Random Password Generator in VANET Environment for a Secured Trust Creation

Milana N. Rao
4th sem M.Tech., Dept. of CS&E
Malnad College of Engineering
Hassan, India
n.milana12@gmail.com

Sharath S.
4th sem M.Tech., Dept. of CS&E
Adichunchanagiri Institute of Technology
Chikmagalur, India
sharuyashassu@gmail.com

***Abstract*— A VANET is an Adhoc network that uses moving cars as nodes in a network to create a mobile network. In VANET the communication between the nodes takes place in a secured way by using security algorithms like TESLA, ECDSA etc. For a secured communication between the nodes in a VANET, a node must trust the communicating node before communicating with it and if it is found legal, then communicate with it. If that node is found to be malicious one while trusting, it avoids communication. A VANET uses a trusted platform module to provide a secured communication between the nodes. In this paper we propose a random password generation scheme that generates a password and parent node will distribute them to the child nodes instead of maintaining long records of node details in central trusted authority.**

Keywords- Password generation, password generator trusted communication.

I. Introduction

The VANET is a mobile internet ad hoc network working in a DSRC band at a frequency of 5.9 GHz [1]. In VANET exchange of messages among the vehicles is a frequent one taking place in a secured manner using TPM [2]. In VANET exchange of data between the vehicles is frequent one. There is the possibility of having malicious vehicle in the network. That vehicle is not known to be malicious for the legal node. The malicious one will take step ahead to hack the secret key/messages from legal node. So the legal one has to keep a test to be passed by the communicating node [3]. Each nodes participating in the network is given a unique identity number to be identified by the neighbors [4]. A long list is maintained by the CTA and it is distributed to the child nodes [3].This list may grow larger in size and it will take too much of time to check the identity of a specific communicating node.

In our work, the central trusted authority will distribute a password to the child nodes it has. When one node is attempting to have communication with the legal node, the legal one will handle the password test. The communicating one must pass the password test by providing appropriate password. If the node passes the test then it will be declared as a legal one and communication request will be accepted and key/message sharing will take place. If the communicating node fails to pass the password test, it is declared as a malicious one and communication with that node is banned entirely so that remaining nodes will be saved from it. The password may be of any desired length.

II. Literature Survey

The VANET works on the DSRC band of 5.9 GHz bandwidth in order to have faster communication among the nodes, because the slower communication will lead to fatal accidents. If a message is not sent at a correct time the information will reach the vehicle only at later part of time after the accident is met. So DSRC is a best mode for communicating in a proper manner. The DSRC is divided into seven 10 MHz wide channels. Channel 178 is the control channel restricted for safety communication mode only. The channels at the edges of the spectrum are meant for the advanced accident avoidance. The remaining channels are used for safety and non safety usage. The TPM is a hardware enabling secured communication among the nodes using both symmetric TESLA and asymmetric ECDSA algorithms.

TESLA is used for the key generation quickly and the ECDSA is used for the secured communication between the nodes .The TPM uses has two keys public and private keys. The private key is known only to the user and public key is supplied to all others. At the sending end the digital signature is created and encrypted and at the receiving end the reverse process takes place and decrypted.

In [3], P.Golle, proposed, that malicious node will try to hack the secret keys/messages and hence a list of legal nodes is maintained by CTA and distributed to the entire children node. In [5], A.Studer, proposed a modified version of TESLA called TESLA++. The TESLA++ provides same computationally efficient broadcast authentication as TESLA but needs only low memory.

In [7], J. Serna, created MACM (Mandatory Access Control Model) and a novel architecture for trust propagation. The MACM specifies who has what type of access to which targets and under which conditions. The novel architecture [6] for trust propagation to get information on the certification authorities and attribute authorities valid for specific geographical area.

In [8], M. Bohge, proposed that TESLA is a broadcast authentication technique having asymmetric properties in spite of using purely symmetric cryptographic functions .TESLA is based up on delayed key disclosure. TESLA has low computation cost. The technique is used to takeoff the false certificates before key disclosure.

In [9] D. Pointcheval, proposed that ECDSA is more secured algorithm than any other. The Elliptic Curve Digital Signature Algorithm is good in its performance and successful against any type of attacks.Its stronger security does not bog down the other applications.

III. Existing System

A VANET is a mobile network environment, in which there is a Central Trusted Authority having a long record list which gives restaurant to the information about the children node, i.e. name and address of children nodes. Each node is assigned a unique identity license number [10]. This list will be sent to all the children.

A child node A has to communicate with other child node B. Now the node B does not know where node A is coming from. A is an unknown person to B. Before communicating with A, node B has to trust A that A is not a malicious one. Now node B has to check the identity license number of A from the list provided by CTA. If the identity number of A is find to be matched then communication request from A is accepted. If the license number of A is not found then A is declared malicious and vigilance information about A is passed to neighbors and A is permanently vanished from the network.

The drawback is that node B has to glimpse each and every position in the list, as the information about A may rest at any position of the list. It will take vast time.

IV. Proposed Work

Instead of using the long list of nodes with unique identities in the CTA we are going to use a password in it and it will be distributed to that to the child nodes present in the list of CTA. For that purpose we are going to generate a password of desired length.

A random password generator (RPG) is either software or a hardware device. It will take the input from a random or pseudo number generator and can generate the password automatically as an inbuilt function. A password generator is one of the part of a password manager. The password-policy enforces complex rules. In this situation, it can be easier to use password generator based on that set of rules than to manually create passwords.

A random number generator (RNG) is device designed to generate a sequence of numbers or symbols that lack any pattern, i.e. they will appear random. An encryption engine placed inside the RPG generates a password of desirable bit length from the input taken from the RNG. This is an inbuilt function. It assumes the key value for each letter/number from ASCII. Now the generated password is supplied to the under lying nodes. The Figure 1 shows the architectural view of password generation and distribution.

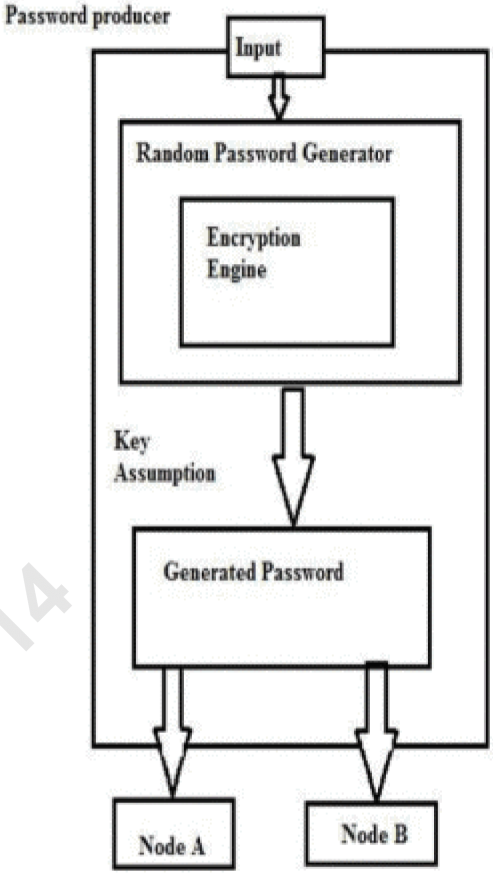

Fig 1. Architecture view of Password Generation and Distribution

A. *Steps for a random password generator (RPG)*

1. Input is taken from the random number generator.

2. The encryption engine is placed inside the random password generator and it converts the received input from the random or pseudo number generator to a password as an inbuilt function by assuming ASCII key values.

3. The generated password is then distributed to the underlying nodes.

The following Figure 2 and Figure 3 will explain the distribution of password and how the trusted communication takes place among the nodes unknown to each other even they are children of a common CTA

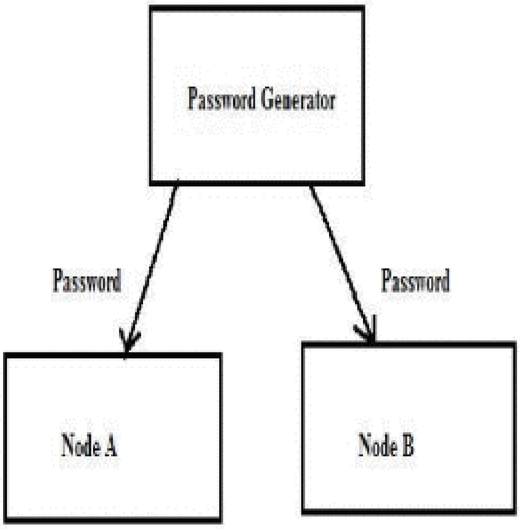

Fig 2. A Block diagram of Password Distribution

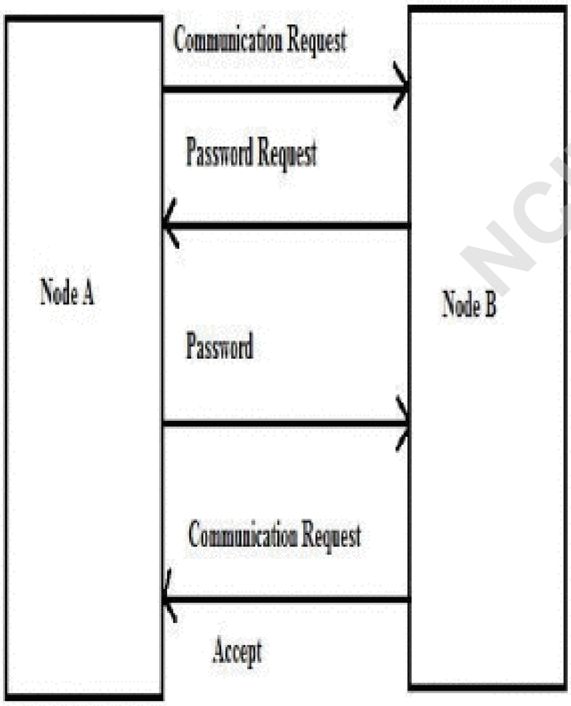

Fig 3. Node Communication

B. Generating and Verifying the password

1. Password generation:

Assume that a CTA node is generating password of n length. Allowable characters are Letters=A....Z & a…z Numbers=O ....9 and Special characters. On giving the password, corresponding ASCII code will be given as output.

2. Password verification:

Compare the password given by communicating node with password given by CTA. If matched, then communication request is accepted. If mismatched, then reject the communication request. Send vigil information about that node to neighbors.

V. Conclusion

A VANET is an Adhoc network that uses moving cars as nodes in a network to create a mobile network. It is a mobile network environment, in which there is a Central Trusted Authority having a long record list which gives restaurant to the information about the children node Thus the password is created in the Central Trusted Authority and this password is shared with the nodes that are legal present in the list and trusted communication takes place among these nodes.

References

[1] A. A. Wagan, B. M. Mughal, H. Hasbullah, "VANET security framework for trusted grouping using TPM hardware," Second International conference on communication software and networks, 2010 page no 85-88 .

[2] P.Golle, D. Greene, 1.Staddon,"Detecting and Correcting Malicious Data in VA NETs," Philadelphia, Pennsylvania, USA, VANET'04, October 1, 2004. Page no 75-77

[3] D. jiang, V. Tiiwaal, A. Meier and holfelder, "Design of 5.9 GHz DSRC-based vehicular safety communication," IEEE Wireless Communications, voU3, no. 5, pp.36-43, October 2006.

[4] B. Xiao, B. Yu, C. Gao," Detection and Localization of Sybil Nodes in VANETs," Los Angeles, California, USA, DIWANS'06, September 26, 2006.

[5] A. Studer, F. Bai, B. Bellur and A. Perrig, "Flexible, Extensible, and Efficient VANET Authentication"

[6] G. Calandriello, P. Papadimitratos, L. P. Haubaux "Efficient and robust pseudonymous Authentication in VANET," VANET, September 10, 2007.

[7] L. Serna, J. Luna, M. Medina, "Geolocation based trust for VANETs privacy", Journal of information assurance and security June 10, 2009.

[8] M. Bohge, W. Trappe, "TESLA Certificates: An Authentication Tool

for Networks of compute-Constrained Devices," In proceedings of 2003 ACM workshop on wireless security (WISE'03) San Diego, CA, USA, August 2003.

[9] A. Menezes, M. Qu, D. Stinson, Y. Wang, "Evaluation of Security Level of Cryptography: ECDSA Signature Scheme," Certicom Research January 15, 2001.

[10] U. F. Minhas, J. zhang, T. Tran, and R. Cohen "A Multifaceted Approach to Modeling Agent Trust for Effective Communication in the Application of Mobile Ad Hoc Vehicular Networks," IEEE transactions on systems, man, and cybernetics-part c: applications and reviews, vol. 41, no. 3, May 2011