ISSN No. 0976-5697

Volume 8, No. 3, March – April 2017

International Journal of Advanced Research in Computer Science

RESEARCH PAPER

Available Online at www.ijarcs.info

Perceptrons Helping to Secure VANETs

Ekta Narwal
Assistant Professor, Department of Mathematics,
M.D.U., Rohtak (India)

Sumeet Gill
Assistant Professor, Department of Mathematics,
M.D.U., Rohtak (India)

Abstract- Security is the main concern in VANETs as in near future smart vehicles will be on road. Smart vehicles have to deal with various systems on road like traffic management system, toll collection systems etc. Many cryptographic techniques are used in VANETs to provide safer communication; one of them is digital signature based on PKI. In this technique, private keys are used to generate digital signatures and these signatures are then used to verify the validity of the message and identity of the sender. These private keys are stored in hardware devices which can be hacked by the third party. In this paper, we propose to apply a new cryptographic technique on these private keys using the artificial neural network to make them secure from intruders**.**

Keywords: TPD (Temper Proof Device); TPM (Trusted Platform Module); EDR (Event Data Recorder); Cryptography; Digital Signatures; ANN (Artificial Neural Network), VANETs.

I. INTRODUCTION

VANET is a distributed self-organizing communication network made up of moving nodes i.e. vehicles. In current years when everything like highway tolls, parking areas, petrol pumps are becoming digital and all are using online payment methods for transactions and payments. There is a great need of security of messages containing account details, user's private details etc. There are many cryptographic techniques like symmetric key approaches, public key approaches, certificate revocation, pseudonym based approaches, identity-based cryptography, identity-based signature, digital signatures etc. present to encrypt these messages during communication.

Digital signatures are the well-known mechanisms for message authentication and privacy preservation in vehicles. In this mechanism, each vehicle as a node digitally signs the message before communication and on the other end; the receiver verifies these signatures to know the authenticity of the message. These digital signatures are produced using private keys so these keys act as the main agent in this encryption process that's why these keys are stored very carefully.

II. SECURITY DEVICES USED IN VANETs

EDR (Event Data Recorder), TPD (Temper Proof Device) and TPM (Trusted Platform Modules) are the mainly used hardware devices in smart vehicles for security purpose. [1] EDR is used to record information related to the vehicle whether outside or inside. Inside information like fuel consumptions, heat, temperature and outside like accident which happened on the road, weather conditions etc. This device record date, time, speed, acceleration, position and reason of the accident. It prepares its own database and store in the memory. Law enforcement agencies and transportation agencies use this data as evidence in the investigation. EDR can create or save information but it cannot secure that information from intruders. Data stored in EDR is very important and need some security so TPD and TPM are used for this purpose. [2] Many Sensors are embedded into the smart vehicles and they provide information related to the vehicle to the CPU and with the help of TPD, CPU performs the authentication, this is internal communication. One OBU (On Board Unit) is also present in smart vehicles for outside communication mean when a vehicle wants to communicate with other vehicles and RSUs (Road Side Units), OBU plays an important role. TPD works as a security agent in both inside and outside communications. [4]

TPD applies cryptographic techniques on the data and messages to save them from unauthorized access. It encrypts the data and messages, digitally sign the messages and also help in verification of sender's identity using cryptographic mechanism. All secret keys used in encryption, decryption and producing digital signatures are stored in TPDs. TPD is both software and hardware protected. [5] A third party device TPM (Trusted Platform Module) is used in place of TPDs. TPM needs some software for communication. It is software protected. This is a small hardware device placed in OBU for storing information and performing cryptographic algorithms on data and messages.

III. PROBLEMS WITH CURRENT DEVICES

- EDR cannot be used for security purpose because it stores only data and information.
- TPD and TPM provide security but both are very expensive. The cost of installing them is more than the cost of the entire vehicle which in turn makes the smart vehicle very costly.
- TPD is both hardware and software protected but it cannot work well in the extreme hot environment.
- TPM is less costly than TPD but it is only software protected and if any intruder finds the security keys he can easily access the TPM data.

IV. PRIVACY CHALLENGES AND CURRENT ISSUES

This section points out the memory attacks which steal the sensitive information from the memory. Memory attacks are basically of two type software-based attacks and hardware based attacks. Hardware attacks directly attack hardware on which the data is stored and access physical memory of the victim machine. Software attacks make use of system's weakness to read the sensitive information from the system memory. [6]

On a highway where many vehicles are moving at a very fast speed can enter or exit the ad hoc environment anytime. So when a vehicle wants to communicate with nearby RSU, then other vehicles can act as routers for them to establish the connection. In such situation, there is a possibility that any fraud vehicle can act as RSU and supply malicious information or message to the receiver or can also retrieve private information of the receiver vehicle. In some cases, RSU broadcast an emergency message to all the nearby vehicles related to the weather conditions or any other important news. Here also an intruder can intrude in the network, act as RSU and can spread false messages to the nearby vehicles. [7]

In both the cases, we can see that there is a need for some proof of identity to attach with the message to preserve the privacy of data and message. This is done by attaching signatures with the messages which contain the identity of the sender and ensure the originality of the origin of the message and message content. TPD plays an important role in it. Many cryptographic algorithms are installed in it for message authentication. One of them is Digital Signatures using PKI. VANETs use Public Key Infrastructure (PKI) technique to create the digital signature based on the private key, public key and the message. This technique is very famous for trust establishment. Safety messages generated by RSUs for all nearby vehicles need not to be encrypted but it is necessary to verify the identity of the sender of these type of messages because a false node can also send this type of message to create mismanagement. So to authenticate its identity, the sender of the message digitally sign the message with a set of public or private key pairs assigned to it. These signatures are then packed with the message, certificate, timestamp and passes to the other end involved in the communication. Then the receiver end node verifies the identity of the signer using signature, certificate and public key. Anyone who has the private key can create the certificate which appears to be signed by the certificate real owner. [8]

Let S be the vehicle who sends the message, R be the receiver, M is the message, T is the time-stamp to validate the message validity, PvK is the private key and C is the certificate of the sender S.

S→R: (M,DSign"PvK" {M│T},C"S")

A vehicle has to store the large keys to maintain the privacy and also need to keep changing them after an interval of time. All these keys are stored in Tamper-proof Device (TPD) to save them from unauthorized access. But due to the very high cost of these devices, we here try to present an approach which is different from the currently used approaches to assure the safety and security of data in the vehicles. We here try to re-encrypt the keys used in the production of digital signatures. We try to change the way of storing the private keys. Keys will be stored in form of network parameters generated during the learning process of Artificial Neural Networks. These weight values are 100% secure because there is no way to produce original input value without knowing all details of the network.

V. SYSTEM OVERVIEW

The encryption mechanism proposed in our scheme is based on the Perceptron model of Artificial Neural Network (ANN). In order to implement confidentiality the private key used in digital signatures are encrypted using this model.

The different stages for this work are:

1. Converting Keys into matrix form
2. Learning Process
3. Replacing Keys with Network Parameters

A. Converting Private Keys into matrix form

Private keys are basically stored in the user profile under rootdirectory. They are encrypted by any encryption mechanism. Any authenticate user can easily get them from there after login. In our scheme, we used an arbitrary key. Now the key is in the form of alphanumerical, so our first step is to convert that into binary form after that they are converted into a suitable matrix which works as an input in the learning process.

This is the private key used in our research

**01B703C327477634349CA686C57949014B2E8AD2C862
B2C9D748896A8B91F636F275D6E8CD19906027315735
644D95GD6763CEM49F56AC2F376E1CEE0EBF282DF
439906F34D96E085BD5656KL931F313D72D395EFE33
CBFF29E4030B3D05A28FB7F18EA27637B07957D32F2
BDE8706227D04665EC91BAF8B1AC3EC9144AB7F21**

This is a 256 bytes private key which is basically used in producing digital signatures in Vanets. This is then converted into 256x8 matrix. Now this 256x8 matrix will work as an input in our network.

B. Learning Process

During this phase, we use Perceptron Model of Artificial Neural Network to make the system learn the private key. Here the 256x8 matrix obtained from the previous phase taken as an input value and the target value for the network and then the training is done using Perceptron Model. This model uses hard-limit transfer function (hardlim). The perceptron output is limited to 0 or 1. The perceptron neuron produces 1 as output if the net input into the transfer function is equal to 0 or greater than 0 otherwise it is 0.[9]

Let w= weight, b= bias, x= input

Then f(x) = w.x + b

f (x)= 0 if w.x+b<0 otherwise f(x)= 1

Perceptron model has three steps:[10]

1) *Scaling Input up and down:* The input values are multiplied by the corresponding weight values. Initially, weights are random values and during learning, they are adjusted according to the error values.
2) *Input summed up:* Modified input values are summed up together to form a single value and bias added to the sum. Biases are also adjusted during the learning phase. Initially, biases are also random values as like weight but after iteration, they both are adjusted and shifted so that the next result can become closer to the desired output.
3) *Activation:* The result thus feeds to an activation function (transfer function) to turned input values into an output. Transfer function here used is hardlim. Fig.1 shows the hardlim (Hard-limit transfer) function.

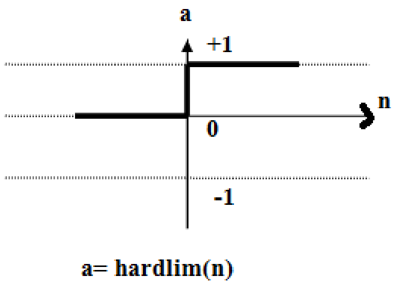


Fig.1 Hard-Limit transfer function

C. Replacing Keys with Network Parameters

Now after the training phase network parameters are obtained as weight values which are saved in form of excel sheet. The original input files are deleted from the computer memory and replaced by these network parameters.

VI. RESULTS AND OBSERVATIONS

There are many cryptographic techniques used in Vanets one of them is the digital signature. Private and public keys are used to produce these digital signatures. Securing private keys from the intruders is a very tough and costly task. Some complex hardware devices are used for these purposes that require some extra effort and cost. So here we try to store these keys in form of network parameters. Time Taken by the network for the training of 256x8 matrix is 0.01 second and only 3 iterations are needed to met the final output with 0 error. Fig.2 shows the network model of our training with 256 neurons as input and 256 neurons as output. Fig.3 shows the performance graph of the training process. Fig.4 shows the various training parameters used in our network.

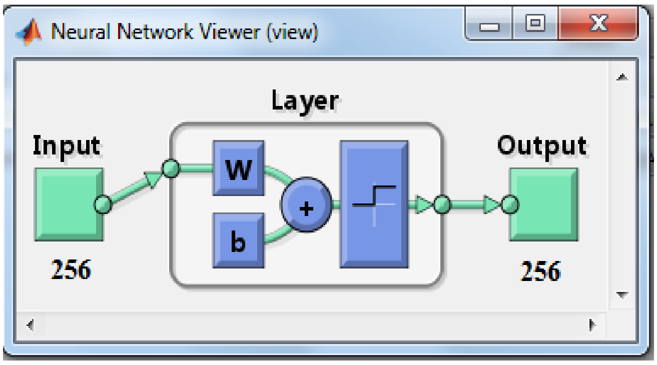


Fig.2 The Perceptron Model

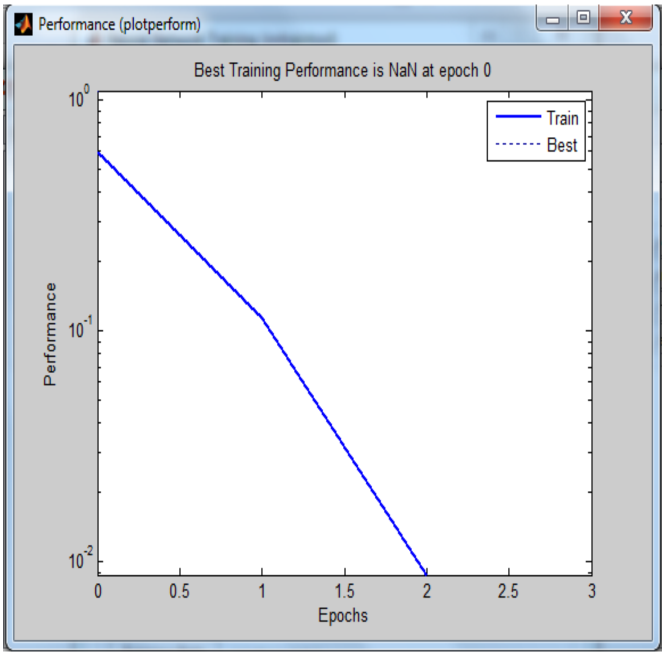
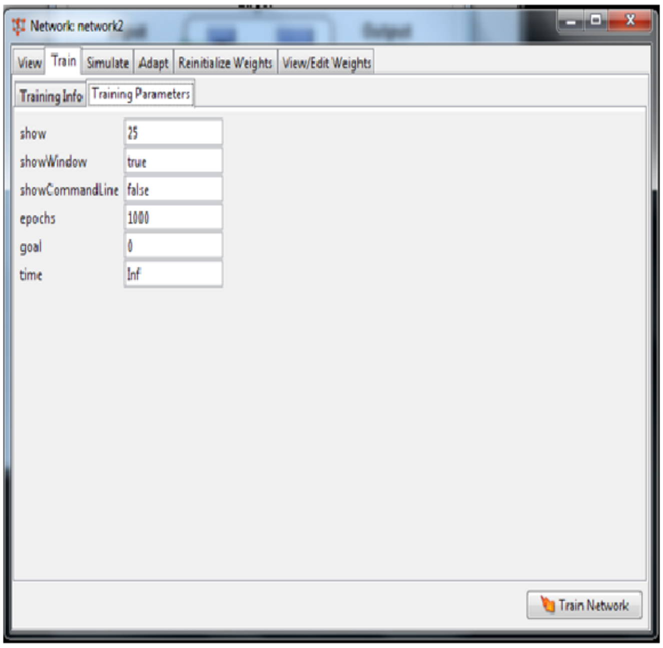


Fig2. Performance Graph of Perceptron Network during Process of Memorizing Pattern



show	25
showWindow	true
showCommandLine	false
epochs	1000
goal	0
time	Inf

Fig.3 Network Parameters

After training network is tested using two input patterns, one set is taken from the known patterns and other is some unknown test pattern. The result is then compared for known pattern output is same as desired and for unknown pattern the output is not same.

VII. CONCLUSION

Digital Signatures are used to make the messages or information in VANETs, more secure, but to verify these signatures in a real-time environment is not easy. Private keys are used to verify these signatures but to secure these private keys is not an easy task. In this paper, we used the Perceptron model of Artificial Neural Network for the quick and secure saving of keys in the memory of a system. Extra hardware devices are used in VANETs for saving any type of cryptographic keys but by using our approach there is no need of such type of extra hardware. Keys are replaced by the weight matrix obtained through the training process and this method is 100% secure because it is impossible to obtain keys from these weight without knowing the original network. There are many network models present in Artificial Neural Network which can be used in place of the Perceptron model.

REFERENCES

[1] I. A. Sumra, H. Bin Hasbullah, and J. A. Manan, “Comparative study of security hardware modules (EDR , TPD and TPM) in VANET,” *Security*, no. Nits, pp. 1–7, 2011.

[2] J. Domingo-Ferrer and Q. Wu, “Safety and privacy in vehicular communications,” *CEUR Workshop Proc.*, vol. 397, pp. 6–11, 2008.

[3] C. Zhang, R. Lu, X. Lin, P. H. Ho, and X. Shen, “An efficient identity-based batch verification scheme for vehicular sensor networks,” *Proc. - IEEE INFOCOM*, pp. 816–824, 2008.

[4] M. Raya, P. Papadimitratos, and J. P. Hubaux, “Securing vehicular communications,” *IEEE Wirel. Commun.*, vol. 13, no. 5, pp. 8–15, 2006.

[5] H. Victor, “World â€TM s largest Science , Technology & Medicine Open Access book publisher Privacy-Preserving

Information Gathering Using VANET Privacy-Preserving Information Gathering Using VANET."

[6] L. Guan, J. Lin, B. Luo, J. Jing, and J. Wang, "Protecting Private Keys against Memory Disclosure Attacks using Hardware Transactional Memory," pp. 3–19, 2015.

[7] S. Mahajan and P. A. Jindal, "Security and Privacy in VANET to reduce Authentication Overhead for Rapid Roaming Networks," *Int. J. Comput. Appl.*, vol. 1, no. 20, pp. 21–25, 2010.

[8] S. Kohli and R. Dhiman, "Secure Message Communication using Digital Signatures and Attribute Based Cryptographic Method in VANET," *Int. J. Inf. Technol.*, vol. 2, no. 2, pp. 591–594, 2010.

[9] M. Veloso, "Perceptrons and Neural Networks," 2001.

[10] P. D'Souza, S.-C. Liu, and R. H. R. Hahnloser, "Perceptron learning," *Proc. Natl. Acad. Sci. U. S. A.*, vol. 107, no. 10, pp. 4722–7, 2010.