SECURITY ISSUES AND SOLUTIONS IN VEHICULAR ADHOC NETWORK : A REVIEW APPROACH

Ram Shringar Raw[1], Manish Kumar[1], Nanhay Singh[1]

Ambedkar Institute of Advanced communication Technologies & Research, Delhi, India
rsrao08@yahoo.in, www.mankumar@gmail.com, nsingh1973@gmail.com

ABSTRACT

Vehicular networks are the promising approach to provide safety to the drivers. It becomes a key component of intelligent transport system. A lot of research work has been done towards it but security issue got less attention. In this article we discuss about the VANET, it's technical and security challenges. We also discuss some major attacks and solutions that can be implemented against these attacks. We compare the solution on different parameters and lastly discuss the mechanisms that are used in the solutions.

KEYWORDS

VANET, MANET, VANET architecture, security, attacks.

1. INTRODUCTION

Now days, the sheer volume of road traffic affects the safety and efficiency of road traffic environment. Approx 1.2 million people are killed every year on the road accidents. Road traffic safety has been the challenging issue in traffic management. One possible way is to provide the traffic information to the vehicles so that they can use them to analyse the traffic environment. It can be achieved by exchanging the information of traffic environment among vehicles. All the vehicles are mobile in nature, hence a mobile network is needed which can be self organised and capable of operating without infrastructure support. With the progress of microelectronics, it becomes possible to integrate node and network device into single unit and wireless interconnection, i.e. ad hoc network. Further this network is evolved as Mobile Ad hoc Network (MANET) [1].

VANET is an application of mobile ad hoc network. More precisely a VANET is self-organised network that can be formed by connecting vehicle aiming to improve driving safety and traffic management with internet access by drivers and programmers. Two types of communication are provided in VANET.

First a pure wireless ad hoc network where vehicle to vehicle communication is possible without any support of fixed infrastructure. Second is communication between the road side units (RSU), a fixed infrastructure and vehicle. Each node in VANET is equipped with two types of unit i.e. On Board Unit (OBU) and Application Unit (AU). OBU has the communicational capability whereas AU executes the program making OBU‘s communicational capabilities. An RSU can be

David C. Wyld (Eds) : ICCSEA, SPPR, CSIA, WimoA - 2013
pp. 339–347, 2013. © CS & IT-CSCP 2013 DOI : 10.5121/csit.2013.3535

attached to the infrastructure network which is connected to the Internet [2]. Figure 1 describes C2C-CC architecture of VANET.

To establish a VANET, IEEE has defined the standard 802.11p or 802.16 (WiMax). A Dedicated Short Range Communication (DSRC) is proposed which is operating on 5.9GHz band and uses 802.11 access methods. It is standardised as 802.11p which provides short range communication with low latency. USA has allocated 75MHz of spectrum in the 5.9GHz band for DSRC to be used by Intelligent Transportation Systems (ITS). Also, Europe has allocated 30 MHz of spectrum in the 5.9GHz band for ITS [3].

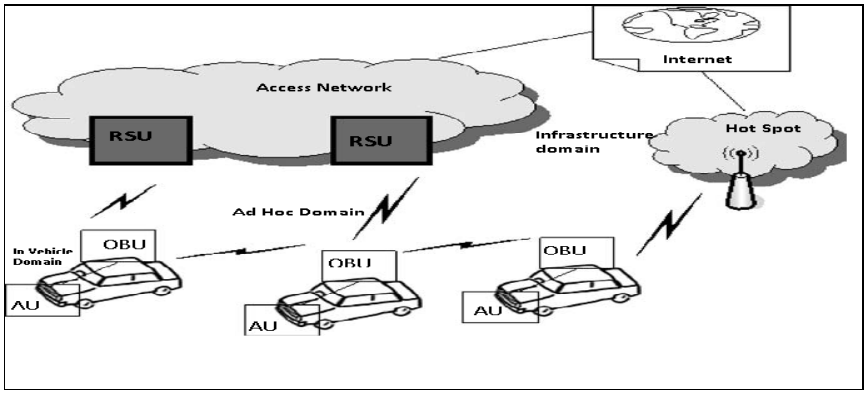

Fig 1. C2C-CC reference architecture [2]

Some protocols are being developed by the other groups also. NOW (Network On Wheels), which is associated with Car-2-Car Consortium has developed some protocols. Ford and General Motors have also created a Crash Avoidance Metric Partnership (CAMP) [4] in order to improve the VANET services.

The ultimate goal of all works toward VANET is to provide road safety information among the nodes hence the frequent exchange of such type of data on the network clearly signifies the role of the security. Any successful attack can cause loss of lives or financial lose. Hence the security of the information in VANET is crucial. In this paper, we discuss the security challenges and major attacks on VANET and also discuss the existing solution for these attacks.

The rest of the paper is organized as follows: The VANET applications and characteristics are described in section 2. Section 3 presents challenging issue in VANET. In section 4 presents security issues in VANET. Solution of previously defined attacks is described in section 5. Section 6 gives discussion and opinion on security and attacks in VANET. Finally section 7 concludes the paper.

2. CHARACTERISTICS OF VEHICULAR ADHOC NETWORK

VANET is an application of MANET but it has its own distinct characteristics which can be summarised as:

- **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 [2].
- **Rapidly changing network topology:** Due to high node mobility and random speed of vehicles, the position of node changes frequently. As a result of this, network topology in VANETs tends to change frequently.

- **Unbounded network size:** VANET can be implemented for one city, several cities or for countries. This means that network size in VANET is geographically unbounded.
- **Frequent exchange of information:** The ad hoc nature of **VANET** motivates the nodes to gather information from the other vehicles and road side units. Hence the information exchange among node becomes frequent.
- **Wireless Communication:** VANET is designed for the wireless environment. Nodes are connected and exchange their information via wireless. Therefore some security measure must be considered in communication.
- **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.
- **Sufficient Energy:** The VANET nodes have no issue of energy and computation resources. This allows VANET usage of demanding techniques such as RSA, ECDSA implementation and also provides unlimited transmission power.
- **Better Physical Protection:** The VANET nodes are physically better protected. Thus, a VANET node is more difficult to compromise physically and reduces the effect of infrastructure attack.

3. CHALLENGING ISSUE IN VANET

Although the characteristics of VANET distinguishes it a different network but some characteristics imposes some challenges to deploy the VANET. These challenges can be categorised into following categories [6]:

3.1 Technical Challenges

The technical challenges deals with the technical obstacles which should be resolved before the deployment of VANET. Some challenges are given below:

- **Network Management:** Due to high mobility, the network topology and channel condition change rapidly. Due to this, we can't use structures like tree because these structures can't be set up and maintained so rapidly as the topology changed.
- **Congestion and collision Control**: The unbounded network size also creates a challenge. The traffic load is low in rural areas and night in even urban areas. Due to this, the network partitions frequently occurs while in rush hours the traffic load is very high and hence network is congested and collision occurs in the network.
- **Environmental Impact:** VANETs use the electromagnetic waves for communication. These waves are affected by the environment. Hence to deploy the VANET the environmental impact must be considered.
- **MAC Design:** VANET generally use the shared medium to communicate hence the MAC design is the key issue. Many approaches have been given like TDMA, SDMA, and CSMA etc. IEEE 802.11 adopted the CSMA based MAC for VANET.
- **Security:** As VANET provides the road safety applications which are life critical therefore security of these messages must be satisfied.

3.2 Social and Economic Challenges

Apart from the technical challenges to deploy the VANET, social and economical challenges should be considered. It is difficult to convince manufacturers to build a system that conveys the traffic signal violation because a consumer may reject such type of monitoring. Conversely, consumer appreciates the warning message of police trap. So to motivate the manufacturer to deploy VANET will get little incentive.

4. SECURITY ISSUES IN VANET

Among all the challenges of the VANET, security got less attention so far. VANET packets contains life critical information hence it is necessary to make sure that these packets are not inserted or modified by the attacker; likewise the liability of drivers should also be established that they inform the traffic environment correctly and within time. These security problems do not similar to general communication network. The size of network, mobility, geographic relevancy etc makes the implementation difficult and distinct from other network security

4.1 Security Challenges in VANET

The challenges of security must be considered during the design of VANET architecture, security protocols, cryptographic algorithm etc. The following list presents some security challenges [2]:

- **Real time Constraint**: VANET is time critical where safety related message should be delivered with 100ms transmission delay. So to achieve real time constraint, fast cryptographic algorithm should be used. Message and entity authentication must be done in time.

- **Data Consistency Liability**: In VANET even authenticate node can perform malicious activities that can cause accidents or disturb the network. Hence a mechanism should must be designed to avoid this inconsistency. Correlation among the received data from different node on particular information may avoid this type of inconsistency.

- **Low tolerance for error**: Some protocols are designed on the basis of probability. VANET uses life critical information on which action is performed in very short time. A small error in probabilistic algorithm may cause harm.

- **Key Distribution:** All the security mechanisms implemented in VANET dependent on keys. Each message is encrypted and need to decrypt at receiver end either with same key or different key. Also different manufacturer can install keys in different ways and in public key infrastructure trust on CA become major issue. Therefore distribution of keys among vehicles is a major challenge in designing a security protocols.

- **Incentives:** Manufactures are interested to build applications that consumer likes most. Very few consumers will agree with a vehicle which automatically reports any traffic rule violation. Hence successful deployment of vehicular networks will require incentives for vehicle manufacturers, consumers and the government is a challenge to implement security in VANET.

- **High Mobility:** The computational capability and energy supply in VANET is same as the wired network node but the high mobility of VANET nodes requires the less execution time of security protocols for same throughput that wired network produces. Hence the design of security protocols must use the approaches to reduce the execution time. Two approaches can be implementing to meet this requirement.

    - *Low complexity security algorithms:* Current security protocols such as SSL/TLS, DTLS, WTLS, generally uses RSA based public key cryptography. RSA algorithm uses the integer factorisation on large prime no. which is NP-Hard. Hence decryption of the message that used RSA algorithm becomes very complex and time consuming. Hence there is need to implement alternate cryptographic algorithm like Elliptic curve

cryptosystems and lattice based cryptosystems. For bulk data encryption AES can be used.

- *Transport protocol choice:* To secure transaction over IP, DTLS should be preferred over TLS as DTLS operates over connectionless transport layer. IPSec which secures IP traffic should be avoided as it requires too many messages to set up. However IPSec and TLS can be used when vehicles are not in motion.

4.2 Security requirements in VANET

VANET must satisfy some security requirements before they are deployed. A security system in VANET should satisfy the following requirements [5]:

- **Authentication**: Authentication ensures that the message is generated by the legitimate user. In VANET a vehicle reacts upon the information came from the other vehicle hence authentication must be satisfied.
- **Availability**: Availability requires that the information must be available to the legitimate users. DoS Attacks can bring down the network and hence information cannot be shared.
- **Non-Repudiation**: Non-repudiation means a node cannot deny that he/she does not transmit the message. It may be crucial to determine the correct sequence in crash reconstruction.
- **Privacy**: The privacy of a node against the unauthorised node should be guaranteed. This is required to eliminate the massage delay attacks.
- **Data Verification**: A regular verification of data is required to eliminate the false messaging.

4.3 Attacks in the VANET

To get better protection from attackers we must have the knowledge about the attacks in VANET against security requirements. Attacks on different security requirement are given below [7]:

- **Impersonate:** In impersonate attack attacker assumes the identity and privileges of an authorised node, either to make use of network resources that may not be available to it under normal circumstances, or to disrupt the normal functioning of the network. This type of attack is performed by active attackers. They may be insider or outsiders. This attack is multilayer attack means attacker can exploit either network layer, application layer or transport layer vulnerability.
- **Identity revealing**: Generally a driver is itself owner of the vehicles hence getting owner's identity can put the privacy at risk.
- **Location Tracking**: The location of a given moment or the path followed along a period of time can be used to trace the vehicle and get information of driver.
- **Repudiation:** The main threat in repudiation is denial or attempt to denial by a node involved in communication. This is different from the impersonate attack. In this attack two or more entity has common identity hence it is easy to get indistinguishable and hence they can be repudiated.
- **Eavesdropping** is a most common attack on confidentiality. This attack is belongs to network layer attack and passive in nature. The main goal of this attack is to get access of confidential data.
- **Denial of Service:** DoS attacks are most prominent attack in this category. In this attack attacker prevents the legitimate user to use the service from the victim node.

5. SOLUTION OF PREVIOUSLY DEFINED ATTACKS

There are many solutions provided to mitigate these attacks. We have taken five solutions that are most effective for above mentioned attack. Following are their descriptions:

5.1 ARAN (Authenticated Routing for Ad hoc network)

In [9], B. Dahill et al proposed a secure routing protocol for ad hoc network based on authentication. This is based on AODV but it prevents from attacks including spoofing. ARAN uses the public key cryptography and requires a certificate server whose public key is known to all nodes. It uses timestamp for the freshness of the route. A source node broadcasts the route discovery packet (RDP) to all its neighbours for route discovery. Each node keeps the record of its neighbour from which it receives the message. After receiving the message all the neighbour again forwards this message to their neighbours with their sign and own certificate. When the message received by the destination, it replies to the first node from which it received the message. No intermediate node can reply the RDP other then destination even if that intermediate node knows the path of destination. The destination node unicasts the reply (REP) in reverse from destination to the source. All REP is signed by the sender and checked by the next hop.

For the shortest path, the source begins with the encrypted shortest path confirmation (SPC) message and broadcasts it to its neighbour. Destination node replies with the recorded shortest path (RSP) to the source through its predecessor. Each neighbour signs the encrypted part of the message and attach its certificate. ARAN requires that each node must keep one routing table for each node in a network. When no traffic is found on node in lifetime it is simply deactivated from the table. If data is received on inactive route, the error message ERR is generated which travels through reverse path of the source. If a node is broken due to the node movement, the ERR message is generated.

5.2 SEAD (Secure and Efficient Ad hoc Distance Vector)

In [10], proposed a new secure routing protocol which protects against multiple uncoordinated attackers who creates incorrect routing in any other node. It is based on the Destination-sequenced Distance Vector (DSDV) routing. SEAD supports the node which has limited CPU processing capability and protects from the DoS attack in which attackers attempts to consume excess network bandwidth. It uses the one way hash function rather than more expensive asymmetric cryptographic operation. It uses destination-sequence number to avoid the long lived routing loop and also protects from replay attack as the destination-sequence number provide the freshness of the packet.

5.3 SMT (Secure Message Transmission)

P. Papadimitratos et al [11] proposed Secure Message Transmission protocol which is light weight and operates on end to end manner. It requires a security association between source and destination. It does not use the cryptographic operation for intermediate nodes.

The source first discovers the path through existing route discovery protocol and determines the initial Active Path Sets (APS) for communication. After completion of this a source have a set of APS. The source disperses the each outgoing messages into a number of pieces and encodes and transmits across different routes. Each dispersed piece carries a MAC (Message Authentication Code) which is used to check the integrity and authentication of its origin. Based on the packet received or failed on different APS, the source node rates the APS path. The destination validates and sends a feedback acknowledgement to the source.

5.4 NDM (Non-Disclosure Method)

A. Fasbender [12] et al proposed this method to protect location information in mobile IP. They resolved the problem of traffic analysis and location disclosure. The NDM approach assumes a number of independent Security agents and each SA uses the public and private key pairs. Hence this approach is based on asymmetric cryptography. In this approach a sender sends the message to the receiver without disclosing any location information. Communication between sender and receiver is performed via SAs. Each SA_i knows the address of AS_{i-1} and $AS_{i+1.}$. Sender sends the message to SA_1, and then SA_1 sends it to SA_2 and so on. Each SA encapsulates the message with its public key. But attacker can trace the message by their length during communication hence a variable padding scheme is also introduced.

5.5 ARIADNE

Y. Chun Hu et al [13] proposed a routing protocol which prevents the attacker from terming the routes of uncompromised nodes and DoS attacks. This approach is based on on-demand routing like DSR. It uses highly efficient symmetric cryptography. In this approach sender and receiver agrees on two keys say K_{SR} and K_{RS} for sender to receiver and receiver to sender respectively using MAC. To authenticate the route request the sender sends the message containing unique data like timestamp and calculates the MAC for this and sends to receiver using $K_{SR..}$ MAC, Digital signature, and TESLA can be used for data authentication in routing message.

we have discussed some important solutions . Table 1 gives the comparison among all solutions.

Table 1. Comparison of solutions

Sr No	Solution	Attacks Covered	Technology used	Security requirements
1	ARAN	1. Replay Attack 2. Impersonation 3. False Warning	1. Cryptographic Certificate	1. Authentication 2. Message Integrity 3. Non-Repudiation
2	SMT	1. Information Disclosure	1. MAC (Message Authentication Code)	1. Authentication
3.	SEAD	1. DoS 2. Routing Attack 3. Resource Consumption	1. One Way Hash Function	1. Availability 2. Authentication
4.	NDM	1. Information Disclosure 2. Location Tracking	1. Asymmetric Cryptography	1. Privacy
5.	ARIADNE	1. DoS 2. Routing Attack 3. Replay Attack	1. Symmetric Cryptography 2. MAC	1. Authentication

6. DISCUSSION AND OPINION

The study of attacks revealed that the attacker generally targets the network layer directly or indirectly hence the routing protocol must be secure enough to prevent the most types of attacks. Each solution must preserve the security requirements like authentication, integrity, and privacy which are more targeted. Since vehicular network is managed by the different operators hence authentication must be required not only for V-V communication but also in V-I and administrative domain. Solutions also used the different cryptographic algorithms broadly categorised into Symmetric and Asymmetric.

The symmetric algorithms are efficient and takes less CPU time but the complexity of generation of key of this algorithm is O (n2) where n is the number of nodes in network[14]. Also the key distribution is the major issue in this approach. When the network becomes larger then symmetric approach will require more no. of space to store keys which are not used when network becomes sparse

In asymmetric approach the complexity becomes O (n) since only one private and public key pair is required for any node [14]. However these algorithms require more execution time and produce the message delay. Since VANET have enough computational power to execute these complex algorithms hence this is not a big deal. Therefore asymmetric cryptography can be applied in VANET.

By using Asymmetric cryptography Digital Signature has been also introduced for authentication and non-repudiation. However this method also requires more computational power to encrypt, decrypt and making signature.

Another approach PKI (Public Key Infrastructure) has been used by different protocols to authenticate the node. In this approach central authority called CA (Certificate Authority) issues the certificate to all nodes. The certificate contains the information about the keys, certificate no. etc and it is signed by the CA. Whenever a node wants to authenticate the node it only authenticates the certificate from the CA. Maxim Raya et al proved this approach can be applied into VANET but certificate revocation is the major issue to implement this approach.

Some protocol like SEAD, SMT used the MAC or Hash function for authentication. This Mechanism is faster than all mechanisms with respect to encryption and decryption.

Apart from traditional mechanism some newer approach also takes the attention of the researchers. Some of them are Elliptic Curve Cryptography (ECC) and NTRU .ECC [16] has been adopted by the many research groups. The use of ECC makes the algorithm secure and faster enough even the key length is less. NTRU cryptosystem [17] is recently adopted by IEEE P1363 working group. It is a asymmetric cryptosystem having quantum computing resistance. It is faster than both RSA and ECC in signing and verification [5].

These cryptosystems are only used for privacy and authentication mainly but availability remains the major issue to solve. This attack is multi-layer attack hence from physical to network layer should implement different mechanism like physical layer may use FHSS (Frequency - Hopping Spread Spectrum) and DSSS (Direct Sequence Spread Spectrum) where as a secure routing protocol can be used to avoid the DoS attack.

7. CONCLUSION

Security is the major issue to implement the VANET. In this article, we study the security requirements and challenges to implement the security measure in the VANET. Different types of attacks and their solutions are also discussed. We discuss some technologies which are used in the different solutions. Among all requirements authentication and privacy are the major issues in VANET. However confidentiality is not required in VANET because generally packets on the network do not contain any confidential data.

REFERENCES

[1] S. Sesay, Z Yang and Jianhua He, "A survey on Mobile Ad Hoc Network", Information Technology Journal 3 (2), pp. 168-175, 2004

[2] Moustafa,H., Zhang,Y.: Vehicular networks: Techniques, Standards, and Applications. CRC Press, (2009).

[3] Yaseer Toor et al., "Vehicle Ad Hoc Networks : Applications and Related Technical issues", IEEE Communications surveys & Tutorials , 3rd quarter 2008, vol 10, No 3,pp. 74-88.

[4] Y.- C. Hu and K. Laberteaux, "Strong Security on a Budget," Wksp. Embedded Security for Cars, Nov. 2006; http://www.crhc.uiuc.edu/~yihchun/

[5] Maxim Raya e al., "The Security of Vehicular Ad Hoc Networks", SASN'05, Nov 7 2005, Alexandria, Verginia, USA, pp. 11-21

[6] Hannes Hartenstein et al., "A tutorial survey on vehicular Ad Hoc Networks" , IEEE Communication Magazine, June 2008, pp. 164-171

[7] Jose Maria de Fuentes, Ana Isabel Gonzalez-Tablas, and Arturo Ribagorda, "Overview of Security issues in Vehicular Ad Hoc Networks", Handbook of Research on Mobility and Computing, 2010.

[8] Murthy, C. S. R.,Manoj, B. S.: Ad Hoc Wireless Networks: Architectures and Protocols. PEARSON,ISBN 81-317-0688-5, (2011).

[9] Dahill, B. N. Levine, E. Royer and Clay Shields, "A Secure Routing Protocol for Ad Hoc Networks", Proceeding of IEEE ICNP 2002, pp 78-87, Nov 2002.

[10] Y. C. Hu, D. B. Johnson and A. Perrig, "SEAD: Secure efficient distance vector routing for mobile wireless ad hoc networks", Elsevier B. V. , pp 175-192, 2003

[11] P. Papadimitratos and Z. J. Haas, "Secure Data Transmission in Mobile Ad Hoc Network", ACM Workshop on Wireless Security, San Diego , CA, September 2003.

[12] Fasbender, D. Kesdogan and O. Kubitz, "Variable and Scalable Security: Protection of Location Information in Mobile IP", IEEE VTS , 46th Vehicular Technology Conference, USA, 1996.

[13] Y. C. Hu, A. Perrig and D. B. Johnson, "Ariadne: A Secure On-Demand Routing Protocol for Ad Hoc Networks", MobiCom'02, pp. 23-26,2002

[14] Fonseca and A. Festag, "A survey of Existing Approaches for Secure Ad Hoc Routing and Their Applicability to VANETS", NEC Network Laboratories, 2006.

[15] Xiaodong Lin et al., "Security in Vehicular Ad Hoc Network", IEEE communications magazine , April 2008, pp. 88-95

[16] Menezes, S. Vanstone, and D. Hankerson, "Guide to elliptic curve cryptography", Springer Professional Computing (Springer, New York 2004).

[17] J. Hof fstein, J. Pipher, J. H. Silverman, "NTRU: A ring- based public key cryptosystem", Lecture Notes in Computer Science, Vol. 1423, 1998, pp 267-288.