ISSN (Online) 2456 -1304

International Journal of Science, Engineering and Management (IJSEM)
Vol 2, Issue 12, December 2017

Data security in VANET Dissemination using advanced cryptographic Techniques

[1] G. Anitha, [2] K.Juliana GnanaSelvi
[1] Assistant Professor, [2] Associate Professor,
[1] Department of Computer Applications, Karpagam University
[2] Dept of Computer Science, Rathinam College of Arts And Science

Abstract:-- **Vehicular Ad Hoc Network is mainly used in safety applications to avoid road accidents by disseminating the alert messages or dangerous information among the drivers securely. This alert messages or dangerous information must be highly secured from the access of intruders or attackers. Misbehaviour or malicious node detection is a major problem in VANET if any vehicles disseminate the messages maliciously. Checking the variation in the behaviour of vehicular nodes, detection of misbehaviour and the malicious vehicular nodes continuously makes a highly secured VANET. In this paper, message dissemination using optimal blowfish algorithm based signcryption technique in vehicular networks is proposed to secure the data from the third party person or attackers.**

Keywords:-- **VANET, Data dissemination, Data Security, Sybil Attack, DOS, Signcryption, Blowfish, Cuckoo Search.**

1. INTRODUCTION

Vehicular Ad Hoc Network (VANET) becomes very popular in automatic industry to improve the safety and comfort travel in case of very high road traffic. It takes a lot of attention in the research area. VANETs may offer a various applications such as safety, traffic management, entertainment and infotainment. A Vehicular Ad Hoc Network is a collection of nodes without any fixed infrastructure and the vehicular nodes are connected with wireless communication. The topology of the ad hoc network is changed dynamically. Each vehicle is considered as a node in VANET. Emergency warning messages are disseminated in a highway using multihop transfer protocol [1]. Safety information is disseminated using intelligent routing protocol in VANET safety applications. An efficient data transmission technique is essential for a safety application to transmit the data to the vehicles securely. Driver assistance, alert signal to vehicles, collision avoidance and automatic alert signal generation are some of the well-known safety applications. Entertainment and infotainment applications are some of the non-safety applications. The Intelligent Transportation Systems (ITS) have been designed based on the safety data dissemination protocol with artificial intelligent techniques in Vehicular Ad Hoc Networks (VANETs) [3, 4].

Driving safety could be enhanced by developing roadway system efficiency in VANET. An accurate traffic and road system data are captured by using cluster based techniques[5].Due to high mobility and broad range of vehicles, protecting the vehicular network is more critical than the other networks such as WSN. Nowadays, the quality of service is affected by the security issues, such as authentication, confidentiality, non-repudiation, localization and verification of data, which are the most vital problem to be solved in the vehicular network. Usually Vehicular ad hoc networks are formed by vehicles moving at high speeds, therefore their communication relations or topology can be altered continuously at fast [6, 7]. In such a highly dynamic environment, traditional security solutions face many problems in VANET initiated by the complex vehicular communications system, dynamic user groups, real time constraints, etc. The privacy and confidentiality of the disseminated messages should be kept safely in VANET communications by implementing schedules in VANET [8]. In Vehicular safety applications such as infotainment, driver assistance, a lot of improvements or enhancements are needed to avoid some security issues.

The drivers take necessary decision based on the traffic information which are collected by the On_Board Unit while receiving the data. The current road situation is improved by using such kind safety applications using VANET. If any node faces hazardous event such as collision occurrence, slippery road, traffic jam road, it will produce the emergency alert signal and disseminate to every other nodes in the network. Every other On-board Unit receive the alert messages and disseminate it to the remaining nodes. This process is continued until all the On-board unit receives the messages. In some cases, the received messages can be changed by the drivers in any On-board Unit. Each OBU should send a message what it receives without doing any changes on it. It must be trustworthy while sending the alert signals to other OBUs. [9,10,11]

ISSN (Online) 2456 -1304

International Journal of Science, Engineering and Management (IJSEM)
Vol 2, Issue 12, December 2017

There are various types of attacks may occur in the network. The root cause of the attack is modifying the original data or Data forgery. It is one of challenging issue to detect the attackers which is supposed to do some alteration in the received data. It should be totally avoided. The connections among the OBU, Tamper Proof Device(TPD) may be affected or attacked while producing the alert signal and sending the alert signals to other OBUs in the VANET. As a result, it produces the wrong signals to other nodes[12].

2. RELATED WORKS

To detect the dissemination of false alert messages in VANETs by using an advanced cryptographic techniques. And also it limits the length of the messages to be sent within the specified duration in the network with the help of the cryptographic techniques. Each vehicular node can send to other nodes in the network. Two concepts such as Proof-of-work and Certificates are used. Maintenance of certificate assures the accountability of the user. Proof-of-work concept is used to protect the network from the intruders or third-party person. Esther Palomar et al. [12] designed this cryptographic technique to avoid attacks and producing proof for different types of malicious behavior in the VANET.

Xuejiao Liu et al. [13] discussed about a new authentication scheme for disseminating a message in the VANET. This authentication scheme extends the cipher text-policy based encryption with a hierarchical structure of multiple authorities. Due to this hierarchical structure, it provides scalability and also provides fine grained access control on the disseminated messages. This scheme disseminates the message in a secured way by using cipher text-policy attribute based encryption.

Jalay S Maru et al. [15] proposed a distributed dissemination protocol based on priority scheduling approach. It works like ‘‘Road-Casting Protocol (RCP)’’. In this approach, the periodic messages are broadcasted from the Road-side Unit to On-board Unit. It reduces the network congestion by disseminating the data based on the priority. It improves the delivery of a message from RSU to OBU. It is simulated and performance metrics are calculated. It shows that end-to-end delay is minimized and the packet delivery ratio is improved.

Saurabh Kumar Gaur et al.[11] discussed various future vehicular applications based on the position of vehicular nodes in the VANET platform. And also critical factors are analyzed in the networking platform which would support the future vehicular application.

Uzma Khan et al. [10] et al. proposed a detailed survey on finding or identifying the malicious or false warning sending node or misbehavior node in VANETs. It classifies the node based on the message it sends to other nodes and its behaviour. It shows various types of nodes and various types of behaviour of malicious nodes in the VANET. By this, VANET becomes highly secured and reliable network.

Nowadays Data dissemination becomes very critical task due to fast changes in the network topology and frequent segmentation of messages. Moumena Chaqfeh et al. [12], proposed two optimization strategies such as the push model and pull model for data dissemination. In Pull based model, Data is disseminated based on demands. In push based model, messages are disseminated automatically without any demands from any other nodes in the VANET. These two optimized models are compared with the existing data dissemination techniques.

VANET consists of only the wireless nodes which are not located in the fixed place. There is no infrastructure in it. Message dissemination delay, Data Traffic, Network congestion is the challenging issue in Vehicular communication system. There are three types of communication available in the network. Road-side Unit to On-board Unit, On-board Unit to On-board Unit and On-board Unit to Road-side Unit are the various types of communications taken place in VANET. Vishal Kumar and Narottam Chand [17] proposed the data scheduling method for dissemination of messages in VANET. Messages are classified and then it is scheduled to disseminate by any one of the three communication methods. Data is obtained from the on-board unit and takes necessary actions to disseminate whether it is to be sent from OBU to RSU, RSU to RSU and OBU to OBU. By this, the transmission delay is decreased and reliability status is improved in the Vehicular Ad Hoc Networks.

Chitra, et.al.,[5] discussed about the merits and demerits of various broadcasting techniques. And also broadcast storm or network congestion, broadcast suppression are discussed. Broadcasting means the way of disseminating the valid messages from one vehicular node to other vehicular nodes in the Ad Hoc Networks. The main challenges in the dissemination in the Ad Hoc Networks are discovery of an efficient route, updation of routing information and other operations. A survey on the existing broadcast suppression techniques is given. A lot of problems are thrown by simply disseminating the message packets in the VANETs.

Lakshmi, et.al., [3] proposed a novel broadcasting method based on the priority of a message. The priority of the

ISSN (Online) 2456 -1304

International Journal of Science, Engineering and Management (IJSEM)
Vol 2, Issue 12, December 2017

messages are classified as general messages, urgent messages and very urgent messages. Then, the binary partition phase was designed to find the node which is disseminated inside the Coverage Area. If any node does not post a response fast, a maximum number of probability may be an accident occurred in the region. It is simulated and finds very high reliability and security.

3. PROPOSED METHODOLOGY

There are variety of applications developed in VANET. Based on the accuracy level, it may be classified into several types. Each vehicular node has a set of equipments for computation, communication and sensing process. Even though there is a lot of equipments and provision to detect and avoid collision, an accident may occur if the driver does not react fast. This is one of the critical problem in the Vehicular Ad Hoc Network.This paper focused on a message dissemination using secured and prioritized techniques in VANET. Assignment of a priority is based on the keywords in the message and the number of messages received. There are various types of messages such as request, information, alert. The request messages are classified as emergency request, entertainment request, general request.The information is transferred in a secured manner.

3.1. Message Prioritization

The first phase of this work is message prioritization. In this phase, the messages are categorized into emergency request, entertainment request and general request. Higher priority is allotted to the very urgent request and the message is processed and disseminated fast and the necessary actions to be taken immediately.

The request is classified based on the keyword and the occurrence of the word in the message received. Classification process is done in the following way. The keywords are stored in a separate document. Whenever the message is received, the priority is allotted to the messages.
The Priority is assigned using the similarity measure for text processing. It depends on the similarity calculation between the words in the messages and the keywords stored in a document. Some extra features are also added in the similarity measurement. This kind of measure is called as symmetric measure. Based on this, the messages are classified into emergency request, entertainment request and the general request.

3.2. Secured Data Dissemination using Hybrid signcryption Algorithm

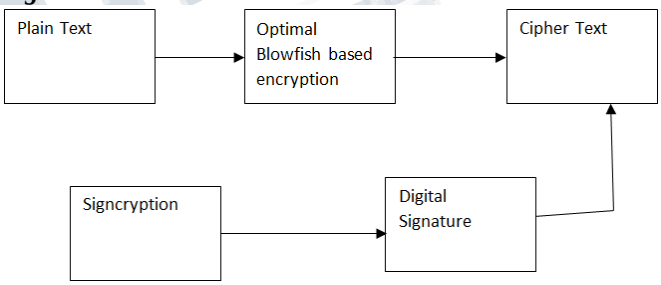
Dissemination of data in between the vehicles is the critical job in VANET. During the dissemination process, intruders or third party person may extract the messages. There are a lot of applications in the military and air force to secure the secret messages from the intruders or adversaries.

In VANET, each vehicle disseminates the message by using the combination of multicast, unicast and broadcast based on the type of the message packets it receives. Every vehicle sends the message in every direction, so that it can be disseminated to the set of vehicles. During the transmission, each vehicular node updates the messages dynamically.

This research proposed a novel signcryption[18] using DEM and KEM. The KEM is one of the random number generation techniques by executing the Key Derivation Function (KDF). And also, Secret key is disseminated along with some additional keys for the encryption process in KEM.

In DEM, Advanced Encryption Standard algorithm is used as a signcryption algorithm. Based on Cuckoo search algorithm, Optimal Blow Fish algorithm is used in Advanced Encryption Standard. The additional information are extracted from the secret key using pseudo random number functions.

Figure:



3.4. Optimal Blow Fish Algorithm

It is used in symmetric key cryptography also it is executed for both encryption and decryption process. It accepts 64 bit block size and key length from 32 bit to 448 bits. It consists P-array and four 32 bit S-boxes. Each P-array consists 18 of 32 bit sub keys and each S-box consists of 256 entries. Blow fish algorithm consists of two sections such as key expansion and data encryption. In key expansion phase, each input key 448 bit into 4168 bytes sub key arrays. In the second phase, ie Data encryption, 16 round feistal network is used. Each round consists of a key dependent substitution and key dependent permutation. Every functions in the blow fish algorithm is done using XOR.

Encryption:
Encryption is the process of converting the plain text into cipher text. The length of the input data is 64 bit. The input data is separated into two 32 bit halves at first round. In blow fish algorithm, XOR operation is performed in the first 32 bit left halves and P-array. The output of the first 32 bit is fed to the function (Ft). Then the output of left halves and the next 32 bit right halves perform the XOR operation. Then these two results are interchanged and the rest of the round goes on till it performs for all the 16 rounds.

Decryption:
In Blow Fish Algorithm, the decryption process is done in a reverse order of operations which are performed encryption process.GA based Cuckoo search algorithm for Optimal key generation in Blow fish algorithm

It is one of the best meta-heuristic algorithm. It was stimulated by the cuckoos's breeding behaviour and to develop easily. In this search, a set of nest are available. Every cuckoo lays one egg at a time in a randomly chosen nest. The high power of eggs will put back to the upcoming generation. Each egg including the cuckoo's egg represent a solution. The set of host's nests are allocated and the host bird finds the nest which contains the egg of a cuckoo. The same process is performed in the worst nest set and the solutions are left for further calculations. The combination of CS-GA algorithm finds the best combination of the generator units using the multi-objective functions. This function takes the generation limit of the generator as the input. The CS algorithm's levy flight search and GA algorithm's crossover and mutation processes are used to find the solution for the updating process. The optimal solution is chosen from the set of updated solution by using the multi-objective function.

4. CONCLUSION

Data security in data dissemination plays a major role VANET. This paper proposes the Hybrid blowfish algorithm based Signcryption technique for data dissemination. It is mainly used for encrypting the data while it is disseminated in the Vehicular Ad-hoc Network. As a result, the data is disseminated securely which cannot be affected by the intruders or any other third party persons. In future, it may be implemented and performance metrics are compared with the existing methods.

REFERENCES

[1] Muhammad Awais Javed, Duy Trong Ngo and Jamil Yusuf Khan, "A multi-hop broadcast protocol design for emergency warning notification in highway VANETs", EURASIP Journal on Wireless Communications and Networking, Vol.179, 2014.

[2] Ramakrishnan, B., Rajesh, D. R., & Shaji, R. S. (2010). An Intelligent Routing Protocol for Vehicle safety communication in Highway Environments. Journal of computing, 2(11), 2010.

[3] S. LAKSHMI and Dr. R.S.D.WAHIDA BANU, "Prioritized Directional Broadcast Technique for Message Dissemination In Vanets", Journal of Theoretical and Applied Information Technology, Vol. 68, No.1, 2014.

[4] M.Chitra and S. Siva Sathya, "Efficient Broadcasting Mechanisms for Data Dissemination in Vehicular Ad Hoc Networks", International Journal of Mobile Network Communications & Telematics (IJMNCT), Vol. 3, No.3,2013.

[5] Ramakrishan, B., M. Milton Joe, and R. Bhagavath Nishanth. "Modeling and simulation of efficient cluster based Manhattan Mobility model for Vehicular communication." Journal of Emerging Technologies in Web Intelligence 6.2 (2014): 253-261.

[6] Ramakrishnan, B., R. S. Rajesh, and R. S. Shaji. "Analysis of routing protocols for highway model without using roadside unit and cluster." International Journal of Scientific & Engineering Research 2.1 (2011): 1-9.

[7] Ramakrishnan, B., R. S. Rajesh, and R. S. Shaji. "CBVANET: A cluster based vehicular adhoc network model for simple highway communication."International Journal of Advanced Networking and Applications 2.04 (2010): 755-761.

[8] Vishal Kumar and Narottam Chand, "Data Scheduling in VANETs : A Review", International Journal of Computer Science & Communication, Vol. 1, No. 2, pp. 399-403,2010.

[9] Ramon S. Schwartz, Anthony E. Ohazulike and Hans Scholten, "Achieving Data Utility Fairness in Periodic Dissemination for VANETs", In.proc.of IEEE 75th Vehicular Technology Conference, 2012.

[10] Uzma Khan, Shikha Agrawal and Sanjay Silakari, "A Detailed Survey on Misbehavior Node Detection Techniques in Vehicular Ad Hoc Networks", Advances in Intelligent Systems and Computing, Vol. 339, pp 11-19, 2015.

[11] Saurabh Kumar Gaur, S.K.Tyagi and Pushpender Singh, "“VANET” System for Vehicular Security Applications",

International Journal of Soft Computing and Engineering (IJSCE), Vol. 2, No.6, 2013.

[12] Moumena Chaqfeh, Abderrahmane Lakas and Imad Jawhar, "A survey on data dissemination in vehicular ad hoc networks",Vehicular Communications,Vol.1, No.4, pp.214–225,2014.

[13] Sofiane Zemouri, Soufiene Djahel and John Murphy, "A fast, reliable and lightweight distributed dissemination protocol for safety messages in Urban Vehicular Networks", Journal on Ad Hoc Networks, Vol.27, No.C, 2014.

[14] Jalay .S Maru and Krunal J. Panchal, "A Literature Survey on Priority Based Scheduling With Reliable Content Delivery in VANET", International Journal of Engineering Development and Research, Vol. 2, No. 4,2014.

[15] Esther Palomar, Jose M. de Fuentes, Ana I. González-Tablas and Almudena Alcaide, "Hindering false event dissemination in VANETs with proof-of-work mechanisms", Transportation Research, Vol. 23,pp. 85–97, 2012.

[16] XuejiaoLiu, ZhenyuShan,WeiYe, RuoyuYan and Zhengliang Wang, "An fficient message access quality model in vehicular communication networks", Journal on Signal Processing, 2014.

[17] Kayhan Zrar Ghafoor,Kamalrulnizam Abu Bakar,Shaharuddin Salleh,Kevin C. Lee,Mohd Murtadha Mohamad and Maznah Kamat, "Fuzzy logic-assisted geographical routing over Vehicular AD HOC Networks", International journal of innovative computing, information & control,Vol.8, No.7(B),2012.

[18] R. Bhagavath Nishanth, Dr. B. Ramakrishnan and M. Selvi, "Improved Signcryption Algorithm for Information Security in Networks", International Journal of Computer Networks and Applications (IJCNA), Vol. 2, No. 3, pp. 151-157, 2015.