ISSN 2278-3091

International Journal of Advanced Trends in Computer Science and Engineering, Vol.3 , No.4, Pages : 55-60 (2014)
Special Issue of ICCEIT 2014 - Held on September 01, 2014 in The Solitaire Hotel, Bangalore, India

Secure Message Broadcasting with Encryption Mechanism in VANETs

Ayana B.C
Department of Computer Science
KMEA Engineering College, Kerala, India.
ayana.babu@gmail.com

Maria Joy
Department of Computer Science
KMEA Engineering College
Kerala, India

Abstract— **Vehicular Ad-hoc NETworks (VANETs) are one of the most promising applications of MANET uses cars as mobile nodes to create a mobile network. A VANET turns every participating car into a wireless router or node. As cars fall out of the signal range and drop out of the network, other cars can join in, connecting vehicles to one another so that a mobile Internet is created. Secured communication in Adhoc wireless networks has more significance since the communication signals are openly available as they propagate through air and are more vulnerable to attacks. The successful deployment of vehicular communication requires Vehicle-to-Vehicle and Vehicle–to-fixed station communication with security. The main idea is to implement an encryption mechanism that aims to encrypt and forward data among the nodes. The encryption method used is RSA. The objective is to tackle the security problem so that VANETs can be implemented in a high security environment. The proposed method demonstrated based on ns-2 simulations.**

Keywords : Vehicular Ad-hoc Networks (VANETs), Encryption, RSA Encryption Method**.**

INTRODUCTION

Vehicular Ad-hoc NETworks (VANETs) creates a mobile network with vehicles as mobile nodes. A VANET allows cars approximately 100 to 300 metres of each other to connect and, in turn, create a network with a wide range. As cars fall out of the signal range and drop out of the network, other cars can join in, connecting vehicles to one another so that a mobile Internet is created.

In VANETs, a safety message is periodically generated (10Hz frequency) and transmitted to one-hop neighbour vehicles. These periodic “heartbeat” messages are the building blocks of many safety applications [1]. By aggregating this local information, each vehicle can construct and maintain a local neighbourhood map that can be utilized by safety applications. Cooperative driver assistance is one of the recent emerging applications in VANETs. Each vehicle periodically generates a small size safety message less than 200 bytes [23] which contains the state information of the vehicle. The goal of the communication is to provide a reliable up-to-date knowledge about the neighbourhood for each vehicle on the road. Each state message has a typical lifetime of less than 200ms after which it is not useful anymore. Having an up-to-date local map could prevent accidents and collisions by informing vehicles of a sharp velocity change. Also this extra information assists the driver to choose alternative driving strategies such as taking over or turning.

Adhoc wireless networks are defined as the category of wireless networks that utilize multi-hop radio relaying and are capable of operating without the support of any fixed infrastructure and nodes communicate directly between one another over wireless channels [6]. As the wireless channels are openly available and propagate through the air, security in adhoc networks is of primary concern [22][5]. In an adhoc wireless network, the routing and resource management are done in a distributed manner in which all nodes coordinate to enable communication among them as a group. This requires each node to be more intelligent so that it can function both as a network host for transmitting and receiving data and as a network router for routing packets from other nodes. As adhoc networks significantly vary from each other in many aspects, an environment-specific and efficient key management system is needed [4]. To protect nodes against eavesdropping, the nodes must have made a mutual agreement on a shared secret or exchanged public keys. For very rapidly changing adhoc networks the exchange of encryption keys may have to be addressed on-demand, thus without assumption about a priori negotiated secrets.

Proposed method concentrates on successful deployment of vehicular communication which requires Vehicle-to-Vehicle and Vehicle–to-fixed station communication with security. The core design is an encryption method using RSA which is used to provide reliability and security for small safety messages with low overhead. The VANET designed with security can enhance passenger safety and preserve the safety messages against threats.

Vehicular Adhoc Network (VANET) is a wireless Adhoc network based on IEEE 802.11 wireless standard, which facilitates vehicle to vehicle and vehicle to roadside communications through air interface. Also intelligent vehicular Adhoc networks (InVANETs) use WiFi IEEE 802.11 and WiMAX IEEE 802.16 for fastest communication between vehicles with dynamic mobility.

The basic idea of working of VANETs is like, Vehicular Networks System consists of large number of nodes, approximately number of vehicles exceeding 750 million in the world today [16], these vehicles will require an authority to govern it, each vehicle can communicate with other vehicles using short radio signals DSRC (5.9 GHz), for range can reach 1 KM, this communication is an Adhoc communication that means each connected node can move freely, no wires required, the routers used called Road Side Unit (RSU), the RSU works as a router between the vehicles on the road and connected to other network devices. The radio used for the communication is Dedicated Short-Range Communications (DSRC), which been allocated as new band in 1999 by the Federal Communications Commission (FCC),the band allocated was 75 MHz at 5.9 GHz frequency for Intelligent Transport System (ITS) applications in north America[16].

MOTIVATION

The motivation of this project is to create a secure message broadcast between vehicular nodes for use in vehicular environment. Thus VANET helps the drivers of vehicles to communicate the information. Also it ensures safe journey by minimizing road accidents, diverting or instructing the vehicle’s direction in less populated roads avoiding traffic jam. Vehicles in a VANET are having high degree of mobility, i.e., the vehicles are moving very fast, especially in high ways. The vehicular nodes communicating in VANETs make constant location changes with different speeds and directions. This allows the network to be dynamic in nature. So, in order to make communication successful, it is challenging to establish security protocols.

The security of VANETs is one of the most critical issues because their information [2] transmission is propagated in open access environments. It is necessary that all transmitted data cannot be injected or changed by users who have malicious goals. Moreover, the system must be able to detect the obligation of drivers while still maintaining their privacy. According to a survey conducted on a total of 186 articles those were extracted from the most relevant scientific sources [19].Their analysis study proves that there doesn’t exist a comprehensive security protocol or framework that covers all security aspects of VANET. Therefore, it is necessary to develop a suitable framework which mitigates all these security problems. This strongly recommends the need for security in VANETs.

VANETs architecture [3] is exposed to different types of attacks, and due to peculiar nature of adhoc and fast moving nodes, a simple attack becomes inevitable. The fast moving nature of the nodes and consequently, complex medium access control as well as the short lifetimes of the links, does not merit a complex cryptographic procedure. However, since a fake safety / warning message may create great confusion, we cannot either leave the communication totally unsecured.

Main benefit of VANET communication is enhanced passenger safety by exchanging warning messages between vehicles. Clearly, VANET can be affected by many attacks like denial of service, message suppression and propagation of false message attacks. In order to increase safety in data transmission, security is the most challenge in VANET. The secure designed VANET can enhance passenger safety and preserve the safety messages against threats [9].

Applications [19] related to road safety, such as road congestion message or accident report, shall be highly localised and delay sensitive. Most of these applications shall have unidirectional communication, containing warning messages. Any delay in timely propagation of warning messages may lead to failure of warning. Similarly any fake warning may lead to some other security hazards, such as traffic jam in other sectors.

VANETs are a subset of MANETs (Mobile Ad-hoc NETworks) in which communication nodes are mainly vehicles. As such, this kind of network should deal with a great number of highly mobile nodes [3], eventually dispersed in different roads. In VANETs, vehicles can communicate each other (V2V, Vehicle-to-Vehicle communications). Moreover, they can connect to an infrastructure (V2I, Vehicle-to-Infrastructure) to get some service. This infrastructure is assumed to be located along the roads.

Vehicular networks have tremendous development nowadays and several applications put forward by this new kind of communication network [15]. However, as those applications have impact in road traffic safety, strong security requirements must be achieved. VANET security should ensure that the information received is correct (information authenticity), the source is who he claims to be (message integrity and source authentication), the node sending the message cannot be identified and tracked (privacy) and the system is robust.

Reliable periodic broadcasting of messages using network coding in VANETs was proposed by Behnam Hassanabadi and Shahrokh Valaee in 2014 which mainly focussed on message broadcasting were a random linear network coding is used. The beneficiary factor is proper assurance of message delivery. The proposal provides improvement to IEEE 1609.4 WAVE Standard [1]. Earlier work of authors was based on network coding [23], given the local feedback information and already heard messages; each node tries to find the best message combining strategy such that the number of nodes that can instantly decode an uncoded packet is maximized. But network coding has no benefits from feedback information. This is because that the feedback information consumes lot of network resources. This would rather increase the implementation cost as well.

Several solutions have been proposed with the aim to improve the efficiency of broadcasting in Adhoc networks. A widely applied approach is based on probabilistic message transmissions [12], in which the messages generated by a traffic source are rebroadcast by other nodes with a certain probability. This solution reduces the overhead with respect to simple flooding; however it may lead to a low delivery ratio, especially in the case of scarcely connected nodes. In counter-based schemes [12], instead, a node determines whether to rebroadcast a packet by counting how many identical packets it receives over a given time interval. In distance-based broadcasting [12], nodes make use of their distance from the previous sender as decision criteria. The main idea is to enable those nodes that are located farther away from the sender to rebroadcast the packet, so as to increase the message spatial progress.

Broadcasting techniques have been recently studied also for the dissemination of alarms or warnings in vehicular networks. In [13] broadcast packets include information about the sender position and the message-propagation direction: whenever a node receives a copy of a broadcast message, it rebroadcasts the packet only if the node follows the sender.

As mentioned in [7], simply using repetition based schemes would aggravate congestion problem. As the messages repeated would reduce packet drop and increase reliability the congestion problem arises. Most of the previous works on the application of network coding in vehicular network deal with the content distribution from a Road Side Unit (RSU) to multiple On Board Units (OBUs).

Another scheme [8] was based on simple random linear coding scheme for reliable communication by D.S. Lun, and demonstrated that it is capacity-achieving as long as packets received on a link arrive according to a process that has an average rate. The analysis was based mainly on long-term throughput, but for delay sensitive safety messages short-term throughput or the successful message reception in a small time window is of interest. This was the main drawback of the analysis scheme.

In [10], [11], authors propose a XOR-based network coding in which each user blindly picks a number of original messages for encoding. It is assumed that Conditional Reception Probability (CRP), defined as the probability that a packet is received by a neighbour vehicle given it is successfully received by the transmitter, is known. The optimal number of packets to encode is then determined based on the CRP. The optimized metric is the average number of pair wise recoveries. This means, if vehicle *A* is transmitting, the number of XORed packets is optimized in order to maximize the expected number of recovered packets by vehicle *B*. However, in practice, after vehicle *A*'s transmission, multiple destinations can potentially decode and a more reasonable metric should be the expected number of decoded packets by all neighbours. The main drawback of the XOR-based coding schemes is the need for feedback information which can consume a fair amount of network resources. In [14], the transmission of each vehicle is triggered by a timer set upon the reception of every new packet. Since neighbours' current reception status is not considered, the broadcasted packets are not always useful for neighbouring vehicles, which decreases the bandwidth efficiency. Also due to lack of coordination between concurrent transmitting vehicles, the scheme tends to suffer from severe collisions, especially under dense vehicular traffic.

Secured communication in Adhoc wireless networks is primarily important, because the communication signals are openly available as they propagate through air and are more susceptible to attacks ranging from passive eavesdropping to active interfering [22]. The lack of any central coordination and shared wireless medium makes them more vulnerable to attacks than wired networks. Nodes act both as hosts and routers and are interconnected by Multi-hop communication path for forwarding and receiving packets to/from other nodes. The objective of this paper is to propose a secure communication between the vehicular nodes through key exchange and encryption mechanism that aims to encrypt and forward data among the nodes.

SYSTEM ENVIRONMENT

Vehicular nodes in a VANET are having high degree of mobility, i.e., the vehicles are moving very fast, especially in high ways. The mobility of nodes is considered at random points. The base transmitter acts as a fixed node for communication between vehicular node and base transmitter. The traffic scenario is created for vehicular nodes at random point. The routing protocol used is Adhoc On demand distance vector routing (AODV).

The Encryption mechanism used here is RSA. In order to implement confidentiality the key for secret key encryption is encrypted using the receiver's public Key. Decryption is carried out with receiver's private Key. For key exchange RSA is used. Once secret keys are exchanged symmetric key encryption is used for communication. The system implemented using ns2 version-2.33.The different stages considered for this work are:

1. Packet transfer
2. Node Connectivity and routing performance
3. RSA Encryption of messages

4. Average end to end Delay and Throughput Evaluation.

Packet Transfer

The packet flow takes place in four simulation scenarios: Vehicle to Fixed Station communication with slow movement of VANETs , Vehicle to Fixed Station with fast movement of VANETs, Vehicle to vehicle communication with normal movement of VANETs and Vehicle to vehicle communication with frequent movement of VANETs. For vehicle to fixed station one node remains as fixed and remaining nodes will be moving .The fixed station acts as base transmitter. For vehicle to vehicle communication all the nodes are moving and communication takes place between vehicles.

Communication capabilities[21] in vehicles are the basis of an envisioned InVANET or intelligent transportation system (ITS). Vehicles are enabled to communicate among themselves (vehicle-tovehicle, V2V) and via roadside access points (vehicle-to-roadside, V2R). Vehicular communication is expected to contribute to safer and more efficient roads by providing timely information to drivers, and also to make travel more convenient. The integration of V2V and V2R communication is beneficial because V2R provides better service sparse networks and long distance communication, whereas V2V enables direct communication for small to medium distances/areas and at locations where roadside access points are not available.

Node Connectivity and routing performance

Vehicular nodes in a VANET are having high degree of mobility, i.e., the vehicles are moving very fast, especially in high ways. The mobility of nodes is considered at random points. The base transmitter acts as a fixed node for communication between vehicular node and base transmitter. The traffic scenario is created for vehicular nodes at random point. Communicating method from one vehicle (source) to another vehicle (destination) through different vehicles (nodes) is called routing.The routing protocol used is Ad-hoc On demand distance vector routing, AODV. Efficient routing protocols can provide significant benefits to Adhoc networks in terms of both performance and reliability. AODV initiates a route discovery process, which goes from one node to the other until it reaches to the destination or an intermediate node has a route to the destination.

AODV is a reactive protocol, even though it still uses characteristics of a proactive protocol [18]. AODV takes the interesting parts of DSR and DSDV in the sense that it uses the concept of route discovery and route maintenance of DSR and the concept of sequence numbers and sending of periodic hello messages from DSDV.

RSA Encryption of messages

RSA is one of the first practicable public-key cryptosystems and is widely used for secure data transmission [17]. In such a cryptosystem, the encryption key is public and differs from the decryption key which is kept secret. In RSA, this asymmetry is based on the practical difficulty of factoring the product of two large prime numbers, the factoring problem. A user of RSA creates and then publishes the product of two large prime numbers, along with an auxiliary value, as their public key. The prime factors must be kept secret. Anyone can use the public key to encrypt a message, but with currently published methods, if the public key is large enough, only someone with knowledge of the prime factors can feasibly decode the message. The encryption mechanism used here is RSA. RSA algorithm employs the use of 512-bit numbers. Cracking such a system requires the ability to factor the product of two512-bit prime numbers [20].

To implement confidentiality the key for secret key encryption is encrypted using the receiver's public Key. Decryption is carried out with receiver's private Key. For key exchange RSA is used. Once secret keys are exchanged, symmetric key encryption is used for communication.

Average end to end Delay and Throughput Evaluation.

The average end-to-end delay in a VANET means that the source node sends packet to destination node and total average time to reach the packet to destination Node. The time consumption is the time taken for encryption which can be thought of as a negligible factor when security is considered.

In communication networks throughput or network throughput is the rate of successful message delivery over a communication channel. This data may be delivered over a physical or logical link, or pass through a certain network node. The throughput is usually measured in bits per second (bit/s or bps), and sometimes in data packets per second or data packets per time slot.

SYSTEM EVALUATION

All simulation experiments are developed and simulated on network simulator NS2 version NS-2.33. A simulation script generally begins by creating an instance of this class and calling various methods to create nodes, topologies, and configure other aspects of the simulation.

The parameters considered here are average end-to-end delay during transmission and throughput observed during transmission. These factors are considered for different scenarios. About 10 wireless nodes are considered for vehicle to vehicle (with encryption), vehicle to fixed station (with encryption), and vehicle to fixed station (without encryption).

The different simulation scenarios considered here are:

1. Simulation1: Normal scenario without encryption.

   In this simulation scenario there are 10 wireless nodes with a base fixed station which acts as a base transmitter and the communication takes place between the vehicular nodes through this base transmitter. The packets sent here are not encrypted. This is quite risk when we consider a secure environment. Even drivers of the vehicles may be misleading to false routes because of fake messages through hackers.

2. Simulation 2: vehicles to fixed station with slow movements with encryption.

   The simulation with encryption is the proposed system. The packets send here are encrypted with high secure RSA technique. The confidentiality is preserved through encryption and it can be considered for a secure environment. The proposed system is also simulated with 10 wireless nodes. Here the vehicular nodes communication takes place through a base transmitter which remains as fixed and packets are transmitted with receiver's public key encrypted. So authentication can be assured. The receiver will decrypt with his private key. The encrypted packets are sent through base transmitter to vehicular nodes. The slow movements of vehicular nodes are considered here. This is to demonstrate medium traffic on the network.

3. Simulation 3: vehicles to fixed station with fast movements with encryption.

   As mentioned before here also encrypted packets are sent between base transmitter and vehicular nodes. The scenario is to demonstrate heavy traffic where the vehicular nodes are congested. The encrypted packets are sent with negligible delay and considerably high throughput. These parameters are obtained without much difference when compared to medium traffic.

4. Simulation 4: vehicle to vehicle with normal movements with encryption.

   Vehicles are enabled to communicate among themselves in vehicle to vehicle communication. The vehicular nodes send encrypted packets to other vehicular nodes. The simulation scenario demonstrates normal movement of VANETs.

5. Simulation 5: vehicle to vehicle with frequent movements with encryption.

   The same vehicle to vehicle scenario as mentioned above considered here with frequent movement of VANETs. This is particularly to demonstrate the communication of vehicles during heavy traffic. The encrypted packets are sent with negligible delay and considerably high throughput. These parameters are obtained without much difference when compared to medium traffic.

The figure 1 represents the screenshot for a vehicle to fixed station scenario.

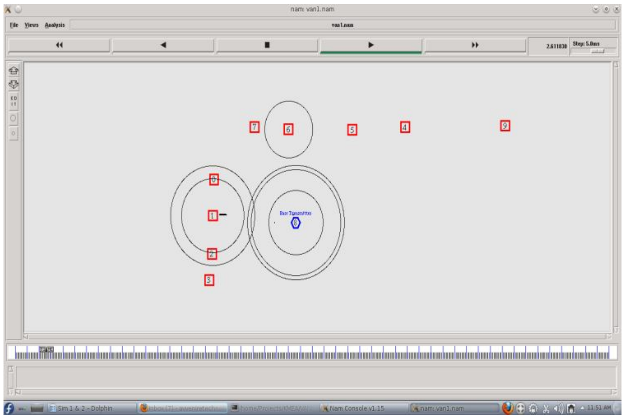

Fig 1: vehicle to fixed station communication

The approximate values calculated for different scenarios are observed. The values obtained are entered in the table below:

Table1: Simulation results for different scenarios.

Scenarios	**Average end to end delay**	**Throughput**
Simulation1	317.512 ms	909.894 KB
Simulation2	371.185 ms	1277.196 KB
Simulation 3	397.492 ms	1133.856 KB
Simulation 4	225.783 ms	888.55 KB
Simulation 5	257.412 ms	693.73 KB

The observation for different simulation is entered in the table. Simulation 1 represents a normal scenario without encryption all other simulation is with encryption. The encryption is considered for four different scenarios with vehicle to vehicle and vehicle to fixed station. Slow and fast movements of nodes are considered to represent medium and congested traffic on the network. The parameters considered are average end to end delay and throughput. As security is given higher priority through encryption the average end to end delay with negligible difference can be neglected. Average end to end delay for the one without encryption is low but the security is at high risk. Simulation 1 is vehicle to fixed station without encryption and simulation 2 and 3 with encryption. The throughput obtained is high for the one with encryption when compared to the one without encryption. Simulations 4 and 5 are vehicle to vehicle communication with encryption with slow and fast movements of nodes to demonstrate medium and heavy traffic on the network.

CONCLUSION

The proposed scheme provides secure broadcasting opportunity. The design can be implemented with additional security by encrypting the message sent between Vehicular Nodes. Security measures guarantees that the transmissions of data are authentic. The encryption allows both sender and receiver to communicate in a secure fashion. The performance of VANET can be enhanced with negotiable end to end delay and considerably high throughput. This provides authentication and high security level in VANETs. This shall be applicable wherever group communications is to be established in a secured manner in an Adhoc environment.

ACKNOWLEDGEMENT

I am thankful to the Management, the department of Computer Science and the department of Information Technology of KMEA Engineering College for their valuable support and guidance.

REFERENCES

[1] Behnam Hassanabadi and Shahrokh Valaee “Reliable Periodic Safety Message Broadcasting in VANETs Using Network Coding” *IEEE transactions on wireless communications, VOL. 13, NO. 3, MARCH 2014.*

[2] *Manpreet Kaur, Rajniand Parminder Singh"*An encryption algorithm to evaluate performance of v2v communication in vanet*",International Journal on Cryptography and Information Security (IJCIS), Vol.3, No. 2, June 2013.*

[3] *M.K. Nasir et al,"Security Challenges And Implementation Mechanism For Vehicular Adhoc Network",International journal of scientific & technology research volume 2, issue 4, April 2013*

[4] Y. P. Fallah, C. Huang, R. Sengupta, and H. Krishnan, “Congestion control based on channel occupancy in vehicular broadcast networks,”in *Proc. 2010 IEEE Veh. Technol. Conf. – Fall.*

[5] Y. Fallah, C.-L. Huang, R. Sengupta, and H. Krishnan, “Analysis of information dissemination in vehicular ad-hoc networks with application to cooperative vehicle safety systems,” *IEEE Trans. Veh. Technol.*,vol. 60, no. 1, pp. 233–247, Jan. 2011.

[6] Lidong Zhou and Zygmunt J. Haas, “Securing Adhoc Networks”, IEEE Network, November 1999

[7] C. Gui, P. Mohapatra, “Efficient overlay multicast for mobile Adhoc networks”, in Proceedings of IEEE Wireless Communications and Networking Conference (WCNC), March 2003.

[8] Q. Xu, T. Mak, J. Ko, and R. Sengupta, “Vehicle-to-vehicle safety messaging in DSRC,” in *Proc. 2004*

[9] D. S. Lun, M. Medard, R. Koetter, and M. Effros, “On coding for reliable communication over packet networks,” *Physical Commun.*, vol. 1, no. 1,pp. 3–20, 2008.

[10] Z. Wang, M. Hassan, and T. Moors, “Efficient loss recovery using network coding in vehicular safety communication,” *IEEE Wireless Commun. Netw. Conf.*, pp. 1–6.in *Proc. 2010*

[11] Z. Wang and M. Hassan, “Blind XOR: low-overhead loss recovery for vehicular safety communications,” *IEEE Trans. Veh. Technol.*, vol. 61, no. 1, pp. 35–45, 2012.

[12] S. Ni, Y. Tseng, Y. Chen, and J. Sheu, “The Broadcast Storm Problem in a Mobile Adhoc Networks,” in *ACM MobiCom*, Aug. 1999.

[13] E. Fasolo, R. Furiato, and A. Zanella, “Smart Broadcast Algorithm for Inter-Vehicular Communications,” in *WPMC*, 2005.

[14] J.-S. Park, U. Lee, S. Y. Oh, M. Gerla, and D. S. Lun, “Emergency related video streaming in VANET using network coding,” in *Proc. 2006 VANET* pp. 102–103.

[15] F. Farnoud and S. Valaee, “Repetition-based broadcast in vehicular Adhoc networks in Rician channel with capture,” *2008 Comput. Commun.Workshops, IEEE INFOCOM.*

[16] GMT Abdalla, SM Senouci “Current Trends in Vehicular Adhoc Networks”, Proceedings of UBIROADS workshop, 2007.

[17] http://en.wikipedia.org/wiki/RSA_(cryptosystem) accessed on 08-05-2014.

[18] http://www.arpapress.com/volumes/vol7issue3/ijrras_7_3_15.pdf accessed on 12-05-2014.

[19] Shidrokh Goudarzi ,et al,” A Systematic Review of Security in Vehicular Adhoc Network” Presented at the 2nd Symposium on Wireless Sensors and Cellular Networks (WSCN'DEC13)

[20] Hafeesa M Habeeb, Selin M,”VANET GBM”National conference on Information and communication Technologies(NCICT- March 2014) .

[21] Aiswarya Sudhakar, Vidya Hari “ Evidence token Scheme Based Efficient Cooperative Message Authentication in Vehicular Adhoc Networks ”National conference on Information and communication Technologies(NCICT-2014).

[22] S. Sumathy and B.Upendra Kumar, “Secure key Exchange and Encryption Mechanism for group communication in wireless Ad-hoc Networks” *Journal on Applications of Graph Theory in wireless Ad-hoc networks v0l2,No:1,MARCH 2010”*

[23] B. Hassanabadi and S. Valaee, “Reliable network coded MAC in vehicular ad-hoc networks,” in *Proc. 2010 IEEE Veh. Technol. Conf.– Fall.*