SURVEY OF ENERGY EFFICIENT ENCRYPTION SCHEME FOR VEHICULAR AD HOC NETWORK

Miss. Pooja Mundhe¹, Prof. V. S. Khandekar²
¹Dept. of Information Technology, Sinhgad Technical Education Society’s SKNCOE, Pune, India
Email.Id: Poooh.m99@gmail.com
²Dept. of Information Technology, Sinhgad Technical Education Society’s SKNCOE, Pune, India
Email.Id: Varsha.khandekar@gmail.com

Abstract: Vehicular Ad Hoc network is a part of mobile Ad Hoc Network. But unlike MANET, vehicular network have high mobility. It performs many activities for providing a safer and comfort driving condition. Energy saving is an important issue in VANET. Since ad hoc networks are broadcast in nature it consumes more energy in transmission and encryption/ decryption process of the packets. For this purpose a very useful method of Network Coding, P-coding can be used for reducing energy consumption at physical layer in VANET. P-Coding is a light-weight encryption scheme, which reduces the energy consumption by encryption/decryption of data. With the efficient permutation encryption it provides security against eavesdropping attack on network coding. Due to permutation encryption perform on coding vector and message content, it is difficult for an attacker to locate a coding vector without knowing permutation. Because of light-weight nature it consumes less energy than any other encryption scheme.

Keywords: Energy saving, light-weight encryption, Network Coding, Vehicular Ad Hoc Network.

Introduction
Vehicular ad hoc network (VANET) has become interesting research topic in area of wireless communication. VANET equipped with vehicles forms a network, which allows vehicles in a particular range to communicate with each other without any infrastructure. It also offer safety services and comfort services such as emergency warning, lane changing, traffic sign violation road condition warning, whether information, location of gas station or restaurants, price information and interactive communication such as internet access etc[2]. For providing this services energy is require. There are several energy-efficient schemes proposed to resolve this issue [3], [4] and [5]. Recent studies shows than network coding [6] can help to achieve minimum energy consumption in VANET. The main idea behind network coding is to mix the data comes from all input node and then forward it to output links [7]. When network coding is used each node in the network can efficiently encode the packet before forwarding it to another node. The encoding of the packet requires less energy due to network coding. With the help of following example this can be clarify. Suppose there
is a hexagon formed by connecting six nodes, and each node’s transmission range reach its left and right neighbour. Each node needs to transmit a message to all other nodes. Here without network coding, each message would require four transmissions, as shown in fig. 1(1).

Without considering the energy required for encryption and decryption operation, it would save ¼ energy.

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

Not only transmission, but encryption and decryption performed at each node for providing security also consume more energy in VANET. For example, in battle field or in a police van data communicated between vehicles should keep confidential during transmission [8]. The encryption schemes used for providing confidentiality in VANET are not efficient. In [9], a Motorola’s “Dragon Ball” embedded microprocessor consume near about 13.9 µJ to send a bit, while consumes another 7.9 µJ per bit for encryption when symmetric-key encryption algorithms are used. The information mixing characteristic of network coding provides intrinsic security, based on which efficient encryption scheme can be designed. In [10], it proposes to encrypt coding vector using Homomorphic Encryption Function (HEF), due to which network coding can perform directly on coding vectors. These approaches given has large overhead of computation or space, therefore they are not suitable for VANET. In this paper, a new encryption scheme is designed for providing security in energy efficient manner. In P-Coding [1] a light-weight encryption scheme both message content and coding vector are randomly permuted which makes eavesdropper impossible to locate coding vector since cannot get any useful information from it. There are different types of attacks and threats possible on VANET discussed in paper [8], such as Denial of Service, Message Suppression Attack, Fabrication attack, Alteration Attack, and Replay attack. The remaining of the paper is organised as follows. Section II describes the related work along with the literature review. Section III discusses about possible attacks and threats on VANET.

Related work PAMAS

In [3] paper, S. Singh proposes PAMAS protocol for reducing energy consumption. In an ad hoc network, the radio channel is shared by all nodes. That is, when a node transmits data to a specific node, all other nodes turn them off till the transmission completes. Therefore author propose a power aware protocol called PAMAS which saves energy by turning off nodes not participating in communication.

Node-join-tree

In [4] paper, author discuss the problem that, in ad hoc wireless network and a multicast request, there is a need to find multicast tree which consumes minimum energy. The author proposes node-join-tree (NJT), which is implemented in distributed fashion and also improve the energy efficiency.

XOR-based algorithm

In Mobile Ad Hoc Network, Network Coding can be applied to
broadcast messages in network which leads to significant consumption of energy by reducing the no approaches [11]. The author proposes two algorithms. First XOR-based coding algorithm that reduces 45% energy as compared to non-coding based approach. Second, Reed-Solomon based coding algorithm which depend only on local information, which gains up to 61% in their simulations.

**Random Linear Network Coding**

Network Coding used in ad hoc wireless network allows intermediate node not only to store and forward packet but also process and mix different incoming packets. In [7] author proposes a random linear network coding (RLNC) which provides security as well as the advantage of reduced computation or space overhead. Confidentiality can be achieved by locking the source coding vector required to decode the encoded packet, without interrupting the intermediate node from running their network coding operation.

**Homomorphic Encryption Function**

In [10] paper, author proposes an efficient Homomorphic encryption operation (HEF) perform on Global Encoding Vector which offer privacy-preserving features, like un-traceability and message content confidentiality. This scheme uses random linear coding, where each sink node invert the GEVs to recover source packet.

**Energy Consumption by Different Security Algorithm**

In [9] paper, author presents an analysis of the energy requirement by different encryption algorithms. The energy consumption by various security algorithm such as asymmetric, hash and symmetric algorithm used for authentication, integrity and secrecy of data is analyzed in this paper.

**RSA, DSA and ECDSA**

RSA is asymmetric encryption algorithm which requires energy for key generation, signing and verification. It is based on integer factorization. Elliptic curve digital signature algorithm ECDSA) provide security based on the discrete logarithm problem defined on elliptic curve. Paper shows that 163-bit ECDSA is energy efficient as compared to 1024-bit DSA. 1024-bit RSA and 163-bit ECDSA digital signature algorithms have complementary energy costs. RSA can efficiently perform the signature verification, while ECDSA requires smaller value for signature generation. There is a huge difference in energy cost for sign and verify function of RSA than ECDSA.

**ECDH and DH**

Elliptic Curve Diffie Hellman (ECDH) and Diffie Hellman (DH) is asymmetric algorithm used for performing key exchange. As per survey, 163-bit ECDH consumes less energy than 1024-bit DH key exchange. The energy cost of DH can be reduced by decreasing the key size from 1024 bits to 512 bits. But due to the reduced key size security also get decreases.

**MD2, MD4, MD5, SHA, SHA1 and HMAC**

Hash algorithms are least complex than other cryptographic algorithm and require least energy cost. MD2 and HMAC are more compute-intensive and incur more energy than rest of hash algorithms. HMAC is keyed hash, and the energy cost is increases with the increase in key size. SHA and SHA1 have larger number of steps and better collision resistance than MD4 and MD5. For these benefits algorithms requires higher energy than MD4 and MD5.

**RC4, BLOWFISH, AES**

RC4 is a fast and efficient stream cipher which is suitable in high speed networking application for encrypting data. RC4 has maximum encryption cost as compared to other symmetric ciphers. In RC4 energy is
consumed in memory access due to cache misses. Blowfish requires highest energy cost for key setup, while lowest for encryption and decryption. AES has competitive energy costs and run extremely fast on 32-bit processor with some space overhead.

Scope of the study
This paper focus on the problem of energy saving in Vehicular Ad Hoc Network based on the encryption technique of network coding.

Conclusion
Previous work shows that with network coding energy consumption can be reduced with less transmission in VANET. Here, P-Coding a light-weight encryption scheme can be used with network coding, to reduce the energy consumption as well as providing security in VANET. P-Coding is efficient in computation and requires minimum energy for encryption decryption operation.

Acknowledgement
I am extremely thankful to my guide Prof. V. S. Khandekar for suggesting topic for survey and providing all the assistance needed to complete the work. She inspired me to work in this area.

References


