Energy Efficient Encryption Scheme for Vehicular Ad Hoc Network

Pooja Mundhe
Dept. of Information Technology
Sinhgad Technical Education Society's SKNCOE,
Pune, India
E-mail: poooh.m99@gmail.com

Prof. V. S. Khandekar
Dept. of Information Technology
Sinhgad Technical Education Society's SKNCOE,
Pune, India
E-mail: varsha.khandekar@gmail.com

***Abstract*---Vehicular ad hoc networks are part of Mobile ad hoc network. They are self-distributed and organized. The main purpose of the VANET is to provide comfort and safety application such as information about fuel station, whether condition, parking, road block, and emergency warning, etc. Energy saving is an important issue in VANET. Energy consumption can be reduced with the help of the network coding with less transmissions. Transmission is not the only source of energy consumption there are many more like encryption and decryption. P-coding is a light-weight security mechanism, which saves the energy in the process of encryption/decryption of data. With the efficient permutation encryption, this method provides security against eavesdropping attack. The permutation encryption makes an attacker difficult to locate the coding vector.**

Keywords- Energy Saving, Light-Weight Encryption, Network Coding, Vehicular Ad Hoc Network.

I. INTRODUCTION

Vehicular ad hoc network is now becoming interesting research topic in the area of wireless communication. Vehicles in the particular range form a network to communicate with each other without the need for a base station. VANET provide comfort and safety applications such as lane changing, traffic sign violation, weather information, road condition, location of restaurants or fuel station, parking and interactive communication such as internet access [2]. For providing these services, energy is required. Thus, energy saving is an important issue in vehicular ad hoc network. There are several energy efficient schemes used to overcome this problem [3], [4] and [5].

Many researchers show that network coding can reduce energy consumption in VANET with less transmission [6]. Network coding can be defined as coding performed at a node in a network, where coding means casual mapping from inputs to outputs. Idea behind it is to mix and forward data to output links [7]. A node in the network encodes the packet with the network coding and then forwards it to another node. Network coding requires less energy for this process of encoding. Figure 1clarify the use of network coding in ad hoc network. Suppose there are six nodes forming hexagon and transmission range of each node reaches to its right and left neighbor. As shown in figure. 1(1) each message would require four transmissions without network coding. When network coding is used as shown in (figure. 1(2), 1(4), 1(4),) a total number of nine transmissions are needed for three messages, i.e., three transmissions per message. It would save ¼ energy without considering energy required for the process of encryption and decryption.

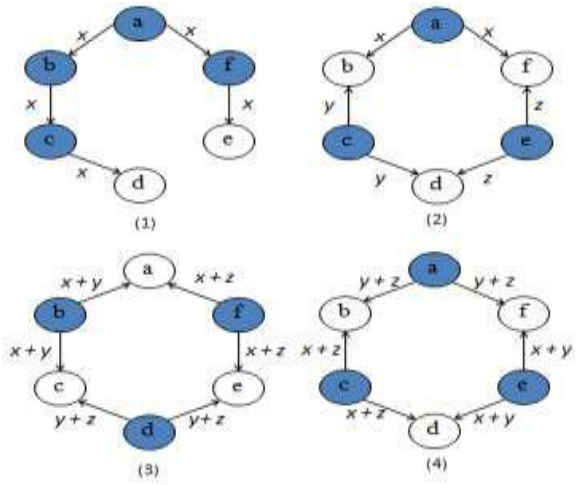

Figure 1: Use of network coding for transmission. Shaded nodes are those involved in transmission [1].

Encryption and decryption performed at each node for providing security also consumes more energy in VANET. For example, data communicated between vehicles in battlefield or a police van should keep confidential during transmission [8]. But the encryption schemes previously used for providing security not work efficiently.

In [9], a Motorola's "DragonBall" embedded microprocessor consume near about 13.9 µJ to send a bit. It consumes 7.9 µJ when symmetric-key encryption algorithm is used for encryption per bit. Intrinsic security is provided by network coding based on which encryption scheme can be designed. In [10], it proposes that coding vector can be encrypted by using Homomorphism Encryption function (HEF), due to which network coding can be performed directly on coding vectors. This scheme has too much computation or space overhead; therefore they are not suitable for VANET.

In this paper, a new encryption scheme is designed which provide security in energy efficient manner. P-coding randomly permutes both message content and coding vector due to which eavesdropper cannot locate coding vector without knowing permutation since cannot reveal useful information [1].

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.

The remaining of this paper is organized as follows. Section II describes the related work along with the literature review. Section III introduces proposed work along with the system architecture. Section IV concludes the paper.

II. RELATED WORK

A. *Rivest Shamir Adleman Algorithm (RSA)*

In [14] paper, author proposes Vehicular Public Key Infrastructure (VPKI) to monitor malicious activities in the network. Certificate authority is used to bind the public key with respective user identities. RSA public key algorithm is used for security and authentication. The work mainly focuses to provide security for location privacy preservation.

B. *Advance Encryption Standard Algorithm(AES)*

In [9] paper, 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.

C. *Secure Practical Network Coding(SPOC)*

In [7] paper, author proposes low-complexity cryptographic scheme that explore intrinsic security of network coding. Secure Practical Network Coding SPOC uses unlocked and locked coefficients that are added and concatenated to the packet header each time whenever a new packet is generated. These unlocked and locked coefficients are encrypted with keys and are used for encoding and decoding. Due to use of SPOC number of operations for encryption is greatly reduced.

D. *Homomorphism Encryption Function(HEF)*

In [15] paper, author focuses on reducing privacy threat in multi-hop wireless network. Homomorphism Encryption Function (HEF) performs linear random combination on incoming packets and gives resultant packets. HEF perform encryption on GEVs to keep it confidential.

E. *Authenticated Routing for Ad Hoc Network(ARAN)*

In [13] paper, author briefly discusses the ARAN protocol. This protocol uses public key cryptography and a certificate server and also prevents from spoofing attack. Author discusses the security challenges and issues in VANET and their solutions. ARAN is one of them solution that is based on the AODV protocol. It uses timestamp for the route freshness. This scheme requires all nodes must keep the routing table for all another node.

F. *Network Coding (NC)*

In [16] paper, author proposes efficient use of network coding for handling content distribution and enhancing the performance. In VANET, network coding can efficiently handle 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.

TABLE 1: LITERATURE SURVEY

Sr. no.	Existing Method	Advantages	Disadvantages
1.	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) Consumes more energy for the key generation, verification and signing operation.
2.	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.
3.	SPOC	1) Use locked and unlocked coefficient. 2) Achieve confidentiality	1) Incurs more computation overhead. 2) Do not provide privacy against flow tracing.
4.	HEF	1) Privacy against flow tracing and traffic analysis. 2) Homomorphism allows recoding	1) computation overhead 2) Incurs more energy consumption.
5.	ARAN	1) Prevent from spoofing 2) Provide message integrity, non-repudiation and authentication.	1) Each node maintains the routing table for each node. 2) Computation overhead and delay.
6.	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.
7.	VPKI	1) Prevents from DOS, replay attack, message suppression attack	1) Causes overhead due to group signature. 2) Network is not stable so cannot form a stable group.

G. *Vehicular public key infrastructure*

In [8] paper, author focuses on security issues and challenges of VANET. Author suggests use of VPKI in which each node have both public and private key. When a node sends a message, it is signed by its private key and also adds certificate authorities (CAs) Certificate.

In existing papers, researchers use methods and schemes to provide security. But these schemes requires

large amount of energy and therefore computation overhead occurs. Hence here an energy efficient light-weight security scheme is proposed to solve these problems.

III. PROPOSED WORK

This paper proposes a security scheme that helps to reduce the eavesdropping attack efficiently. Due to use of permutation encryption it is difficult to 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. The proposed architecture is based on the following parts.

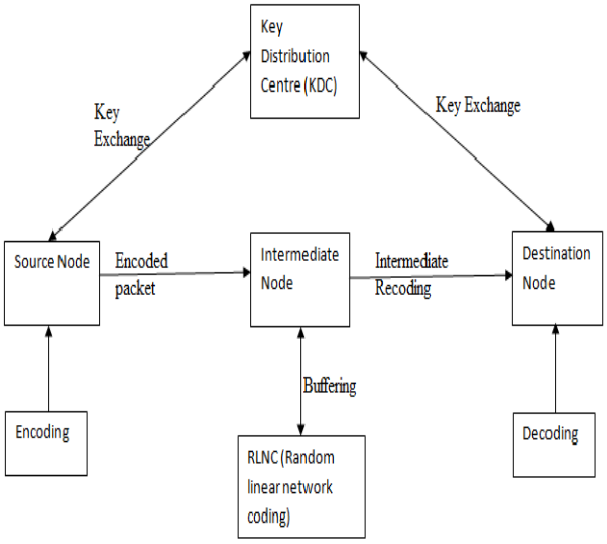

Figure 2: System diagram

The proposed system assumes that both the communicating parties must share a symmetric key by means of a key distribution centre.

This P-coding scheme initially consists of three stages as follows: source encoding, intermediate recoding and sink decoding[12].

A. *Source encoding*

Source encoding tries to encode the data comes from different nodes in order to transmit it more efficiently. Let the source node has sequence of message to send. Source prepends the local encoding vector (LEV) to these messages and then forwards these messages to the intermediate node.

B. *Intermediate recoding*

In this stage, permutation encryption function helps to rearrange the corresponding Global Encoding Vector (GEV) and symbols of the message. The key used for encryption is kept secret from the intermediate node.

C. *Sink Decoding*

On receiving the message from a source node, receiver decrypts the message by performing permutation decryption on it. Once the independent messages are collected, sink prepares the matrix representation of them. Finally, by applying Gaussian elimination original message can be recover.

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

- A key distribution center is used for sharing keys, and both communicating parties use the same key.
- Source encrypts the data with permutation encryption and appends a global encoding vector (GEV) to the packet and then forwards it to the intermediate node.
- Intermediate node forwards the packet to outgoing links with some modifications according to the P-coding.
- Sink node on receiving all the packets decrypts the packet with permutation decryption.
- Finally, to recover the original packet Gaussian elimination is performed.

IV. MATHEMATICAL MODEL

- Consider a VANET of N nodes,
  G= (V, E), where, V= {v1 ,….., vn} and E= {e1,….., en}
- Assume a node v ε V where,
  (-v)= Links terminating at v.
  (+v)= Links originated from v.
- Here, a link has capacity of carrying one packet per unit i.e. y (e).
- When a source wants to send series of packet $X= [x_{1,\ldots\ldots,}x_t]$ to a set of sink T where, $T \subseteq V$ then source computes y(e) as[1],
  $y(e)= \sum_{e\in(-v)} \beta(e)y(e)$
  where, $\beta(e)$ is a Local Encoding Vector(LEV)
- Global Encoding Vector can be appended to message as[1],
  $y(e) = \sum_{i=1}^{t} g_i(e)x_i = g(e)x$
  $Y = GX$
- Source encrypts packet with permutation encryption[1],
  $C[y(e)] = \sum_{e\in(-v)} \beta(e)C[y(e)]$
- Intermediate node forward packet to sink node with simple recoding with no extra efforts.
- Sink node will decrypt the packet as[1],
  $D\{c[y(e)]\}= E^{-1}\{E[y(e)]\} = y(e)$
- Thus source packets simply recover by applying Gaussian elimination,
  $X = G^{-1}(Y)$.

V. CONCLUSION

In this work, a light-weight encryption scheme is used for providing security in energy efficient way. This scheme is based on the network coding. In previous work, author shows that network coding can

be used to reduce the energy consumption by fewer transmissions. Here P-coding is used with network coding to reduce the energy consumption as well as to provide security in VANET. This scheme requires less energy for the process of encryption and decryption operation.

ACKNOWLEDGMENT

I would like to thank my guide Prof. V. S. Khandekar for her valuable feedback, constant encouragement and exemplary guidance throughout the duration of the paper. Her suggestions were of immense help throughout this paper. I am also thankful for the concern members of iPGCON2015 for their constant guidelines and support.

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] 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.

[3] S. Singh, C. Raghavendra, and J. Stepanek, ''Power- Aware broadcasting in Mobile Ad Hoc Networks,'' in Proc. IEEE PIMRC, 1999, pp. 1-10.

[4] J. Wieselthier, G. Nguyen, and A. Ephremides, ''Algorithms for Energy-Efficient Multicasting in Static Ad Hoc Wireless Networks,'' Mobile Network. Appl., vol. 6, no. 3, pp. 251-263, June 2001.

[5] B. Chen, K. Jamieson, H. Balakrishnan, and R. Morris, ''Span: An Energy-Efficient Coordination Algorithm for Topology Maintenance in Ad Hoc Wireless Networks'' Wireless Network, vol. 8, no. 5, pp. 481.

[6] R. Ahlswede, N. Cai, S.-Y.R. Li, and R.W. Yeung, ''Network Information Flow,'' IEEE Trans. Inf. Theory, vol. 46, no. 4, pp. 1204-1216, July 2000.

[7] J.P. Vilela, L. Lima, and J. Barros, ''Lightweight Security for Network Coding,'' in Proc. IEEE ICC, May 2008, pp. 1750-1754.

[8] Ghassan Samara, Wafaa A.H. Al-Salihy, R. Sures, Penang "Security Issues and Challenges of Vehicular Ad Hoc Networks (VANET)".

[9] 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.

[10] Y. Fan, Y. Jiang, H. Zhu, and X. Shen, ''An Efficient Privacy-Preserving Scheme Against Traffic Analysis in Network Coding,'' in Proc. IEEE INFOCOM, Apr. 2009, pp. 2213-2221.

[11] P. Zhang, Y. Jiang, C. Lin, Y. Fan and X. Shen, ''Pcoding: Secure Network Coding Against Eavesdropping Attacks,'' in Proc. IEEE INFOCOM, Mar. 2010, pp. 1-9.

[12] Ram Shringar Raw, Manish Kumar, Nanhay Singh "SECURITY CHALLENGES, ISSUES AND THEIR SOLUTIONS FOR VANET" International Journal of Network Security & Its Applications (IJNSA), Vol.5, No.5, September 2013.

[13] Mahalakshmi.R.S, Alangudi Balaji.N, "Privacy Preserving Authentication for Security in VANET" International Journal of Advanced Research in Computer Science & Technology (IJARCST 2014), 2014, IJARCST All Rights Reserved 200 Vol. 2 Issue Special 1 Jan-March 2014

[14] Suini Paul, Priyadarshini K.R, "Network Coding for Privacy Protection against Traffic Analysis in Multi-Hop Wireless Networks" International Journal of Advanced Research in Computer Science and Software Engineering, April 2012.

[15] Seung-Hoon Lee, Uhin Le, Kang-Won Lee, Mario Gerla "Content Distribution in VANETs using Network Coding: The Effect of Disk I/O and Processing O/H."