is sent and the time required for encryption and transmitting the message from the sender to receiver. All the receivers who do not have access to decryption key cannot decrypt the cipher text. Thus security is maintained by providing access only to the desired persons.



Port Setting

Enter COM Port Name: COM5

Message

Received Message: el/Y7aodBh56YE4jmvl495cghicL

Enter Key: kls

Decrypted Message: welcome to git

Message Received
Time :1.028 msec

Fig.10: Receiver Side User Interface

Similar the sender side, the receiver side also has a user interface. As shown in Fig. 10. The receiver side also has three boxes as specified. The (1) box is the encrypted message that is receives from the sender. The (2) box is the Decryption key, where the receiver inserts the decryption key, and the (3) box displays the original message, as shown in Fig. 10. Once the receiver enters the Decryption key, the receiver have to click on the "Decrypt" button, then if the key is correct, the original message is displayed in the third box. At the same time, a popup window is displayed, indicating that the original message is received, the also shows the time to decrypt the cipher text to plane text.

In both the user interface, there are two more buttons, "Clear" which is used to clear all the fields in the user interface and the "Close" button used to close the user interface. The closing of interface also indicates that the data communication between the sender and receiver is terminated.

C. Results

Table 6 shows the time requires to encrypt and send the cipher text from the sender side. Similarly, the decryption time is also taken for various files. We have taken a sample of 15 files, with varying file sizes from 54 Kb to 603Kb.

Table- VI: Proposed scheme results.

Sl. No.	File Size in Kb	ECDH (Time in milliseconds)	
		Encryption time	*Decryption time*
1	54	2.343	0.863
2	102	3.579	0.934
3	108	3.316	1.039
4	136	3.651	1.028
5	161	4.817	1.048
6	203	4.996	1.054
7	264	5.447	1.062
8	303	6.012	1.070
9	351	6.978	1.074
10	401	7.087	1.075
11	442	8.103	1.085
12	476	9.025	1.094
13	500	9.396	1.089
14	561	10.012	2.099
15	603	10.745	2.102

A seen from the Fig. 11, in the graph we can see that encryption time is increases gradually. But we should also keep in mind that encryption time also includes time to send the file also.

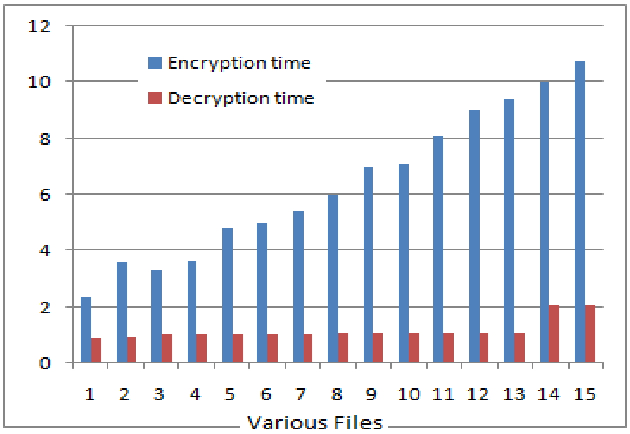


Fig.11: Encruption and transmission time vs Decryption time

On the other hand, the decryption takes considerably less time. Indeed the decryption time is less than 2.2 milliseconds where the decryption time is only after the message has been received, at the receiver side. The average time for encryption for 15 files is 6.367 milliseconds; similarly the average time for decrypting the same 15 files is 1.181 milliseconds.

Further we have also compared our results with the results obtained with a cryptographic simulator called Cryptool Simulator. For comparison we have considered a traditional cryptographic algorithm, i.e. RSA and the same ECDH algorithm in the Cryptool simulator. First we compare the encryption time. Table 7 below shows the results we have obtained.

Table- VII: Comparison of Encryption time.

Sl. No.	File Size in Kb	Encryption time (in milliseconds)		
		RSA (Cryptool)	*ECDH (Cryptool)*	*Proposed Scheme HC12 & ECDH*
1	54	0.031	0.843	1.343
2	102	0.063	1.422	2.579
3	108	0.078	1.422	2.316
4	136	0.094	1.796	2.651
5	161	0.11	2.17	3.817
6	203	0.141	2.686	3.996

7	264	0.172	3.547	4.447
8	303	0.219	4.016	5.012
9	351	0.234	4.78	5.978
10	401	0.281	5.407	6.087
11	442	0.297	6.331	7.103
12	476	0.312	6.375	8.025
13	500	0.328	6.639	8.396
14	561	0.375	7.796	9.012
15	603	0.39	8.407	9.745

As we can see from the Table 7 and the graph as shown in Fig. 12, we can see that the encryption of ECDH in the Cryptool is similar with our results obtained in a real world scenario. We have to also keep in mind that our results obtained also include the transmission time, whereas the Cryptool is a simulator and tested on a standalone system.

Similarly we also have compared our decryption results with the Cryptool results. Table 8 depicts the decryption time.

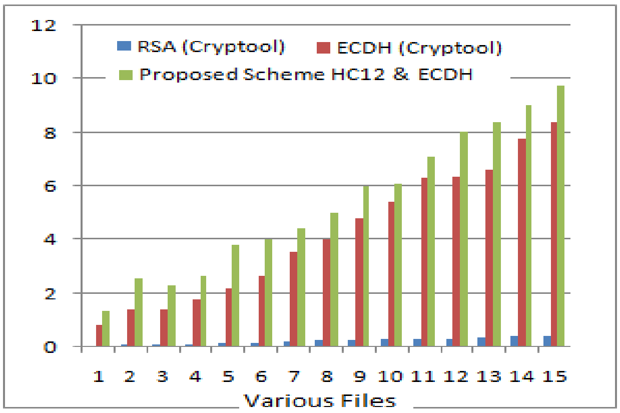


Fig.12: Comparision of Encryption time

Table- VIII: Comparison of Decryption time.

Sl. No.	**File Size in Kb**	**Decryption time (in milliseconds)**		
		RSA (Cryptool)	***ECDH (Cryptool)***	***Proposed Scheme HC12 & ECDH***
1	54	0.486	0.014	0.863
2	102	0.891	0.031	0.934
3	108	0.952	0.031	1.039
4	136	1.188	0.016	1.028
5	161	1.406	0.031	1.048
6	203	1.766	0.032	1.054
7	264	2.327	0.047	1.062
8	303	2.656	0.046	1.07
9	351	3.079	0.046	1.074
10	401	3.531	0.047	1.075
11	442	3.859	0.079	1.085
12	476	4.141	0.063	1.094
13	500	4.389	0.063	1.089
14	561	4.889	0.078	2.099
15	603	5.28	0.078	2.102

As we can see from the Table and the graph as shown in Fig. 13 below, we can clearly see that the decryption of our results are far less than the results of RSA in the Cryptool simulator.

VI. CONCLUSION

VANET is a promising field that is growing rapidly. But the concerns are the communication between other types of nodes and the major issue to be addressed is the security of data or information used in the communication of nodes. VANETs are open to various types of attacks, and should be handled cautiously in order to make VANET a safe network in the near future.

Our objective is to have a simple way of communication between the nodes itself and other types of nodes; hence we have used a P2P system into VANET for communication. The hardware used is a HC12 LoRa communication module. To solve the security issue, we have used ECDH algorithm for encryption and decrypting the data. We propose a framework that is capable to accomplish upper security and faster data communication, in a realistic scenario using P2P scenario. The results that have been obtained by our system, we have compared it with the results of two cryptographic algorithm obtained from the Cryptool simulator results. Thus we can say that using P2P and ECDH is very much suitable for VANET for a secure data transmission.

In the future, the system can be capable to transmit various types of files or messages like multimedia files, or an image file or even an audio file. The range of transmission can also be improved by using higher LoRa modules. We are also keen in improving the latency in data transmission of various files resulting in an efficient, faster and a secure data transmission.

REFERENCES

1. Rakhi, G.L.Pahuja,"Component Importance Measures based Risk and Reliability Analysis of Vehicular Ad Hoc Networks", International Journal of Computer Network and Information Security(IJCNIS), Vol.10, No.10, pp.38-45, 2018.DOI: 10.5815/ijcnis.2018.10.05.
2. Akash Vaibhav, Dilendra Shukla, Sanjoy Das, Subrata Sahana, Prashant Johri,"Security Challenges, Authentication, Application and Trust Models for Vehicular Ad Hoc Network- A Survey", International Journal of Wireless and Microwave Technologies(IJWMT), Vol.7, No.3, pp.36-48, 2017.DOI: 10.5815/ijwmt.2017.03.04.
3. Rajdeep Kaur, Tejinder Pal Singh and VinayakKhajuria, "Security Issues in Vehicular Ad-hoc Network(VANET)", Department of Computer Science and Engineering, Chandigarh University, Mohali, India. Proceedings of the 2nd International Conference on Trends in Electronics and Informatics (ICOEI 2018) IEEE Conference Record: # 42666; IEEE Xplore ISBN:978-1-5386-3570-4. 978-1-5386-3570-4/18/$31.00 ©2018 IEEE.
4. Amrish Kumar and Shri Niwashn Sir, "Implementation of VANET in Transportation using Wireless Sensors", Computer Science & Engineering Subharti Institute of Engineering & Technology, Meerut, India. International Journal of Scientific Research Engineering & Technology (IJSRET), ISSN 2278 – 0882, Volume 4, Issue 6, June 2015.
5. Saurabh Kumar Gaur, S.K.Tyagi and Pushpender Singh, "VANET System for Vehicular Security Applications", Saurabh Kumar Gaur, Asst. Professor, Dept Of CSE, Loard Krishna College Of Engineering Ghaziabad, U.P,India. International Journal of Soft Computing and Engineering (IJSCE). ISSN: 2231-2307, Volume-2, Issue-6, January 2013.

6. Sherali Zeadally, Ray Hun, Yuh-Shyan Chen, Angela Irwin and Aamir Hassan ―Vehicular ad hoc networks (VANETS): status, results, and challenges‖, Springer Science+Business Media, LLC 2010.
7. Aqeel Khalique, Kuldip Singh and Sandeep Sood, Implementation of Elliptic Curve Digital Signature Algorithm‖, International Journal of Computer Applications (0975 – 8887) Volume 2 – No.2, May 2010.
8. Song Ju, "A Lightweight Key Establishment in Wireless Sensor Network Based on Elliptic Curve Cryptography", School of Computer and Information Technology, Beijing Jiaotong University Beijing, China. 978-1-4673-1332-2/12/$31.00 ©2012 IEEE.
9. M. Brown, D. Hankerson, J.Lopez and A. Menezes, "Software Implementation of the NIST Elliptic Curves Over Prime Fields", Dept. of C&O, University of Waterloo, Canada, Dept. of Discrete and Statistical Sciences, Auburn University, USA, Dept. of Computer Science, University of Valle, Colombia and Certicom Research, Canada.
10. Swapnoneel Roy and Chanchal Khatwani, "Cryptanalysis and Improvement of ECC Based Authentication and Key Exchanging Protocols", School of Computing, University of North Florida, Jacksonville, FL 32224, USA; n01029842@ospreys.unf.edu. Cryptography 2017, 1, 9; doi:10.3390/cryptography1010009.
11. Sandeep S.V, Hameem Shanavas.I, Nallusamy.V and Brindha.M, "Hardware Implementation of Elliptic Curve Cryptography over Binary Field", . J. Computer Network and Information Security, 2012, 2, 1-7, Published Online March 2012 in MECS (http://www.mecs-press.org/), DOI: 10.5815/ijcnis.2012.02.01.
12. Rounak Sinha, Hemant Kumar Srivastava and Sumita Gupta, "Performance Based Comparison Study of RSA and Elliptic Curve Cryptography", Amity University, Noida, India. International Journal of Scientific & Engineering Research, Volume 4, Issue 5, May-2013 ISSN 2229-5518.
13. Swathi N S, Swathi P and Mr. Rajesh N V, "Efficient Performance Analysis of Elliptic Curve Cryptography over RSA to Secure the Data", BMS Institute of Technology & Management. International Journal of Computer & Mathematical Sciences IJCMS ISSN 2347 – 8527 Volume 7, Issue 4 April 2018.
14. A. Harsha and Basavaraj Patil, "A Review: Security of Data in Cloud Storage using ECC Algorithm", Bonfring International Journal of Software Engineering and Soft Computing, Vol. 6, Special Issue, October 2016. ISSN 2277-5099 | © 2016 Bonfring. DOI:10.9756/BIJSESC.8262
15. Christian Lederer, Roland Mader, Manuel Koschuch, Johann Grosschad, Alexander Szekely, and Stefan Tillich, "Energy-Efficient Implementation of ECDH Key Exchange for Wireless Sensor Networks", O. Markowitch et al. (Eds.): WISTP 2009, LNCS 5746, pp. 112–127, 2009. ©IFIP International Federation for Information Processing 2009.
16. N. Renugadevi and C. Mala, " Ternary Tree Based Group Key Agreement for Cognitive Radio MANETs", Department of CSE, National Institute of Technology, Tiruchirapalli, Tamilnadu, I.J. Computer Network and Information Security, 2014, 10, 24-31 Published Online September 2014 in MECS (http://www.mecs-press.org/) DOI: 10.5815/ijcnis.2014.10.03
17. Christian Haas, Joachim Wilke and Fabian Knittel, "Evaluating the Energy-Efficiency of the Rich Uncle Key Exchange Protocol in WSNs", Institute of Telematics, Karlsruhe Institute of Technology, Karlsruhe, Germany. 38th Annual IEEE Conference on Local Computer Networks. 978-1-4799-0537-9/13/$31.00 ©2013 IEEE
18. Jingwei Liu and Kyung Sup Kwak, "Hybrid Security Mechanisms for Wireless Body Area Networks", The State Key Lab of ISN Xidian University, Xi'an 710071, China. UWB Wireless Communications Research Center, Inha University, Incheon, Korea 402-751. 978-1-4244-8086-9/10/$26.00 ©2010 IEEE
19. Najmus Saqib, "Key Exchange Protocol for WSN Resilient against Man in the Middle Attack", Rajasthan Technical University, Kota, Rajasthan. 2016 IEEE International Conference on Advances in Computer Applications (ICACA), 978-1-5090-3770-4/16/$31.00©2016 IEEE.
20. Robert Rozee, "HC-12 Wireless Serial Port Communication Module", User Manual version 2.3B, Edited on 15 January 2016, 2016/01 version 2.3B Translated v2.3 online and merged with v1.1 by RR
21. Syed Rameem Zahra and Mir Shahnawaz Ahmad, "PPLS: Personnel Presence Locator System – An Amalgam of RF Ranging & Zigbee in WSN", Shri Mata Vaishno Devi University, J&K, India and Maulana Azad National Urdu University – ASCW, Budgam, J&K, India. I.J. Wireless and Microwave Technologies, 2018, 4, 78-95 Published Online July 2018 in MECS(http://www.mecs-press.net) DOI: 10.5815/ijwmt.2018.04.06
22. Himadrinath Saha, Shashwata Mandal, Shinjan Mitra, Soham Banerjee and Urmi Saha, "Comparative Performance Analysis between nRF24L01+ and XBEE ZB Module Based Wireless Ad-hoc Networks", Department of Computer Science & Engineering, Institute of Engineering & Management, Kolkata, India. I. J. Computer Network and Information Security, 2017, 7, 36-44 Published Online July 2017 in MECS (http://www.mecs-press.org/) DOI: 10.5815/ijcnis.2017.07.05
23. D. D. Piromalis, K. G. Arvanitis and N. Sigrimis, "DASH7 Mode 2: A Promising Perspective for Wireless Agriculture", Technological Educational Institute of Piraeus, Department of Automation, P. Ralli & 250 Thivon Str., Egaleo, Greece and Agricultural University of Athens, Department of Natural Resources Management and Agricultural Engineering, Athens, Greece. 4th IFAC Conference on Modelling and Control in Agriculture, Horticulture and Post Harvest Industry August 27-30, 2013. Espoo, Finland. 10.3182/20130828-2-SF-3019.00028.
24. Oktay Cetinkaya and Ozgur B. Akan, "A DASH7-based Power Metering System", Next-generation and Wireless Communications Laboratory, Department of Electrical and Electronics Engineering, Koc University, Istanbul, Turkey. 2015 12th Annual IEEE Consumer Communications and Networking Conference (CCNC). 978-1-4799-6390-4/15/$31.00 ©2015 IEEE.
25. J. Jegan, S. Shangeetha and A. Abihael, " An Event Reporting and Monitoring in Underground Coal Mine Environment using Wireless Sensor Networks", Department of CSE, Kings College of Engineering, Thanjavur. International Journal of Engineering Research & Technology (IJERT), ISSN: 2278-0181, NCICCT - 2018 Conference Proceedings.

AUTHORS PROFILE

Ravi U. Kalkundri completed his Bachelor of Engineering in Computer Science and Engineering and completed in 2009 from Gogte Institute of Technology, Belgaum. He worked in industries at different positions like Software Engineer and Senior Software Engineer. In 2011, he went on to peruse Masters in Technology in Computer Science and Engineering, from Gogte Institute of Technology, Belgaum. Currently he is working as Assistant Professor at Gogte Institute of Technology in the Department of Computer Science and Engineering, and perusing his PhD in the field of Network Security. His research interests are in the area of Ad Hoc Networks specializing in the area of VANETS and Security.

Dr. Rajashri N. Khanai received her PhD in error correction coding and cryptography for wireless networks from the Visvesvaraya Technological University, Belagavi, Karnataka, India. Her research interests include error control codes, cryptography, and machine learning applications to signal analysis. She is currently is Professor and Head of Department of Electronics and Communication Engineering, KLE's Dr. M. S. Sheshgiri College of Engineering and Technology, Belagavi, Karnataka, India. She has published over 20 academic papers. Dr. Rajashri is a member of IEEE.

Praveen U. Kalkundri completed his Bachelor of Engineering in Electronics and Communication Engineering and completed in 2009 from Gogte Institute of Technology, Belgaum. He worked in industries at different positions like Software Engineer and Senior Software Engineer. In 2011, he went on to peruse Masters in Technology in VLSI Design in Embedded Systems, from KLE Dr. M.S. Sheshgiri College of Engineering and Technology, Belgaum.

Currently he is working as Assistant Professor at Gogte Institute of Technology in the Department of Electronics and Communication Engineering, and currently perusing his PhD in the field of VLSI Design. Assistant Professor Praveen is a Life Member of Indian Society for Technical Education.