Survey on Improving Performance and Security in VANET using Lattice Based Cryptographic Technique

Jeet Gandhi[1]**, Jay Amin**[2]
[1, 2] Department of Computer Engineering
[1, 2] L.J. Institute of Engineering and Technology, Ahmedabad, India.

Abstract- *Vehicular Ad-Hoc Network (VANET) is a wireless connection of network which is formed between the vehicles. In VANET, there is communication between vehicles V2V or between vehicle and road side unit V2R. In VANET, there are various possible attacks done by the malicious node which are to be withstand. Therefore, the ad-hoc network must be securely developed in order to avoid attacks. In this paper, we discuss the security aspects by reviewing various routing protocols and some of the encryption techniques for the VANET along with the possible attacks.*

Keywords- *VANET, V2V, V2I, AODV, Encryption Techniques, RSA, NTRU*

I. INTRODUCTION

Vehicles are connected to each other through an ad-hoc formation which forms a wireless network called "Vehicular Ad-hoc Network." It infrastructure less, distributed,self-organizing, communication networks. More precisely it is network aiming to improve driving safety and traffic management with internet access. [7] It includes vehicle to vehicle (V2V) and vehicle to infrastructure (V2I) communication in a short range of 100 to 300m. The nodes in the network which are the vehicles communicate to one other by means of North American DSRC (Dedicated Short Range Communication) standard that employs the IEEE 802.11p. It uses 5.850-5.925 GHz band for the use of public safety and private applications [8]. In VANET, the access and the routing protocols are facing several issues like available bandwidth estimation, medium access control, hidden and exposed node problem, high mobility, support of heterogeneous vehicles, fast speed, obstacles and fast handovers. [1] Because of high mobility VANET face challenges in routing protocols.[6] There are numerous routing protocols introduced for the VANET which still faces tremendous challenges like node mobility, limited resources and limited physical security.[1]

Another major concern is the message security in the network. The communication takes place between V2V or V2I so it is easy for any attacker to attack the message and compromise the privacy and security of the node. Hence, there is required secured environment in order to have efficient communication between the nodes.

II. VANET ARCHITECTURE

From the vehicular communication perspective, it can be categorized into: Road-vehicle and the inter vehicle communication. The VANET architecture is as follows:

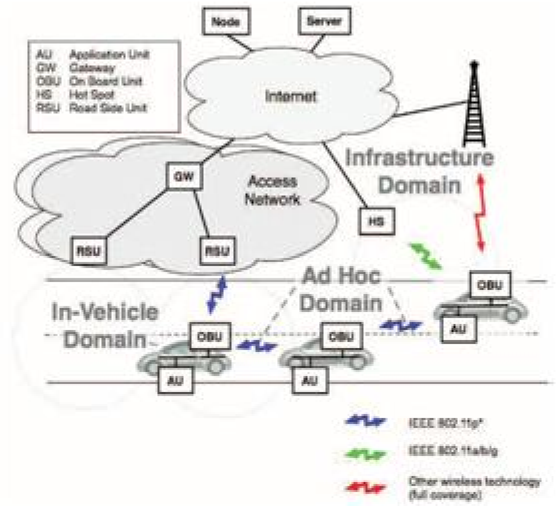

Fig.1 C2C-CC draft reference architecture[8]

There are various components in VANET architecture.

- **On board unit (OBU):** It is a physical device located in the vehicle. It is responsible for the V2V and V2R communication. AU and OBU are connected by Ethernet. Its two main components are reporter which automatically detects road traffic events and delivers them to the disseminator. And other component is receiver which receives messages from disseminator.
- **Road side Unit (RSU):** It is a physical device located at fixed positions along roads, highways or dedicated locations.
- **Application Unit (AU):** It is an in-vehicle or road-side entity and runs applications that can utilize the OBU's and RSU's communication capabilities. Its main component is disseminator which aggregates road traffic event reported by clients and propagates them to other receivers.

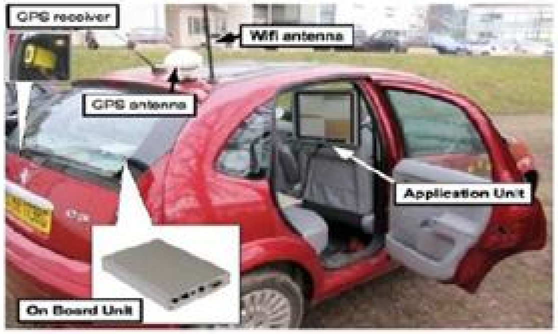

Fig.2 Example of OBU, AU[11]

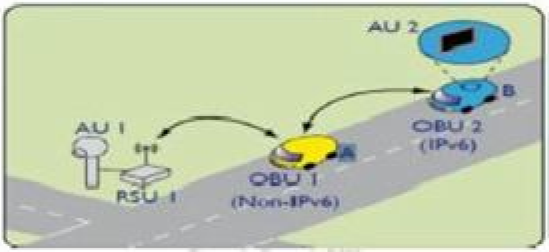

Fig.3 Example of RSU[11]

III. CHARACTERISTICS OF VANET

Vehicular networks have specific characteristics which have to be taken into account while building the architecture. [4][7]

- **High mobility:** The nodes in VANETs usually are moving at high speed. This makes harder to predict a node's position and making protection of node privacy.
- **Continuously changing network topology***:* Due to high node mobility and random speed of vehicles, the position of node changes frequently. Hence, network topology in VANETs tends to change frequently.
- **Unbounded network size:** VANET can be implemented for one city, several cities or for countries, which means the network size in VANET is geographically unbounded.
- **Time Critical:** The information in VANET must be delivered to the nodes with in time limit so that a decision can be made by the node and perform action accordingly. [7]
- **Wireless Communication:** VANET is designed for the wireless environment. Nodes exchange their information via wireless network.
- **Better Physical Protection:** The VANET nodes are physically better protected. Thus, VANET nodes are more difficult to compromise physically and reduce the effect of infrastructure attack. [7]
- **Central Authority***:* Each and every vehicle in the network has to be registered with a common Centralized Authority and should be assigned an unique identifier for the vehicles security purpose. This hence provides with better security.
- **Power Consumption***:* In traditional wireless networks, nodes are power limited and their life depends on their batteries. But Vehicles can provide continuous power to their computing and communication devices. [5]

IV. SECURITY CONCERNS IN VANET

VANET suffers from various attacks which are listed below: [1] [7]

A. *Types of Attacks*:

- **Denial of Service attack:** The attacker in this type of attack jams the communication channel. It also takes the control of the node's resources.
- **Fabrication Attack:** An attacker can enforce by transmitting false information into the network.
- **Alteration Attack:** The attacker alters an existing data, like delay in the transmission, replaying earlier transmission, or altering the data transmitted.
- **Replay Attack:** Here an attacker replay the transmission of earlier information to take advantage of the situation of the message at time of sending.
- **Sybil Attack:** This attack happens when an attacker creates large number of pseudonymous, e.g.: jam ahead and force them to take alternate route.
- **Routing attack:** Routing attacks re the attacks which exploits the vulnerability of network layer routing protocols. In this type of attack the attacker either drops the packet or disturbs the routing process of the network.

B. Security Requirements:

There are various security requirements to be fulfilled in order to have secure transmission of the data: [1] [7]

- **Authentication:** In Vehicular Communication every message must be authenticated, to make sure for its origin and to control authorization level of the vehicles.
- **Availability:** Vehicular network must be available all the time, for many applications vehicular networks will require real-time.
- **Non-repudiation:** Non-repudiation will facilitate the ability to identify the attackers even after the attack happens. This prevents cheaters from denying their crimes.
- **Privacy:** Keeping the information of the drivers away from unauthorized observers, this information like real identity, trip path, speed etc.

- **Real-time constraints:** Vehicles move in high speed, this will require a real-time response in some situation, or the result will be devastating.
- **Integrity***:* Integrity for all messages should be protected to prevent attackers from altering message contents.
- **Confidentiality***:* The privacy of each driver must be protected from outsiders from gaining the drivers information.
- **Security Enhancement***:* Security stands the most important and challenging issue in safety applications of VANETs. If no security is provided in routing protocols, a malicious node can enter the network and cause damage. This could lead in misleading of information which can be used by terrorists to trap innocent people as dead end tunnel.

V. ROUTING PROTOCOLS

There are various routing protocols used in the VANET. The existing routing protocols used are divided into three categories: [2]

- TBR, Topology based routing
- PBR, Position based routing
- Hybrid routing

Among them, the routing protocol based on topology should be divided into pre-active routing protocols and reactive routing protocols, as described in figure which shows the VANET routing protocol classification. The designing on VANET routing protocol referenced the Ad hoc working group on the traditional network DSDV and AODV and other network protocol, and made the comprehensive use of position or velocity information and put forward the GPSR, GPCR and GeoDTN + Nav routing protocols.

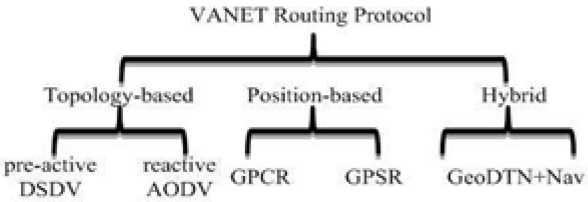

Fig.4 VANET Routing Protocol Classification [2]

The detailed information is provided for the topology based routing protocols:

A. Proactive routing protocol: Proactive routing protocols, also known as table-driven protocols, allow every network node to maintain a routing table for storing the route information to all other nodes, every next hop node is maintained in the table entry that comes in the path towards the destination from the source. [9]

- *Destination Sequenced Distance Vector (DSDV) Routing Protocol:* It is based on the distance vector strategy using shortest path algorithm. It implements a single route from source to destination which has been maintained in the routing table. A routing table is maintained for each node containing information of every accessible node in the network and total number of hops needed to succeed those nodes. The destination node initiates a sequence number to every entry in the table. Each node maintains the route reliability by broadcasting their routing table to the neighbouring nodes. DSDV protocol does not allow cyclic routes, reduces control message overhead and excludes extra traffic caused by frequent update. The total size of routing table is reduced as DSDV keeps solely the best possible path to each node instead of multi paths. DSDV is not able to control the networks congestion that decreases the routing efficiency.

B.Reactive routing protocols: Reactive routing protocols, also known as on-demand routing protocols. They are called so because on requirement of a route that does not exist from source node to destination node, the route discovery starts. Flooding of the network helps in route discovery mechanism by sending a route request message. Any node existing on the route towards the destination on receipt of the request message, sends back a route response message to the source node using unicast communication. [9]

- **Ad-hoc On-demand Distance Vector (AODV) Protocol:** AODV protocol reduces flooding in the network and gives low network overhead comparing to the proactive protocols. This routing protocol minimizes the routing table by creating a route when a node needs to send information data packets to other nodes in the network, hence reducing the memory size required. The routing table keeps the entries of the recent active nodes and the next hop node of the route instead of keeping the whole route. AODV uses destination sequence numbers (DesSeqNum) for route discovery which eliminates looping in routes and provides dynamic updates for adapting the route conditions. AODV is more suitable for large networks and network having high dynamic topology. This protocol causes delay in route discovery process. When route failures occur, new route discovery is required causing additional delays thus decreasing the data transmission rate and increasing the network traffic. This causes more bandwidth consumption that is increased due to increasing number of nodes in the network which causes collision leading to packet loss problem.

- **Dynamic Source Routing (DSR) Protocol:** DSR routing protocol is a reactive protocol which implements routing process using low overhead and quick reaction to frequently changing topology to ensure successful packet delivery even if change in network happens. DSR is a multi-hop routing protocol decreases the network traffic by decreasing periodic messages. DSR provides two processes that are the route discovery mechanism and route maintenance process.

The information regarding position based routing is as follows:

- **Greedy Perimeter Stateless Routing (GPSR):** GPSR follows greedy routing mechanism for routing in VANETs. During this protocol routing, every node sends a data packet to different intermediate nodes that are close to destination node, until the data reaches the destination. If there are not any neighbouring nodes nearer to message's destination, it makes use of perimeter forwarding technique to come to a decision to which node the message should be delivered.

VI. Existing Encryption Techniques[3]

Classical methods of creating digital signatures rely on the fact that it is difficult to deduce the private key, which is used to create a signature, from the public key, which is used to verify it. Some of these are as follows:

a) PKCS: Public Key Cryptography is based on the creation of mathematical puzzles that are difficult to solve without certain knowledge about how they were created. The creator keeps that knowledge secret (the private key) and publishes the puzzle (the public key). The puzzle can
then be used to scramble a message in a way that only the creator can unscramble.

b) RSA: The RSA algorithm, used products of two large prime numbers as the puzzle: a user picks two large random primes as her private key and publishes their product as her public key. The difficulty of factoring ensures that no one else can derive the private key (i.e., the two prime factors) from the public one. However, due to recent progress in factoring, RSA public keys must now be thousands of bits long to provide adequate security.

Drawbacks:

The RSA encryption scheme can also be used to perform signatures, but only if the enemy is unable to factor large numbers. A forger with a quantum computer, for
instance, could successfully create false signed messages. The same problem arises when RSA is used for encoding secret information, and can be partially circumvented by quantum key distribution.

c) Quantum Digital Signatures: In fact, instead of having the public key be a string of classical bits, we let the public key be a number of quantum bits. Given n classical bits, there are only 2n possible values, and by looking at the string, we can tell exactly which one we have. There are many more possible states of n qubits. This means that we can let the public key be one of these
many possible quantum states, chosen at random, while the private key says which of the states it is. Only theperson who picked the state knows the private key,
which enables them to sign messages without fear of having them forged.

Drawbacks:

The quantum processing and storage required for this scheme are just beyond the edge of current technology. Also, an enemy who gets too many copies of the public key will be able to figure out its identity, so to prevent this; the sender has to limit the number of copies she distributes. It is possible to make that number very large, however, so this is not too severe a restriction.

d) Elliptic Curve: An elliptic curve is a plane curve defined by an equation of the form $y2 = x3 + a\,x + b$
The set of points on such a curve (i.e., all solutions of the equation together with a point at infinity) can be shown to form an abelian group (with the point at infinity as
identity element). If the coordinates *x* and *y* are chosen from a large finite field, the solutions form a finite abelian group. The discrete logarithm problem on such elliptic curve groups is believed to be more difficult than the corresponding problem in (the multiplicative group of nonzero elements of) the underlying finite field. Thus keys in elliptic curve cryptography can be chosen to be much shorter for a comparable level of security.

VII. NTRU Encryption Techniques

In this section, we present the algorithm that is designed as having 6 classes:

(i) **KeyGenerator**: responsible for generating public and private keys.
(ii) **Encoder**: responsible for encoding.

(iii) **Decoder**: responsible for decoding.
(iv) **PolynomialOperations**: responsible for polynomial operations such as multiplication and inversion.
(v) **RandPolyGenerator**: responsible for construction of random polynomial.
(vi) **Analyzer**: contains test routines.

It is an open source and patented public-key cryptosystem which uses lattice-based cryptography for encryption and decryption of files. The two keys used in this algorithm are: public key and private key. The key is used for the encryption is Public Key or to verify the digital signature but private key is used for decryption or to create digital signature, as shown in Fig.5

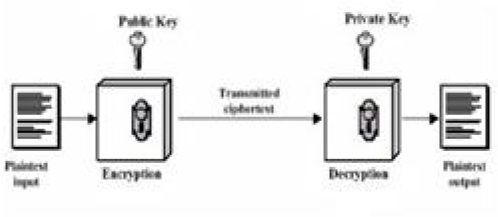

Fig.5 Working of NTRU algorithm [10]

It is based on polynomial arithmetic; therefore it provides very fast computation for the encryption and decryption of the message. NTRU has less complexity i.e. O(N2).

The main characteristics of NTRU algorithm are low computational and memory requirements for providing a high level security. In this algorithm the difficulty is faced during the factorisation of the polynomials into two different polynomials having very less coefficients NTRU is a widely usable, well-accomplished and promising cryptosystem.

VIII. COMPARISON OF DIFFERENT METHODS

Sr. No.	Paper Title	Method Used	Advantage	Disadvantage
1.	AODV Routig in VANET for Message Authentication Using ECDSA	ECDSA for message authentication with aodv	Provides better message authentication	Takes longer time for sign generation for large files
2.	SECURITY AWARE ROUTING PROTOCOL FOR MANET USING ASYMMETRIC CRYPTOGRAPY USING RSA ALGORITHM	RSA algorithm	Prevents misuse of data and data loss	Takes longer time for encryption, decryption
3.	Implementing Authentication Mechanism using Extended Public Key Cryptography in Wireless Network	Hybrid Cryptography	Malicious node is rejected	Performance evaluation needs to be carried out
4.	Application of NTRU Cryptographic Algorithm for SCADA(Supervisory Control and Data Acquisition) security	NTRU encryption technique	Performance is 2 to 35 times faster than RSA and can withstand attacks like brute force, man in the middle	Yet to be implemented in VANET
5.	A Comparative Analysis & Enhancement of NTRU Algorithm for Network Security	Enhanced NTRU	Requires less memory, less storage	Key size is to be increased to increase the security which degrades performance

	and Performance Improvement			

VIII. CONCLUSION

Vehicles are becoming a part of the global network. They could benefit from spontaneous wireless communications in a near future, making VANET a reality. Vehicular networks will not only provide safety and life saving applications, but they will become a powerful communication tool for their users. Hence, there is required a powerful security to be integrated with the VANET environment in order to have efficient communication.

ACKNOWLEDGMENT

This work is a combined effort of me and my guide professor Jay Amin who helped me in this work by giving his deep knowledge about the security of vehicular ad-hoc network. Without his guidance it wouldn't have been possible for me to survey this paper.

REFERENCES

[1] Kalkundri Ravi, Kalkundri Praveen, "AODV Routing in VANET for Message Authentication Using ECDSA", IEEE, ISBN:978-1-4799-3357-0, April 2014, pp. 1389-13893.

[2] Lu Chen, Hongbo Tang, Junfei Wang, "Analysis of VANET Security Based on Routing Protocol Information", IEEE, June 2013, pp. 134-138.

[3] Rashmi Jha, Anil Kumar saini, "A Comparative Analysis & Enhancement of NTRU Algorithm for Network Security and Performance Improvement", IEEE, 3-5 June 2011, pp. 80-84.

[4] Ravinder Kaur, Dr. Neeraj Sharma, "A Node Authentication Mechanism to Enhance the Security in VANETs", IJETER Vol.1 Issue 2, ISSN: 2454-6410, July 2015, pp. 16-22.

[5] Amritha Puliadi Premnath, Ju-Yeon Jo, Yoohwan Kim, "Application of NTRU Cryptographic Algorithm for SCADA security", IEEE, ISBN: 978-1-4799-3187-3, 7-9 April 2014, pp. 341-346.

[6] Navroop Kaur, Harjit Singh, Amandeep Nagpal, "Pros and Cons: Various Routing Protocols based on VANET's: A Survey", IJCA Vol. 106 No.8, Nov. 2014, pp. 40-43.

[7] Ram Shringar Raw, Manish Kumar, Nanhay Singh, "SECURITY CHALLENGES, ISSUES AND THEIR SOLUTIONS FOR VANET", IJNSA Vol.5 No.5, Sept. 2013, pp. 95-105.

[8] Yue Liu, Jun Bi, Ju Yang, "Research on Vehicular Ad Hoc Networks", IEEE, 2009, pp. 4430-4435.

[9] Shilpi Dhankhar, Shilpy Agrawal, "VANETs: A Survey on Routing Protocols and Issues", IJIRSET Vol.3 Issue 6, ISSN: 2319-8753, June 2014, pp. 13427-13435

[10] Amandeep Kaur Gill, Charanjit Singh, "Implementation of NTRU Algorithm for the Security of N-Tier Architecture", IJCSIT Vol. 5 No. 6, ISSN: 0975-9646, 2014, pp. 7631-7636.

[11] DEESHA G. DEOTALE & UMA NAGARAJ, "SURVEY OF VEHICLE AD-HOC NETWORK", IJCNS Vol. 1 Issue 4, ISSN: 2231-1882, 2012, pp. 86-90.