International Journal of Science and Research (IJSR)
ISSN (Online): 2319-7064
Index Copernicus Value (2013): 6.14 | Impact Factor (2014): 5.611

Light-Weight Energy Efficient Encryption Scheme for Vehicular Ad Hoc Network

Pooja Mundhe[1], V. S. Khandekar[2]

[1]Department of Information Technology, Sinhgad Technical Education Society's SKNCOE, Pune, India

[2]Professor, Department of Information Technology, Sinhgad Technical Education Society's SKNCOE, Pune, India

Abstract: ***Vehicular Ad Hoc Networks are a one form of wireless networks in which Road Side Units (RSU) and vehicles are the communicating nodes, providing each other with information such as traffic information and safety warning. They are self-distributed and organized. They can be useful in avoiding accidents and traffic congestion. Providing safety and comfort applications such as information about road block, fuel station, and traffic are main purposes of the VANET. VANET's are highly dynamic and energy constraint in nature, Due to this nature of VANET it is more challenging to achieve the security. Security and energy consumption are important issues in VANET. Previously data confidentiality can be achieved by AES algorithm in VANET's. But AES requires more energy for the process of encryption and decryption. This paper introduces A Light-Weight Energy Efficient Encryption Scheme for achieving security in energy efficient way. Transmission of data is not the only source of energy consumption there are many much like encryption and decryption. Light-Weight Energy Efficient Encryption scheme saves the energy in the process of encryption/decryption of data.***

Keywords: Light-Weight Energy Efficient Encryption, Security, Vehicular Ad Hoc Network.

1. Introduction

Vehicular Ad Hoc Networks are formed by Vehicles in the particular range to communicate Safety information. There are two types of VANET's such as Vehicle to Vehicle (V2V) and Vehicle to Infrastructure (V2I). Vehicle to Vehicle (V2V) is a variation of MANET's (MANET) with the emphasis now the node is a vehicle. On the other hand, Vehicle to Infrastructure Communication takes place in between vehicle and Road side infrastructure for sharing safety-related data [2]. Safety and comfort application provided by VANET's are lane changing, traffic sign violation, weather information, road condition, a location of restaurants or fuel station, parking and interactive communication such as internet access [3]. According to World Health Organizations (WHO), annually approximately 1.2 million deaths are caused by road accidents; one-fourth of that caused by injury. Also, around 50 million persons get injured in accidents [4]. A lot of accidents take place in foggy conditions because drivers couldn't detect that some incident has occurred in front of them. Safety could be enhanced with the help of VANET since it enables drivers to get information about such incidents from RSU.

The Vehicular Communication (VC) system has recently attracted computer engineering and computer science researchers due to a wide range of applications ranging from wireless networking to automotive industries. In VANET most new vehicles will be outfitted with short-range radios capable of communicating with road side infrastructure or other vehicles at a distance of at least one kilometer [6]. With the help of this short range radios equipped with both road side infrastructure and vehicles, a driver can inform another vehicle about a sudden deceleration of its speed. Sharing location information could reduce blind spot and support drivers during route changes; this could prevent drivers from accidents. Lane changes or route changes were responsible for over 630,000 crashes in the United States alone [5]. In 1999, the U. S. Federal Communications Commission (FCC) allocated a block of spectrum in the 5.85 to 5.92 GHz band for function mainly projected to improve the security of highway system [8].

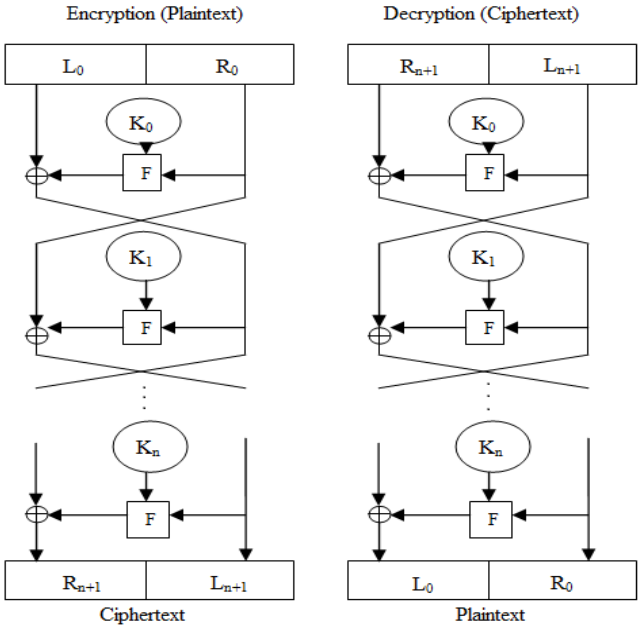

Figure 1: Feistel Cipher [1].

Above figure 1 shows the structure of Feistel Cipher. The LEE is based on Feistel cipher which is a symmetric structure used for the construction of block ciphers. The Feistel cipher structure has the benefit that encryption and encryption operations are very parallel, requires simply reversal of key schedule. In this paper, a new encryption strategy is designed which provide security in energy efficient manner. Light-weight Energy Efficient Encryption (LEE) can be used in devices which are battery operated for the communications.

This encryption algorithm does not contain operations like S-Boxes or any complex operators. This algorithm is implemented in Java. There are different types of attacks and threats possible on VANET [8] such as Denial of Service, fabrication attack, alteration attack, message suppression attack and reply attack described here.

2. RELATED WORK

Public key cryptography has been considered unsuitable for wireless networks since its pricey computational operations [7]. In this paper, asymmetric key encryption is used for providing security. These public keys should be signed and issued by trusted authority. For this purpose of issuing certificates by trusted authority author uses PKI (Public Key Infrastructure).

In [15] paper, Author proposes encryption scheme which requires less energy as compare to other encryption scheme. P-Coding uses the permutation encryption which performs encryption on coded message. Haphazardly permuting the symbols of the message makes eavesdropper unable to get original text.

In [8] paper, the author proposes location based routing that is able in delivering the contents of passenger's interest. In this scheme, RSU is used as a mediator for communication in between server and client (vehicle). When a source node wants to send data to destination first distance between source and destination is calculated, if a distance is less than the threshold, then the source can directly send data to a destination or it communicate through RSU.

Stream ciphers are faster than block cipher for that reason they can be used in resource constrained networks [9]. The RC5 encryption algorithm is considered as a potential solution for Wireless networks. RC5 requires less energy and memory that other encryption algorithm.

Random Linear Network Coding (RLNC) is a kind of network coding used in ad hoc network to securely transfer data and improve the throughput of the network [10]. In RLNC source generates some packets, buffers them until a generation is composed. Then Source forwards packet to the destination.

In [11] paper, the author proposes an efficient use of network coding for handling content distribution and improving the performance. In VANET, network coding can efficiently handle the node mobility and random errors. In VANET, content distribution is a challenge due to dynamics of network and high mobility. There are some resource constraints that have a light impact on encoding and storage operations performed by network coding.

In [12] paper, the author gives the brief study of energy consumption characteristic of different encryption algorithms. Encryption and decryption in symmetric cipher algorithm process through the sequence of mathematical computation. As compared to other symmetric key algorithm AES require minimum energy for the purpose of key setup and encryption/decryption.

Table 1: Literature Survey

Sr. no.	*Existing Method*	*Advantages*	*Disadvantages*
1.	PKI	1) Cluster heads are responsible for information dissemination. 2) Digital signature used before sending a message.	1) Due to use of cluster head it causes high security over head. 2) Network traffic increases with a use of cluster-head.
2.	P-Coding	1) Due to the use of permutation encryption, an eavesdropper cannot recover the original message. 2) Requires minimum energy as compare to other encryption scheme	1) Cannot work efficiently when a source wants to send a large volume of data. 2) Key management is challenging in the case of high node mobility.
3.	LB-VANET	1) Reduces energy consumption required for routing 2) Overcomes the issue of packet loss and delay.	1) Need to manage routing table. 2) Requires energy for managing routing table.
4.	RC5	1) Supports variable length keys, variable block size and also a variable number of rounds. 2) Algorithm is Based on the use of Random permutation.	1) Susceptible to differential cryptanalysis attack.
5.	RLNC	1) Improves throughput of the network	1) Requires energy and time 2) Delay in arriving packets
6.	RSA	1) Increased security and convenience. 2) Provide the digital signature that cannot be repudiated.	1) Slower than the secret key method. 2) Can be vulnerable to impersonation if hacked. 3) This method consumes more energy for the key generation, verification and signing operation.
7.	AES	1) AES is more secure as compare to 3DES. 2) AES is less susceptible to cryptanalysis. -AES is faster.	1) AES in counter mode is challenging to implement.
8.	Network coding	1) Network coding in VANET can efficiently handle mobility and increases throughput.	1) Performance issue if no. of generations is more. 2) Vulnerable to eavesdropping attack.

In existing papers, researchers use methods and schemes to provide security. But these schemes require a large amount of energy and, therefore, computation overhead occurs. Hence, here an energy efficient light-weight security scheme is proposed to solve these problems.

3. How Vehicular Networks Work

Vehicular network systems consist of a various number of vehicles; these vehicles will require a central authority to administrate it. Each vehicle of this network can communicate with other vehicles using short radio signals DSRC (5.9 GHz), for the range can reach 1 KM. This is an ad hoc communication that means each node is free to move, no fixed infrastructure required.

The routers used for communication called RSU (Road Side Unit), work as a router between vehicles on the highway and connected to other devices [13].

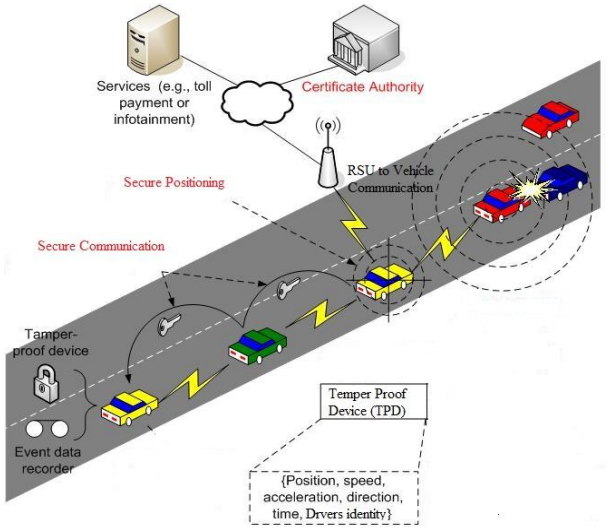

Figure 2: Structure of VANET [13].

Each vehicle has an OBU (On Board Unit), RSU is connected to the vehicle with this unit via DSRC radios. There is an another device called TPD (Temper Proof Device), which holds all the secret information about a vehicle like trip details, route, drivers identity, keys, the speed of vehicle….etc.

4. Attacks and threats

This paper focus on security of messages communicated between vehicles, providing privacy to drivers or passengers safety is not in the scope of this paper.

4.1 Denial of Service Attack

This attack happens when the attacker takes control of a vehicle's resources or jams the communication channel used by the Vehicular Network, so it prevents critical information from arriving.

4.2 Message Suppression Attack

An attacker selectively drops packets from the network, these packets may hold critical information for the receiver, the attacker suppresses these packets and can use them again in other time.

4.3 Fabrication Attack

An attacker can make this attack successful by transmitting false information into the network.

4.4 Alteration Attack

This attack happens when attacker alters an existing data. It includes delaying the transmission of the information, replaying earlier transmission, or altering the actual entry of the data transmitted.

5. Proposed Work

Due to the use of Light-weight energy efficient encryption, it is difficult to the adversary to recover the original packet. The lightweight encryption scheme used here requires less time for the process of encryption and decryption. The time is reduced therefore energy required for these processes greatly reduced [14]. The proposed architecture is based on the following parts.

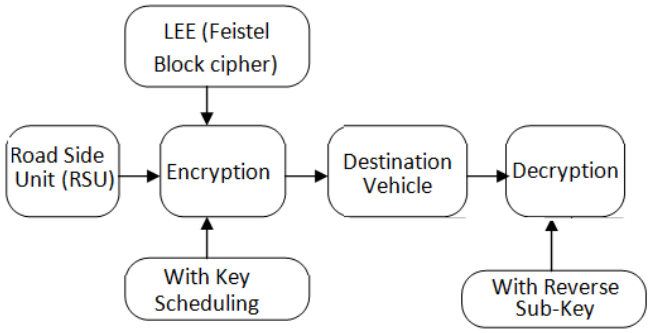

Figure 3: Architecture of Proposed System

The LEE algorithm is motivated by XTEA algorithm [14], LEE is a 64-bit block Feistel network which uses 128-bit key length and 32 rounds. The Feistel function is a symmetric structure used for the construction of Block cipher.

The Feistel structure has the advantage that encryption and decryption operation are very similar, requires only a reversal of the key schedule. Therefore, the size of code need to implement this cipher is just about halved.

LEE includes fixed length rotation, shift operation, XOR and addition modulo 2^{32}.

At the source node, Feistel cipher encrypts the data to transmit it more efficiently. Let the source node has a sequence of the message to send. Plaintext block is split into two half. After 32 rounds of processing, they are again combined to produce cipher text block. Therefore, the original input of algorithm (i.e. plaintext) is $P = L_0R_0$ and final cipher text is $C= L_{32} R_{32}$.

5.1 Road Side Unit (RSU)

Road-side Unit contains all information about vehicles in its range. RSU informs the vehicle about any emergency situation occurs in that range so that vehicle should change

their route for their safety. The message conveyed between RSU and Vehicle is encrypted with LEE.

5.2 Encryption

At the source node, Message is encrypted with the help of Light-weight Energy Efficient Encryption. In LEE, the plain text block is divided into two halves. Then each half is used for encrypting the other half plain text while 32 rounds of processing. Finally, both halves are combined to produce the required cipher text block.

5.3 Destination Vehicle/Node

On receiving the packet from road side unit, Destination node decrypts the packet to revels original message. The decryption process is similar to that of encryption process only with the difference, in decryption key should be reversed. Due to this process code need to implement is less as compared to other encryption algorithm. So it also requires less energy to implement.

Following steps are used for providing security and saving energy in VANET

- When a Source node has a message to communicate with the destination. The message is first encrypted with an encryption algorithm.
- Source encrypts the Message with Light-Weight Energy Efficient Encryption (LEE) a Feistel structure and key scheduling algorithm.
- In an encryption process the message is first divided into half and again combined to produce cipher text.
- The Key scheduling algorithm is used to produce 128-bit cipher key to encrypt plaintext.
- At the receiving node, original message is recovered using similar process used at encryption.
- In decryption process, cipher text is used as input to algorithm and key is used in reverse order.\

6. System Model

LEE is 64-bit block Feistel network with 32 rounds and 128-bit key.

Table 2: Notations Used in the Description of Lee

Symbol	*Description*
←	Shift To Left
→	Rotation to Right
⊕	XOR

The Feistel function is based on shift operation and XOR, fixed length rotation and additions modulo 2^{32}.

- Consider a VANET of R Road Side Stations and V Vehicles
  Where V= $\{v_1, v_2, \ldots, v_n\}$, and R=$\{r_1, r_2, \ldots, r_n\}$
- Assume a node v ϵ V joins the network and travelling from one station to another,
- When a source wants to send message to destination vehicle, it encrypts the message as follows:
- Size of the message is calculated in bytes for the further computation.
- The given plaintext is divided into the two halves L_0 (left-half) and R_0 (right-half).
- Therefore input of the algorithm is, P= L_0 and R_0 and the cipher text C=$L_{32}R_{32}$ .The relation between the output L_{i+1},R_{i+1} and input L_i,R_i for *i*th round of algorithm is as follows:
- To calculate time required to perform encryption and decryption define following:
- Let X be the start time defined before execution of algorithm.
- Let F be the round function and K_0, K_1 …. K_n be the number of keys for round 0, 1…..n Respectively.
- Following calculation is done for each round:
  $L_{i+1} = R_i$
  $R_{i+1} = L_i \oplus F(R_i, K_i)$
  Where K=K_0, K_1,….K_n keys for n rounds.
- Function F operates in following way:
  $R_i' = (R_i \leftarrow 4) \oplus (R_i \rightarrow 5)$
  R_i' can be calculated with performing XOR operation on Bitwise rotation to right of R_i and Bitwise shift to left of R_i.
- Then Round function can be calculated as follows:
  $F(R_i,K_i) = (R_i' + K_i)$
  Here, calculated R_i' and key K_i are added to get the round function.
- Decryption of the cipher text can be produced in the following way:
  $R_i = L_{i+1}$
  $L_i = R_{i+1} \oplus F(L_{i+1}, K_i)$
  Where, i = n, n-1 …0
- Finally, the plaintext (L_0, R_0) can be obtained.
- Let Y be the end time defined after the execution of algorithm.
- Let T_E as total time required to perform encryption operation, From 1 and
  $$T_E = (Y - X) / 1000$$
- Let T_D as total time required to perform decryption operation,
  $$T_D = (Y - X) / 1000$$
- Since execution time is known, energy consumption can be calculated by calculating energy used by CPU.
- Here total Energy Consumption T_E, for Process of encryption and decryption can be calculated as follows,
  $$T_E = [(T_E + T_D) * 65.74] / 1000$$

Here it is considered that, CPU requires 65.74 watts of energy for executing the algorithm. So it is divided by 1000 to convert it into the Joules.

7. Experiments

The performance of proposed algorithm is evaluated using the metrics such as energy consumption, encryption time, and decryption time. For performing implementation of LEE, first message i.e. plain text is divided into two halves. Then message is encrypted to get the cipher text. Experiment environment used here is a Windows 7 with 3.30GHz Core i3 CPU and 4GB Ram Memory.

8. Result and Discussion

8.1 Encryption Time

Here size of plaintext is calculated in terms of bytes. As shown in table 3, time required to encrypt the packet is calculated with the help of current time defined before execution of algorithm and end time of the system defined after execution of algorithm. The values of time are varying because the time required for encrypting any packet is not same, the time is changes according to the resources used by the algorithm for execution.

Table 3: Encryption Time

Packet Size (Bytes)	AES (Existing System) Time in (ms)	LEE (Proposed System) Time in (ms)
13	0.17	0.10
38	0.29	0.15
88	0.22	0.11
74	0.23	0.17
15	0.27	0.12

Following Figure 4 shows the comparison of time required to encrypt the packet using AES and time required to encrypt the packet using LEE. Here time is calculated on the basis of packet size. It can be seen that encryption time is increased with the increase in size of packet.

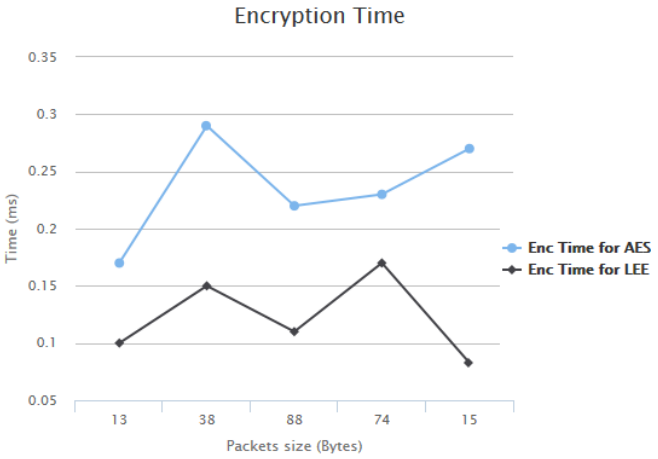

Figure 4: Encryption Time for AES Vs LEE

8.2 Decryption Time

Decryption time is also measured as same as encryption time. Decryption time is the time required to decrypt the given size of packet. Table 4 shows the comparisons of time required AES and LEE to decrypt the packets.

Table 4: Decryption Time

Packet Size (Bytes)	AES (Existing System) Time in (ms)	LEE (Proposed System) Time in (ms)
13	0.38	0.17
38	0.39	0.13
88	0.32	0.12
74	0.35	0.16
15	0.38	0.12

Following Figure 5 shows the comparison of time required to decrypt the packet by AES and LEE. Decryption time is calculated in terms of microseconds.

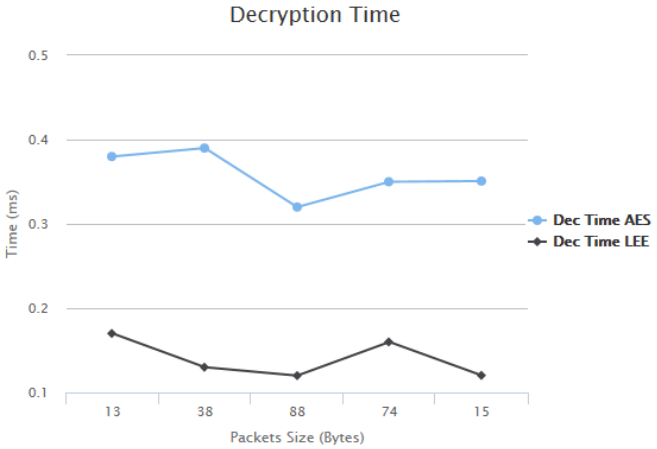

Figure 5: Decryption Time for AES Vs LEE

8.3 Energy Consumption

Less amounts of time means less energy required. Table 5 shows the energy consumption required for the process of encryption and decryption of message for Both AES and LEE algorithms. LEE requires less number of operations for the process of encryption and decryption as compare to AES therefore it requires less amount of energy.

Table 5: Energy Consumption

Packet Size (Bytes)	AES (Existing System) Energy in (µJ)	LEE (Proposed System) Time in (µJ)
13	0.036	0.017
38	0.044	0.0184
88	0.035	0.0151
74	0.038	0.0219
15	0.042	0.015

Figure 6 shows energy required to Encrypt and Decrypt the packet. As it can be seen in the figure LEE requires less energy as compare to AES.

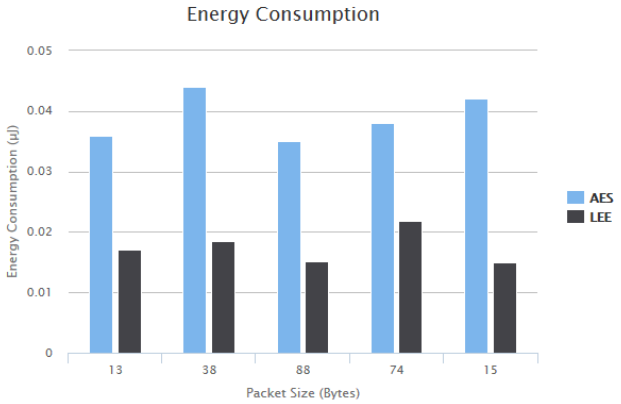

Figure 6: Energy Consumption

Here time required for the process of encryption and decryption is calculated and by adding that total time energy is measured.

9. Conclusion

In this work, a light-weight Energy Efficient encryption scheme is used for providing security in energy efficient way. In previous work, author shows that network coding can be used to reduce the energy consumption by fewer transmissions. Here LEE is used to provide improved security and reduce the energy consumption in VANET. Since this scheme uses reverse key to decrypt packets it provide strong security as compare to previous encryption algorithms. This scheme requires less energy for the process of encryption and decryption operation. Hence it can be conclude that LEE requires less time and Energy as compare to AES and it also provide better security.

10. Acknowledgment

I would like to thank my guide Prof. V. S. Khandekar for her feedback, constant encouragement and guidance throughout the duration of the paper. Her suggestions were of immense help throughout this paper.

References

[1] Peng Zhang, Chuang Lin, Yixin Jiang, Yanfei Fan, and Xuemin (Sherman) Shen "A Lightweight Encryption Scheme for Network-Coded Mobile Ad Hoc Networks," IEEE Trans. Parallel and Distributed Systems, Vol. 25, No. 9, September 2014.

[2] Reza Azimi, Gaurav Bhatia and Ragunathan (Raj) Rajkumar "Vehicular Networks for Collision Avoidance at Intersections" SAE International Journal 2011.

[3] A. Rahim, I. Ahmad, Z. S. Khan, M. Sher, M. Shoaib, A. Javed, R. Mahmood "A Comparative Study of Mobile And Vehicular Ad Hoc Networks," International Journal of Recent Trends in Engineering, Vol 2, No. 4, November 2009.

[4] M. Peden, Richard Scurfield, D. Sleet, D. Mohan, et al. "World report on road traffic injury prevention" (PDF). World Health Organization. Retrieved 2008-02-29.

[5] John Chovan, Louis Tijerina, Graham Alexander, and Donald Hendricks. Examination of lane change crashes and potential IVHS countermeasures. http://www.itsdocs.fhwa.dot.gov/JPODOCS/REPTS_TE/61B01!.PDF, March 1994.

[6] Ghassan Samara, Wafaa A.H. Al-Salihy, R. Sures, Penang "Security Issues and Challenges of Vehicular Ad Hoc Networks (VANET)" New Trends in Information Science and Service Science (NISS), 2010 4th International Conference on 11-13 May 2010.

[7] Maxim Raya and Jean-Pierre Hubaux "Securing vehicular ad hoc networks", Journal of Computer Security 15 (2007) 39–68.

[8] Prerana Deshmukh, Prof. Shrikant Sonekar "Improving Energy and Efficiency in Cluster Based VANETs through AODV Protocol" Prerana Deshmukh et al, / (IJCSIT) International Journal of Computer Science and Information Technologies, Vol. 5 (3) , 2014, 4788-4792.

[9] R. Venugopalan, P. Ganesan, P. Peddabachagari, A. Dean, F. Mueller, M. Sichitiu, "Encryption overhead in embedded systems and sensor network nodes: Modeling and analysis", International Conference on Compilers, Architectures and Synthesis for Embedded Systems, 2003.

[10] Tracey Ho, Muriel Médard, Ralf Koetter, David R. Karger, Michelle Effro, Jun Shi, and Ben Leong "A Random Linear Network Coding Approach to Multicast" IEEE Transactions onn Information Theory, Vol. 52, NO. 10, OCTOBER 2006.

[11] Maxim Raya and Jean-Pierre Hubaux "Securing vehicular ad hoc networks" Journal of Computer Security 15 (2007) IOS Press.

[12] N.R. Potlapally, S. Ravi,A.Raghunathan, andN.K. Jha, "A Study of the Energy Consumption Characteristics of Cryptographic Algorithms and Security Protocols, " IEEE Trans. Mobile Computing, vol. 5, no. 2, pp. 128-143, Feb. 2006.

[13] Wenshuang Liang, Zhuorong Li, Hongyang Zhang, Shenling Wang, and Rongfang Bie, "Vehicular Ad Hoc Networks: Architectures, Research Issues, Methodologies, Challenges, and Trends" Hindawi Publishing Corporation International Journal of Distributed Sensor Networks Article ID 745303.

[14] A. J. Menezes, S. A. Vanstone, and P. C. Van Oorschot, Handbook of applied Cryptograph.y, CRC Press, Inc., 2001.

[15] Yanfei Fan, Xuemin (Sherman) Shen, Peng Zhang, Yixin Jiang, Chuang Lin "P-Coding: Secure Network Coding against Eavesdropping Attacks" INFOCOM, Proceedings IEEE 14-19 March 2010.