Covert Communication in VANETS using Internet Protocol Header Bit

Kimi Manchanda
M.Tech Research Scholar
Department Of CSE
ACET,Amritsar

Amarpreet Singh
Associate Professor
Department of CSE
ACET,Amritsar

ABSTRACT
Moving into the VANET (Vehicular adhoc network) makes very beneficial for the vehicles to converse with each other and every node (vehicles) present in the VANET through Intelligent Transport System (ITS). In today's scenario, Security is a big issue in adhoc networks because adhoc are wireless as like VANETS. VANETS are more prone to attacks due to mobility of the vehicles. Privacy, security and authenticity are some of the required application that is essential before the vehicular adhoc networks are deployed. way. So, to counter such problem, this paper proposes a new scheme that makes use of Covert Channels to secure the data from third party which is also a part of that network.

Keywords
Covert Channel, VANET, ITS, Adhoc, Overt**,** Subliminal Channel, Steganography.

1. INTRODUCTION
In VANET, the communication is done through the Intelligent Transport System (ITS). All the communications between the vehicles are handled by On-Board Unit (OBU). To provide security in the VANET adhoc network, the implementing the security techniques for this purpose. There are many techniques to provide the security of sharing of undisclosed information from the third party.

1.1 Why do VANET need security
VANET networks need security of data between two nodes from the intimidation of leaking the secret information to the unauthorized party. This paper lights to what is the need of security in VANET with the help of an example:

Suppose in the VANET networks, there are vehicles or nodes which are categorised into three types according to their profile.

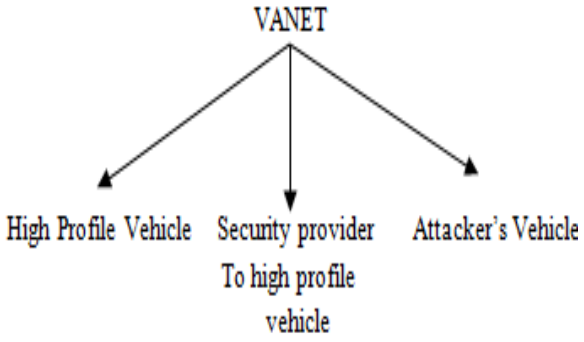

Fig 1: Classification of Vehicles According To Their Rank

1.1.1 High Profile
High profile vehicle within a VANET is one that carries some delegate/sensitive entity (suppose any Minister).

1.1.2 Security provider
The vehicle of security provider (suppose security pilot) is that which is going in the same network for providing the security to High profile vehicle. This is also the part of same network.

1.1.3 Invader
Invader's vehicle is that which a part of the same network is also.

1.2 Threat Scenario
When the high profile vehicle and the security provider vehicle communicates some sensitive information in the network then the third party or the attacker's vehicle can access that information which is transferred between high profile and security provider vehicle and can use this information as a tool to cause some dreadful destructive work.

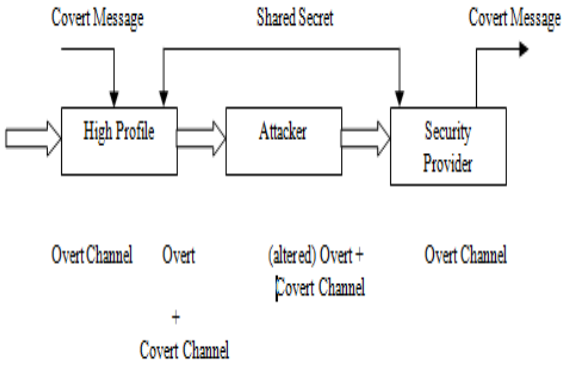

Fig 2: Covert Channel Communication

To prevail over from this problem, some security measures have to be implemented for ceasing the leakage of information between two parties.

1.3 Types of Security Techniques
There are various types of security techniques to overcome the problem of data sharing.

1.3.1 Encryption
Encryption is the technique used for security intention. In encryption, the data has to be sent is referred to as plain text and this type of text is encrypted using an encryption algorithm. Then that text is known as Cipher text. The receiver uses the decoding algorithm for decrypting the text. But the encryption technique doesn't prevent hacking. The

efficient hacker can read the data without any problem.

1.3.2 Steganography

Steganography can be used to conceal the critical data and prevent them from illegal and direct access[1] by the invader. Steganography of data can be done in various ways:

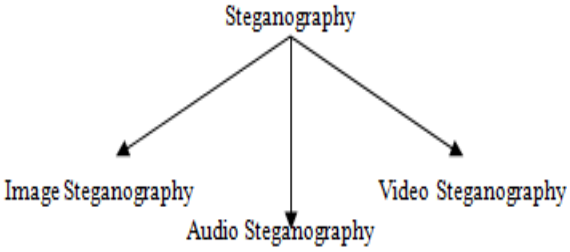

Fig 3: Ways of Steganography Done on Data

1.3.3 Cryptography

In the cryptography technique, there is a division of users in two levels; Level 1 and Level 2. The users of Level 1 have access to their own private encrypted data and unclassified public data, whereas Level 2 users have access to their own private data and also classified data which is stored in an encrypted form.

1.3.4 Hashing

In Hashing, the variable length data is distorted into a fixed length data using hash functions which can't be access by the third party with all these security techniques.

Though above discussed techniques are useful to secure sensitive information but they have one or the other limitation. In the encryption technique, the data is easily hacked by the invaders by decrypt the code easily because in this technique data is encoded in some other language and the invader noticed that some data is transferred in some encoded form. With the help of man-in-the middle attack attacker attacks on the secret files and decrypt them. In case of steganography, the disadvantage is that the when the original images are altered to encrypted image then Message is hard to recover if image is subject to attack such as translation and rotation. In this technique it causes scratch to picture appearance. This can be easy to detect because Message easily lost if picture subject to compression such as JPEG. This paper throws light on another technique named as Covert Channel.

1.3.5 Covert Channels

A covert channel is a logical link between two authenticated systems through which they can secretly exchange information without being detected by the third party or attacker. This channel remains untraceable by the intermediators. Secret information is embedded in the legitimate channel packets by the sender and the receiver retrieves this information from the message packet. The third party is unable to detect this data transfer through the legal channel packets.

According to the Lampson in 1973[30], Covert Channels that was not intended for communication between the two processes. It was authoritative to communicate, but not the way they actually are.

According to Murdoch [31], a covert channel can be described as a communication in a mainframe system where the sender and the receiver plan to leak information over a channel which is not designed for that communication to take place, in violation of a required access control policy.

A covert channel is a double sword communication system because they have legal use also. At one time to a particular entity, in a communication it may acts as threat and on the other hand it can be used as subversive means of achieving privacy and overtly transfer the data between the two authorized parties. The communication can be done secretly without surveillance by the attacker that is present in the entire network. It exchanges information, without changing any firewalls or invaders detectors on the network which provides an additional layer of security to that provided by the different layers of protocol stacks.

2. HOW COVERT CHANNEL CAN BE ESTABLISHED

Communication can be done steadily in the VANET network with the establishment of Covert channels between those nodes. If the covert channel is established in the VANET network, then the security is maintained between High profile vehicle and Security provider vehicle and can share secret data covertly with each other and the attacker or you can say that the other vehicles that are present in this network can't detect the covert channels. Covert channels can be established into two ways:

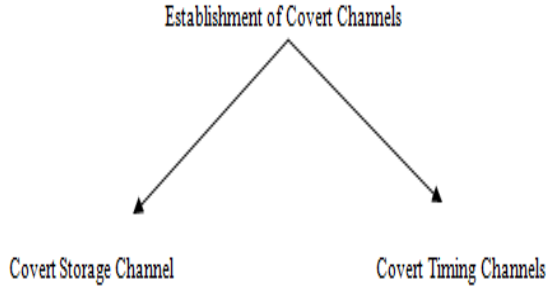

Fig 4 : Ways For Establishing The Covert Channels

2.1 Covert Storage Channels

In the Covert Storage Channel, it involves the storage of data in any spot by one node present in the VANET and can be read by another node in the network. In the Storage Covert Channels, the data is stored in the form of objects[3]. Objects need memory location for the storage purpose. Storage channels mainly use two aspects for embedding the covert data.

2.1.1 Object Attributes

The data that is to be embedded secretly which has properties about the files, files are used for storage channels.

2.1.2 Resources which are sharable

The resources like blocks, physical memory, I/O buffers such as printers and plotters can be used as storage channels.

2.2 Timing Covert Channels

Timing channels involve the signalling information by adapt the use of resource over time such as the receiver can receive the information, monitor it and decipher this information.

Timing Channels can be classified into two categories:

2.2.2 Active

Timing channels that need an supplementary connection to relocate covert data. The throughputs of active timing channel are very high compared to Passive.

2.2.3 Passive

There is no need of an extra connection for transferring the

covert data. It uses an existing connection. The data can't be detected easily when the data is embedded into it.

3. BACKGROUND AND RELATED WORK

In the existing work, the communication channel which is used for secure data communication always is in secret mode. The Flow Chart of existing work is as shown in Fig. 5 above.

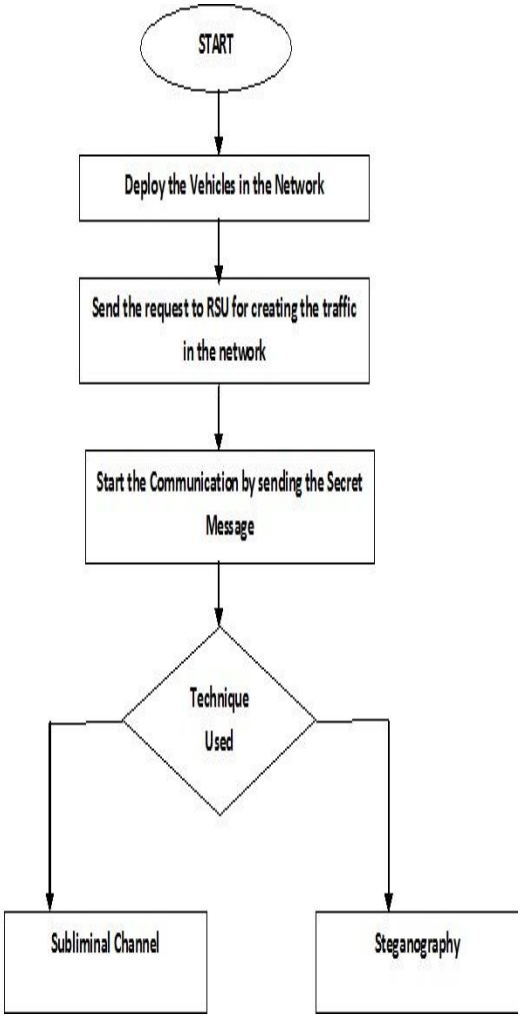

Fig 5: Flow Chart of the Existing Technique

It uses two secure mode options named as stegnaography and subliminal channels. In both the options the sensitive information that the sender wants to protect from eavesdropper is in secure mode. In the subliminal channel the information is entrenched in to the messages that can be used to exchange the information over the insecure network. In the steganography technique there is amendment of messages by varying the least significant bits for hiding the information that can be transmitted over the network

4. PROBLEM STATEMENT

To fulfill the above gap one has to encounter a new conception of transmitting the secure data with the covert channel communication. In this work the communication is going on with normal mode as well as secure mode. With the help of this covert communication the small amount of sensitive data is entrenched into the legal packet and transmitting over the insecure network. The attacker may be having watch on traffic and he/she will try to break the security. If the attacker will get success in breaking the security but in this case it is not sure that he will get sensitive data because one has to implement a dual mode channel in this work which is based on bit selection mode and the selection of bit is random in nature so the attacker is always in predicament to find the mode (i.e. the sender sends the data in normal or covert mode) of the data which is transmitted over the secure channel. In this work, the probability of getting the sensitive data is very low.

5. PROPOSED WORK

To fulfill the above gap one has to encounter a new conception of transmitting the secure data with the covert channel communication. In this work the communication is going on with normal mode as well as secure mode. With the help of this covert communication the small amount of sensitive data is entrenched into the legal packet and transmitting over the insecure network. The attacker may be having watch on traffic and he/she will try to break the security. If the attacker will get success in breaking the security but in this case it is not sure that he will get sensitive data because one has to implement a dual mode channel in this work which is based on bit selection mode and the selection of bit is random in nature so the attacker is always in predicament to find the mode (i.e. the sender sends the data in normal or covert mode) of the data which is transmitted over the secure channel. In this work, the probability of getting the sensitive data is very low. The flow Chart of the proposed technique is as shown in fig.6 below:

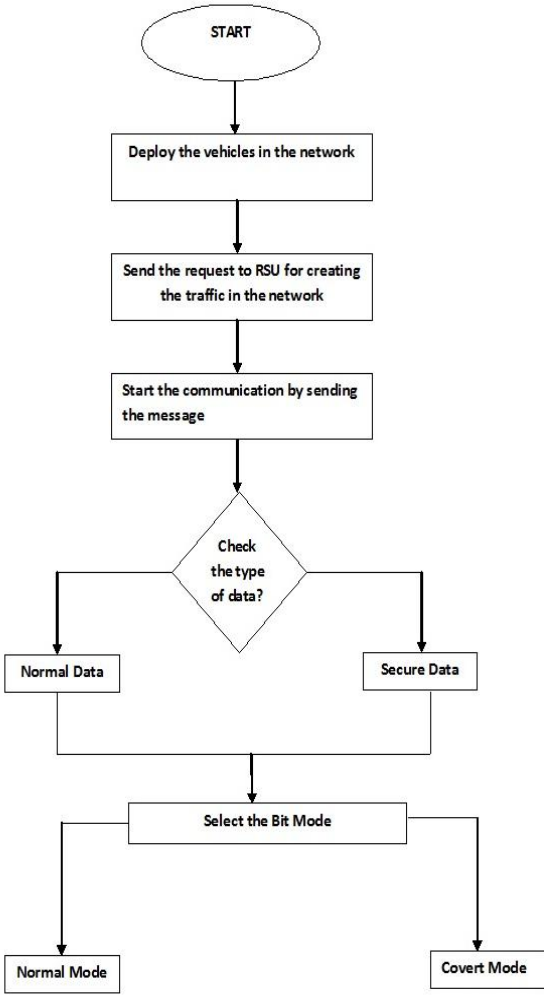

Fig 6: Flow Chart of the Existing Technique

6. CONCLUSION AND FUTURE WORK

In this paper, one has to present an inkling of how covert channels can be implemented in the VANET. In this paper, the discussion is on the different ways for the establishment of covert channels and also explored the ways for the data transfer in the covert channels. The future scope of this paper is to establishment of Bit selective mode storage covert channels in VANETs and also evaluate the parameters like End to End Delay, Throughput, Packet Drop and Packet delivery ratio in Normal mode as well as covert mode

7. REFERENCES

[1] Fuentes J, Blasco Jeorge , Isabel A., and Manzano L.," Applying Information Hiding in VANETs to Covertly Report Misbehaving Vehicles", International Journal of Distributed Sensor Networks Volume 2014, Article ID 120626, 15 pages

[2] Jose Maria de Fuentes, Jorge Blasco, Ana Isabel González-Tablas, and Lorena González-Manzano,'' Applying Information Hiding in VANETs to Covertly Report Misbehaving Vehicles'', International Journal of Distributed Sensor Networks Volume 2014 (2014), Article ID 120626, 15 pages.

[3] Ahmed Al-Haiqi, Mahamod Ismail, and Rosdiadee Nordin," A New Sensors-Based Covert Channel on Android", Department of Electrical, Electronic and Systems Engineering, National University of Malaysia (UKM), 43600 Bangi, Malaysia, Article ID 969628, 14 pages, Hindawi 2014.

[4] Vibhor Kumar Vishnoi, Sunil Kumar," Detection of TCP/IP Covert Channel based on Naïve-Bayesian Classifier", International Journal Of Engineering And Computer Science ISSN: 2319-7242 Volume - 3 Page No. 8312-8316,ICES 2014.

[5] Esther Palomar, Jose M. De Fuentes, Almudena Alcaide," Hindering false event dissemination with VANETS with proof-of-work mechanisms", Department of Computer Science, Elsevier 2014.

[6] Albert Wasef and Xuemin (Sherman) Shen," EMAP: Expedite Message Authentication Protocol for Vehicular Ad Hoc Networks", IEEE Transactions on Mobile Computing, vol. 12, no. 1, January 2013, IEEE 2013.

[7] Alexandre Viejo, Qianhong Wu, Josep Domingo-Ferrer,"Asymmetric homomorphisms for secure aggregation in heterogeneous scenarios",Information Fusion ,Elsevier 2013.

[8] Andreas Tomandl, Florian Scheuer and Hannes Federrath," Simulation-based evaluation of techniques for privacy protection in VANETs", 8th International Conference on Wireless and Mobile Computing, Networking and Communications (WiMob), IEEE 2012.

[9] Gadkari Mushtak Y, Sambre Nitin B. ,"Routing Protocols, Security Issues", ISSN: 2278-0661 Volume 3, Issue 3 (July-Aug. 2012), PP 28-38.

[10] Syeda Khairunnesa Samantha, Nusrat Nur Afrose Shoma, K. M. Azharul Hasan ,"An Approach for Alleviating the Starvation Problem in Road Side Units (RSUs)-based Vehicular Ad Hoc Networks (VANETs)", ISSN 2223-4985 Volume 2 No. 2, February 2012.

[11] Marco Di Felice , Luca Bedogni, Luciano Bononi," Group communication on highways: An evaluation study of geocast protocols and applications", Department of Computer Science, University of Bologna, Italy 1570-8705 , Elsevier 2012

[12] Huaqun Wang, Yuqing Zhan," On the Security of an Anonymous Batch Authenticated and Key Agreement Scheme for Value-Added Services in VANETs" International Workshop on Information and Electronics Engineering (IWIEE), 1735 – 1739, Elsevier 2012.

[13] Osama Abumansoor and Azzedine Boukerche," A Secure Cooperative Approach for Nonline-of-Sight Location Verification in VANET", IEEE Transactions on Vehicular Technology, Vol. 61, no. 1, January 2012, IEEE 2012.

[14] Paul Bijan, Ibrahim Md., Naser Bikas Md. Abu," VANET Routing Protocols.", International Journal of Computer Applications (0975 – 8887) Volume 20– No.3, April 2011.

[15] Khaleel Mershad and Hassan Artail," REACT: Secure and Efficient Data Acquisition in VANETs", 7th International Conference on Wireless and Mobile Computing, Networking and Communications (WiMob), IEEE 2011

[16] Luca Anchora, Luca Cason, Giovanni Ciccarese, Mario De Blasi, Pierluigi Marra, Cosimo Palazzo'' An Optimal Setting For The Parameters Of An Intelligent Flodding Scheme In VANETS'', European wireless Conference 2010 .

[17] Kumar Maurya Prashant, SharmaVaishali , Sahu Gaurav, Roberts Ashish, Srivatava Mahendra ,"An Overview of AODV Routing Protocol", International Journal Of Engineering And Computer Science, IJES 2009

[18] Steven J. Murdoch,'' Covert channel vulnerabilities in anonymity systems'', Cambridge University, December 2007.

[19] S. Zander, G. Armitage, and P. Branch, "Covert Channels in the IP Time To Live Field," Proc. Australian Telecommunication Networks and Applications Conf. (ATNAC), Dec. 2006.

[20] E. Cauich, R. Gómez Cárdenas, and R. Watanabe, "Data Hiding in Identification and Offset IP Fields," Proc. 5th Int'l. School and Symp. Advanced Distributed Systems (ISSADS), Jan. 2005, pp. 118–25.

[21] S. J. Murdoch and S. Lewis, "Embedding Covert Channels into TCP/IP," Proc. 7th Information Hiding Wksp., June 2005.

[22] M. C. Perkins, "Hiding out in Plaintext: Covert Messaging with Bitwise Summations," Master's thesis, Iowa State University, 2005.

[23] Ankita Agrawal1, Aditi Garg2, NiharikaChaudhiri3,Shivanshu Gupta4,DevesPandey5,TumpaRoy," Security onVehicularAd Hoc Networks (VANET)"

[24] A. Galatenko et al., "Statistical Covert Channels through PROXY Server," Proc. 3d Int'l. Wksp. Mathematical Methods, Models, and Architectures for Computer Network Security, Sept. 2005, pp. 424–29.

[25] J. Rutkowska, "The Implementation of Passive Covert Chan- nels in the Linux Kernel," Proc. Chaos

Communication Congress, Dec. 2004.

[26] H. Qu, P. Su, and D. Feng, "A Typical Noisy Covert Channel in the IP Protocol," Proc. 38th Annual Int'l. Carnahan Conf. Security Technology, pp. 189–92,Oct. 2004.

[27] S. Cabuk, C. E. Brodley, and C. Shields, "IP Covert Timing Channels: Design and Detection," Proc. 11th ACM Conf. Com- puter and Communications Security (CCS), Oct. 25–29, pp. 178–87, 2004.

[28] S. Bhadra, S. Shakkottai, and S. Vishwanath, "Communication Through Jamming Over a Slotted ALOHA Channel," Proc. 42nd Allerton Conf. Commun., Control, and Computing, Oct. 2004.

[29] K. Szczypiorski, "HICCUPS: Hidden Communication System for Corrupted Networks," Proc. 10th Int'l. Multi-Conf. Advanced Computer Systems, Oct. 2003, pp. 31–40.

[30] B. Lampson,"A note on Confinement problem", Communication pf the ACM, Vol. 16,no.10, Oct. 1973,pp. 613-615

[31] National Conference Security Center, US DoD, " Trusted Computer System Evaluation Criteria ",Tech. Rep. DOD 5200.28-STD, National Computer Security Center,Dec.1985, http://csrc.nist.gov/publications/history/dod85.pdf

[32] http://www.cs.ucf.edu

[33] http://www.it.ecei.tohoku.ac.jp