HCTL Open International Journal of Technology Innovations and Research (IJTIR)
http://ijtir.hctl.org
Volume 21, Issue 1, July 2016
e-ISSN: 2321-1814, ISBN (Print): 978-81-932623-1-3

An Approach to Minimize Faulty Data Propagation in Vehicular Adhoc Network

Nazish Siddiqui[1], Mohd. Shahid Husain[2]

nazishcs@iul.ac.in

Abstract

The recent advancements in wireless communication technologies allow for information exchange in high mobility. Such a mobile network that comprises of vehicles and the road side units as the nodes and allows information exchange among them is called Vehicular ad Hoc Network (VANET). In VANETs, vehicles broadcast information to other nearby vehicles in their surroundings. However, if the authenticity of this information exchange is not maintained, then it may lead to some severe security threats. The presence of faulty and malicious nodes are responsible for the dissemination of fake and forged messages in the network. This paper proposes an approach for the minimization of faulty data dissemination in the vehicular adhoc network to improve the security and reliability of the network. The main idea is to check for the authenticity of the message, to ensure the message being correct and reliable and consequently, reduce the propagation of malicious and faulty messages from the network.

Keywords

VANET , authenticity, credit, cost, threshold.

Introduction

The integration of information technology within vehicles resulted in vehicles being more than just a case of glass and steel. It is actually network of computers which are in motion. The need for security is growing as vehicles are increasingly made automated and connected to the internet. Thus the connected vehicles will face the security threats in the same way as other network devices and this opens up the possibility for malicious adversaries to control and govern certain aspects of the vehicle.

The Vehicular Ad-Hoc Network, or VANET, is a network that incorporates a technology that uses vehicles in motion, as nodes in a network, thus forming a mobile network. Every participating vehicles, at a distance of approximately 200 to 400 meters among them, act as wireless router or node, and connect with each other to create a network with a wide range. If some vehicles drop out of the network as they fall out of the signal range of the communicating vehicles, others can join in, connecting them to one another, hence creating a mobile Internet. VANET, a type of MANET (Mobile Ad-hoc NETwork) is a network of number of communicating vehicles, eventually dispersed on roads. In VANETs, vehicles can communicate with each other (V2V, Vehicle-to-Vehicle communications), as well as with the infrastructure unit present on roadsides (V2I, Vehicle-to-Infrastructure) to get various services from it, using DSRC as the short range radio standard [2].

The communication in a VANET depends on the exchange of information among different nodes present in the vehicular network. This information exchange helps to implement and improve the safety on the road, driving conditions, ease and comfort on the journey and the efficiency of the network. All this is possible by utilizing the information received from the vehicles to make majority of the decisions. Hence the reliability of a vehicular network relies on the information broadcasted by the vehicles. However, in order to get advantage over other vehicles or to gain access to the network resources in a wrongful manner, a node may behave malicious or selfish. A misbehaving node may tamper messages , create congestion in the network , transmit fake and false alerts, or even drop, delay and duplicate packets [11,13]. Thus, it is very important and crucial to detect misbehavior in VANET as being careless about it might have disastrous consequences. To detect misbehavior in the network, the receiver node must check for the sender's authenticity, before it could take appropriate action depending on the messages received by the sender node so as to ensure reliability of the messages. Moreover, the reliability of a message and the security of the network could be even more enhanced if the message received by the receiver node could be checked for its authenticity and truthfulness.

Several important research works has been proposed on improving safety and security in VANETs by detecting misbehavior and malicious nodes and excluding them from the network. This paper proposes an approach called CTS- Credit based Threshold System, to minimize the faulty data dissemination in the vehicular network, thus improving the security and reliability of the network. Two of the most prevalent and efficient techniques to achieve the property of message reliability are Threshold method[6,7,9] and Credit-based model[1,3,5,8]. In this paper, the proposed "Credit based Threshold System", is based on both the threshold concept of authenticating a message and the Credit based model of checking the truthfulness of a message. Both these approaches are used together with a slight distinction from the existing methods to enhance the probability of a message being truthful. The main concept used in our work is to check for the authenticity of the message, to ensure that it could be relied upon and consequently prevent the propagation of malicious and faulty messages from the network. To check the authenticity of a message, certain parameters are considered and based on them a formula for message authentication has been proposed. Depending on the value of message authenticity, a message is either accepted or rejected from further transmission and thus improving the network security. A message with high value of authenticity is accepted and rest are discarded; as a result the presence of faulty data could be minimized in the network.

The remainder of this paper is organized as follows: In Section II, we present a brief review of the related works in literature. Our solution based on CTS approach is described in Section III. Section IV presents the implementation of the work and the experimental results. Finally, Section V concludes this paper.

Literature Review

To address the security issues in the vehicular ad hoc network, many schemes have been proposed having emphasis on various aspects and with varying degree of success or failure. Here, in this paper, we will focus on research that are particularly relevant to providing reliability and authenticity of the message transmitted in the network. Some of the remarkable approaches, based on the concept of credit based models as well as threshold based authentication are discussed here.

The use of Credit based model to achieve reliability is a common approach in literature [1,3,5,8]. We refer reader to the paper of Nadia et al. in [1]. The authors proposed an approach called VIME that stands for Vehicular incentive model with exclusion for malicious nodes. It is is based on managing the credit count, that each node receives at the beginning of the application, following the concept of the signaling theory of economics. In their work [3] and [8], the authors proposed Distributed Trust Model, termed DTM2, adapted from the job market signaling model. Nadia et al., here in [3] and [8], consider the harmful presence of malicious node and selfish nodes, in the network, who spread forged and false data and cooperate only for their own benefit respectively. It deals with allocating credits to the nodes and managing them securely. Nodes require a reception cost, to access data in the network. Besides this, it also requires the sending cost, ensuring higher cost for malicious nodes.

An approach to provide security authentication method, based on the concept of trust evaluation is proposed by Zhou et al. in [5], to guarantee security of the entire network. The trust evaluation scheme is divided into two parts; in the first part, authentication is provided based on direct trust evaluation and in the second part indirect trust evaluation is used to provide secure authentication. In the direct trust evaluation approach, direct trust is calculated when the security behaviors of the new vehicle is compared with the historical evaluation of security that is collected from the AU [5]. Whereas, in the indirect trust evaluation approach, the trust degree is calculated based on the recommendation trust vectors of the vehicle nodes in the network. Information cascading and oversampling [4], are the two common problems present in social networks that affects the trust management schemes in VANETs adversely. Zhen et al. proposed a novel voting scheme in [4], to deal with these problems. The authors details about each vehicle having different voting weight depending on the distance from the event; with the closer vehicle possessing higher weight. The authors in their paper emphasize on considering only the first hand information besides the opinions of all neighboring nodes, for getting better results.

The problem of misbehavior in the network can be solved to a greater extent by using the threshold method of authentication. Shao et al. in their work in [6], proposed the features of threshold authentication and efficient revocation of nodes in a new authentication protocol for VANET that in a decentralized group model, uses a new group signature scheme. In the decentralized group model, with each group under the control of distinct RSU, the threshold authentication method, can work well as they are integrated using new anonymous authentication protocol. Another threshold mechanism, proposed by Liqun et al. in [7] is termed as Threshold Anonymous Announcement service (TAA) to handle both authorized parties and adversaries. A good balance is maintained between hardware and software to improve the performance. The authors discussed and detailed the use of tamper-resistant black box [7][14], [7][17], equipped in vehicles for performing secure operations. Besides, the good working of the TAA scheme as claimed, Chun et al. in [9], proposed some modifications on the Chen et al.'s scheme in [7] for more efficient and reliable performance Another solution is k-times anonymous authentication approach proposed by Teranishi et al. in [10], based on the concept that there are many applications that need to restrict the number of times a user can have access to a service. Each AP [10] is independent and free to determine

the maximum number of times, a user is allowed to access. A k-time anonymous signature scheme allows revealing the identity of the signer, if it signs the same message more than k times.

There are several approaches used to implement authentication and improve reliability of the messages in the network. Only few of them have been mentioned and discussed here. All these approaches individually focus on different aspects of security in VANET. However, we have combined the concepts of these approaches and proposed a new scheme called Credit based Threshold System, which is discussed in the next chapter.

Proposed Work

VANET, is a network of vehicles that broadcast information about their surroundings to other nearby vehicles, so that appropriate action could be taken as per requirement, upon receiving the messages. However, this broadcasting is not always trustworthy and reliable, due to the presence of malicious and faulty nodes in the network, which consequently results in the transmission of fake and forged messages. A message announced could be considered to be reliable and true only if the receiver is assured that it was sent by a legitimate vehicle, unmodified and also that the content of the message represents the actual situation.

To attain the property of message reliability, we have proposed an approach called “Credit based Threshold System (CTS), which combines the features of both the threshold concept of looking for a threshold number of vehicles sending the same message, so that it could be accepted, on one hand and the Credit based model on the other ,that enables for sending the message on the stake of some cost and thereby managing the credits of the nodes. Our proposed approach differs from the existing approaches in a way that the authenticity of a message is checked using a formula based on certain parameters. Instead of looking only for the credit score of the reporting vehicles or the threshold value of the number of nodes, here, the density of the network, the total credit score along with the threshold value of number of nodes sending the message is checked, so as to ensure the authenticity of the message.

The message that is found authentic or the one with higher value of message authenticity, would be accepted or else it would be discarded. For this. the scaling of the values of message authenticity is done on the scale of “0-10” with different range of values categorized as High, Medium and low. The messages having “Higher” or “Medium” value of authenticity are more likely to be accepted, while the messages with “Lower” value of authenticity will be discarded.

We propose the following formula to check the authenticity of the message,

$$m_{auth} = \alpha d + \beta n + \gamma(\Sigma c_i) + \mu$$

Network Model

To implement our proposed approach, we consider the following components to be present in the network model of the vehicular adhoc network. These are similar in features and functionalities to the components of a traditional vehicular network.

1. **Central Authority (CA)** - A trusted authority (TA) at the centre.

2. **Road Side Unit (RSU)** – The base stations located at distinct locations on road, another local trusted authority.

3. **Vehicles –** Includes smart cars or other vehicles equipped with latest technology.

4. **On Board Unit (OBU)-** The main processing unit present in a vehicle.

5. **Tamper Proof Module (TPM)-** A highly secured tamper resistant device (TRD), present in a vehicle that cannot be attacked.

Assumptions

The Credit based threshold system proposed is based on following assumptions:

1. A straight road scenario such as Highways, so that density of the network could be determined easily.
2. Each vehicle is equipped with GPS, Trusted component (TPM) etc.
3. Each node (vehicle or RSU) will first register itself with the Central Authority (CA).
4. The Central Authority will provide the vehicle with a Certificate, after registering it, to authenticate it as a valid user.
5. The certificate includes the signature of the CA, along with the identification of the nodes as a vehicle or RSU, say ID_v or ID_{RSU} respectively.
6. The information broadcasted by the RSU will always be the trusted one.
7. The CA must provide some set of Pseudo-id's to different RSU's.
8. RSU's are responsible to assign different pseudo id's to different vehicles coming into its network.
9. The CA also provides the vehicles with some credits (say=10) at the beginning as the vehicle joins the network.
10. Each vehicle sending or receiving messages in the network must have the credits with it.
11. A vehicle short of credits will not be able to send or receive the messages.
12. Vehicle sending the message must send it at the stake of some cost.
13. Each vehicle has a tamper proof device (TPM) that automatically increases or decreases the credit count of the vehicle as per the response from other nodes.

Notations

The table below shows various notations of the CTS schemes.

Table1: Notations of the CTS scheme

SYMBOLS	DESCRIPTION
d	Density of nodes(vehicles) in the network.
n	Number of nodes sending the message with the same content.
c_i	Cost at which different vehicles send the message
cr	Total credits available with the nodes.
v_s	Sender node
v_r	Receiver node
msg	Message
α	Coefficient of network density
β	Coefficient of number of nodes sending the message
γ	Coefficient of total summation of cost at which different vehicles send the message.
μ	Constant
m_{auth}	Authenticity of a message on the scale of 0-10, i.e. High , Medium or Low.

Proposed Algorithm

Following are the steps involved in the proposed work:

- Each vehicle first register itself with the CA.
- The CA provides it with some credits along with the certificate to access the network.
- RSU after verifying the certificate of the vehicle, provides it with a pseudo id.
- The sender node Vs, sends the message “msg”, along with some cost “c”, as

  $$Data=msg+c;$$
- When the sending vehicle sends the message, TPM present in it, automatically decrement its credits by the amount “c”, and its new credit score will become as

  $$cr_{new}= cr_{old}-c;$$
- Receiver node Vr, when receives the data will check for the following parameters:
  1. Density “d” of the nodes in the network.
  2. Number of nodes “n”, from where the same message has been received.
  3. The cost “c_i” at which different vehicles sent the same message.
- The authenticity of the message is checked by the proposed formula

  $$\mathbf{m_{auth}= \alpha d+\beta n+\gamma(\Sigma c_i)+\mu;}$$

where the value of **α=-1.4, β=1.7, γ=0.21 and μ=3.1** as derived through the training phase.

- The value of "m_{auth}" i.e. authenticity of the message is checked as given below

```
If (m_auth >=7)
{
        Authenticity =High;
        Accept the message;
}
Else if (m_auth >=4 && m_auth <7)
{
        Authenticity=Medium;
        Either accept or reject the message;
}
Else
{
        Authenticity=Low;
        Reject the message;
}
```

- If the receiving vehicle V_r finds the message correct, it returns an acknowledgement (ACK) to the sending nodes.
- The TPM of the sending node will then increment its credits by the amount "2c", and its new credit score will be updated as

$$cr_{new} = cr_{old} + 2c;$$

- In case of rejecting the message, no such ACK is sent.

Experimental Results

In our proposed approach, we have focused to check the authenticity of the message to minimize the faulty data propagation from the network. For this the proposed formula for message authentication is given below:

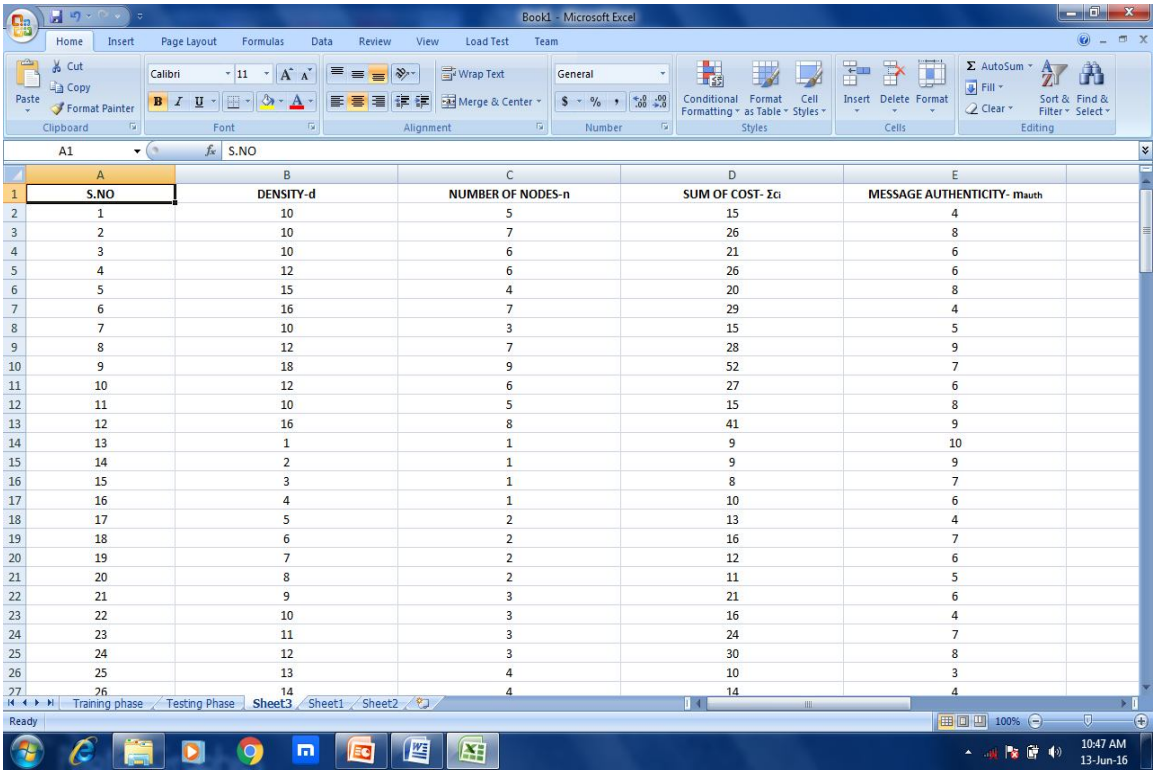
$$\mathbf{m_{auth} = \alpha d + \beta n + \gamma(\Sigma c_i) + \mu}$$

The proposed formula contains several coefficients, coefficient of density (**α),** coefficient of number of nodes sending the same message **(β)** and the coefficient of total sum of costs at which different vehicles send the message (**γ**), along with the constant (**μ).** In order to derive and verify these values of various coefficients **α, β, γ and** the constant **μ** used in the above mentioned formula, there are two main phases, we have gone through- the "Training Phase" and the "Testing Phase".

Training Phase

The training phase deals with obtaining the values of **α, β, γ** and **μ,** while varying the values of other variables **d, n, c_i and m_{auth}** used in the formula. About 150 different values are assigned to the variables **d, n, c_i and m_{auth}**, thus forming 150 different linear equations based on the structure of the above proposed formula. The snapshot below in Figure 1, contains the tables showing some of the assumed values of **d, n, c_i and m_{auth}** from the total 150 different assumptions.

HCTL Open International Journal of Technology Innovations and Research (IJTIR)
http://ijtir.hctl.org
Volume 21, Issue 1, July 2016
e-ISSN: 2321-1814, ISBN (Print): 978-81-932623-1-3



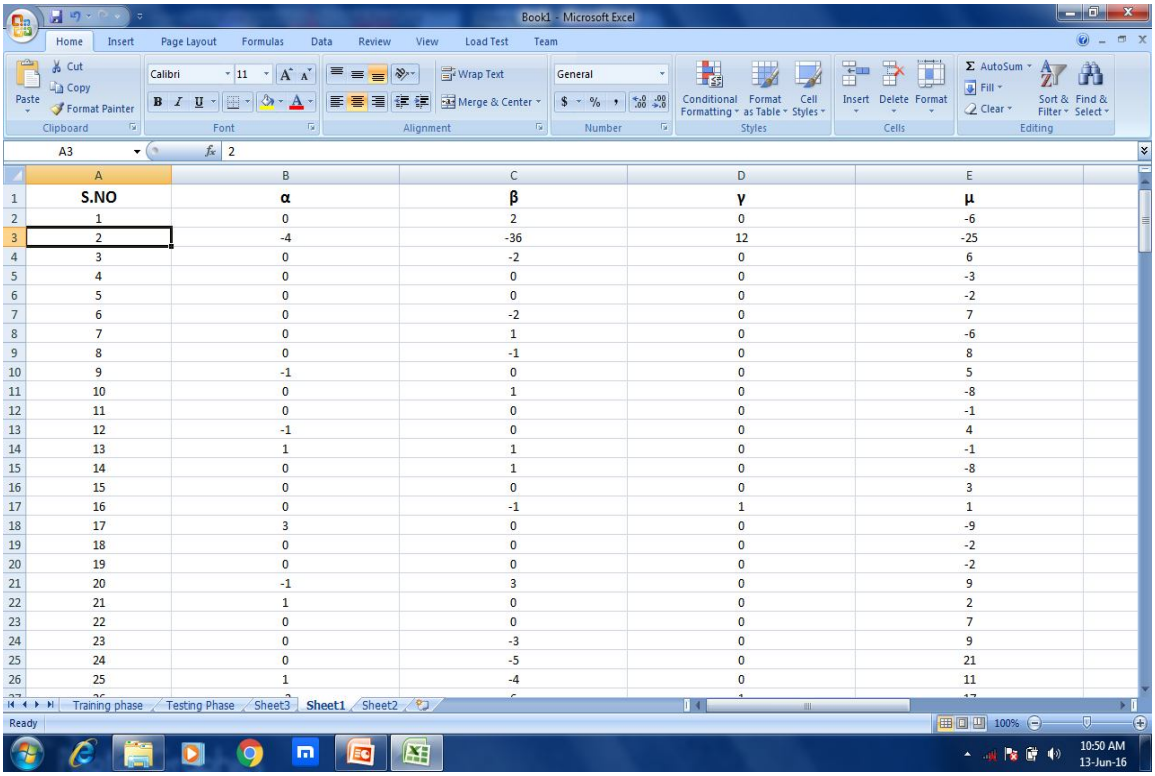
S.NO	DENSITY-d	NUMBER OF NODES-n	SUM OF COST- Σc_i	MESSAGE AUTHENTICITY- m_{auth}
1	10	5	15	4
2	10	7	26	8
3	10	6	21	6
4	12	6	26	6
5	15	4	20	8
6	16	7	29	4
7	10	3	15	5
8	12	7	28	9
9	18	9	52	7
10	12	6	27	6
11	10	5	15	8
12	16	8	41	9
13	1	1	9	10
14	2	1	9	9
15	3	1	8	7
16	4	1	10	6
17	5	2	13	4
18	6	2	16	7
19	7	2	12	6
20	8	2	11	5
21	9	3	21	6
22	10	3	16	4
23	11	3	24	7
24	12	3	30	8
25	13	4	10	3
26	14	4	14	4

Figure 1: Training Phase- Assumed values of the variables -d, n, c_i and m_{auth}

These 150 linear equations of the assumed values are further grouped in the combination of 4 different linear equations together at a time to determine the values of four constants **α, β, γ and μ.** We have obtained 200 such sets of varying combinations of 4 different linear equations together, and they are solved. Once 200 values of these coefficients **α, β, γ and μ** are obtained, their average is determined to finalize the generalized values of them. The snapshot below contains the table showing some of the derived values of **α, β, γ and μ** from the total 200 different derivations.

Hence the final values of the coefficients **α, β, γ and μ** as derived from the training phase are:

1. **Coefficient of density, α= -1.4**
2. **Coefficient of number of nodes sending the message, β= 1.7**
3. **Coefficient of summation of different cost at which message is sent, γ=.21**
4. **Constant, μ=3.1**



S.NO	α	β	γ	μ
1	0	2	0	-6
2	-4	-36	12	-25
3	0	-2	0	6
4	0	0	0	-3
5	0	0	0	-2
6	0	-2	0	7
7	0	1	0	-6
8	0	-1	0	8
9	-1	0	0	5
10	0	1	0	-8
11	0	0	0	-1
12	-1	0	0	4
13	1	1	0	-1
14	0	1	0	-8
15	0	0	0	3
16	0	-1	1	1
17	3	0	0	-9
18	0	0	0	-2
19	0	0	0	-2
20	-1	3	0	9
21	1	0	0	2
22	0	0	0	7
23	0	-3	0	9
24	0	-5	0	21
25	1	-4	0	11

Figure 2: Training Phase- Derived Values of the coefficients- α, β, γ and μ

Testing Phase

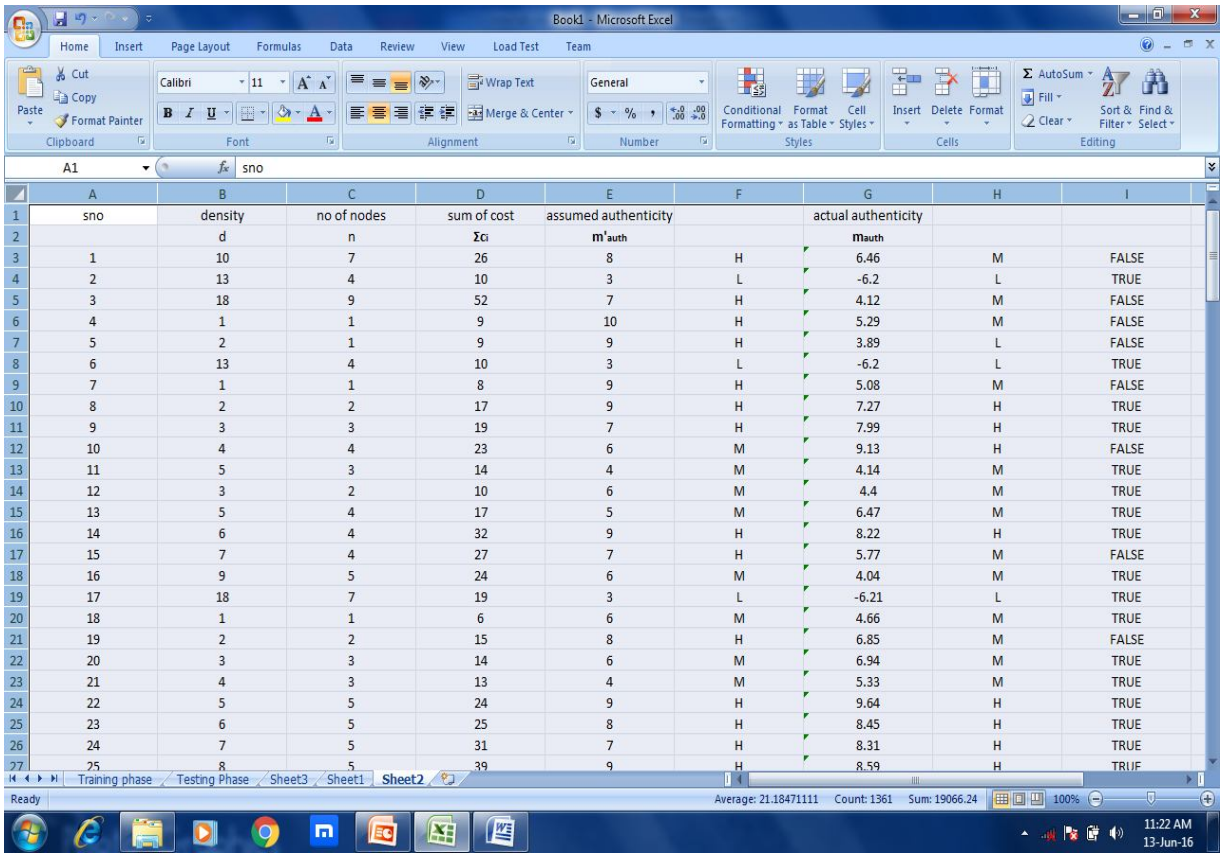
Testing phase deals with the verification of the values of **α, β, γ and μ** as obtained from the training phase**.**

For this, following are the steps involved.

- About 150 different values of the variables **d, n, and c_i** and the assumed authenticity **m'_{auth}** are assumed and assigned.
- Based on the range of message authenticity, the value of assumed authenticity (**m'_{auth}**) is categorized as High, Medium or Low.
- Now the value of actual message authenticity **m_{auth}** is obtained from the proposed formula by keeping the values of **α, β, γ and μ** as obtained from the training phase.
- Again, the value of **m_{auth}** obtained, is categorized as High, Medium or Low based on the range of message authenticity.
- Finally, the values of derived authenticity (**m_{auth}**) and assumed authenticity (**m'_{auth}**) are compared based on their categorization as High, Medium or Low in Figure 3 .

The Authenticity range of message is proposed as under:

<0 or 0 or <4	4 to <7	7 to 10 or >10
LOW=L	MEDIUM=M	HIGH=H



sno	density	no of nodes	sum of cost	assumed authenticity		actual authenticity		
	d	n	Σc_i	m'_{auth}		m_{auth}		
1	10	7	26	8	H	6.46	M	FALSE
2	13	4	10	3	L	-6.2	L	TRUE
3	18	9	52	7	H	4.12	M	FALSE
4	1	1	9	10	H	5.29	M	FALSE
5	2	1	9	9	H	3.89	L	FALSE
6	13	4	10	3	L	-6.2	L	TRUE
7	1	1	8	9	H	5.08	M	FALSE
8	2	2	17	9	H	7.27	H	TRUE
9	3	3	19	7	H	7.99	H	TRUE
10	4	4	23	6	M	9.13	H	FALSE
11	5	3	14	4	M	4.14	M	TRUE
12	3	2	10	6	M	4.4	M	TRUE
13	5	4	17	5	M	6.47	M	TRUE
14	6	4	32	9	H	8.22	H	TRUE
15	7	4	27	7	H	5.77	M	FALSE
16	9	5	24	6	M	4.04	M	TRUE
17	18	7	19	3	L	-6.21	L	TRUE
18	1	1	6	6	M	4.66	M	TRUE
19	2	2	15	8	H	6.85	M	FALSE
20	3	3	14	6	M	6.94	M	TRUE
21	4	3	13	4	M	5.33	M	TRUE
22	5	5	24	9	H	9.64	H	TRUE
23	6	5	25	8	H	8.45	H	TRUE
24	7	5	31	7	H	8.31	H	TRUE
25	8	5	39	9	H	8.59	H	TRUE

Figure 2: Testing Phase- Comparison of Assumed Authenticity m'_{auth} and Derived Authenticity m_{auth}

Result Analysis

The experimental results from the testing phase, verifies our proposed formula for message authentication. We analyze the values of assumed authenticity $\mathbf{m'_{auth}}$ and the actual authenticity $\mathbf{m_{auth}}$, and on comparing them, it is found that both the values are nearly the same and falls under the same category of authentication range, in almost most of the cases. We have tested about 150 equations with different values of variables, and obtained that only 27 results out of 150 were "False" and all the other equations were found "True", on comparison. Hence the success rate of the proposed formula is 82%, while only 18% of the values were found out of range.

Hence the final values of the coefficients **α, β, γ and μ,** as obtained from the training phase are given below as:

α	β	γ	μ
-1.4	1.7	0.21	3.1

Based on these values, the proposed formula for checking the authenticity of a message is derived as:

$$\mathbf{m_{auth} = (-1.4)d+1.7\ n+0.21\ \Sigma c_i+3.1}$$

The above formula for message authentication $\mathbf{m_{auth}}$ is proposed with the following conclusions:

- The message authenticity $\mathbf{m_{auth}}$ depends on negative coefficient of density (d) of network, i.e. α= (-1.4).
- The coefficient "β" of number of nodes sending the same message (n), has high positive value, i.e. β=1.7 , thus affecting the value of $\mathbf{m_{auth}}$ to a greater extent.
- The message authentication $\mathbf{m_{auth}}$ depends on the summation of different costs at which different nodes send the message (Σc_i), with a coefficient "γ" with a small value, where γ = 0.21 .
- Along with these parameters, the message authentication $\mathbf{m_{auth}}$, also depends on a constant "μ" , where μ=3.1 .

Based on the above conclusions, the value of messag e authentication $\mathbf{m_{auth}}$, is calculated, and is generally obtained between the range 0-10. Therefore, its scaling is done between 0-10 with different range of values categorized as High, Medium and Low. Moreover, if the value of $\mathbf{m_{auth}}$ is obtained greater than 10 or less than 0 then it is categorized in the range of "High" and "Low" respectively.

Conclusion

In VANETs, vehicles broadcast information to other nearby vehicles in their surroundings The presence of malicious and faulty messages in the vehicular network can have a negative impact on the network performance. In this paper, we consider the harmful presence of faulty messages in the network and propose, an approach to minimize their dissemination in the network. For, this, a formula for message authentication has been proposed in which we assumed that message authentication depends on certain parameters which are directly proportional to it. These parameters includes- the density of the network, number of nodes sending the message and the different costs at which nodes send the message. We have classified the different range of values of authenticity as High, Medium & Low, and based on these classification, a message is either accepted or rejected from the network. The messages with High or Medium range of values of authenticity are considered as truthful and are accepted, while those with the value in the Lower range of authenticity are discarded as they are considered as faulty or malicious. The proposed formula for message

authentication has been verified by the experimental values. The result analysis shows that the success rate of the proposed formula is very high, thus making it efficient and reliable to calculate message authenticity and thereby preventing the propagation of faulty and malicious data in the network.

References

[1] Nadia Haddadou, Abderrezak Rachedi and Yacine Ghamri-Doudane, "Trust and Exclusion in Vehicular Ad Hoc Networks: An Economic Incentive Model based Approach", IEEE, Computing, Communications and IT Applications Conference, pp.13-18, 2013.

[2] Sourav Kumar Bhoi, Pabitra Mohan Khilar, "Vehicular communication: a survey", ©The Institution of Engineering and Technology, 3(3), pp. 204-217, August 2013.

[3] Nadia Haddadou, Abderrezak Rachedi, and Yacine Ghamri-Doudane, "A Job Market Signaling Scheme for Incentive and Trust Management in Vehicular Ad Hoc Networks", IEEE Transactions on Vehicular Technology, Institute of Electrical and Electronics Engineers, 64(8), pp.3657- 3674, 2015.

[4] Zhen Huang , Sushmita Ruj , Marcos A. Cavenaghi ,Milos Stojmenovic ,Amiya Nayak, "A social network approach to trust management in VANETs", Peer-to-Peer Netw. Appl., Springer Science+Business Media, LLC, 2012.

[5] Ao Zhou, Jinglin Li, Qibo Sun, Cunqun Fan, Tao Lei and Fangchun Yang, "A security authentication method based on trust evaluation in VANETs", EURASIP Journal on Wireless Communications and Networking, a Springer open journal, 2015.

[6] Jun Shao, Xiaodong Lin, Rongxing Lu and Cong Zuo "A Threshold Anonymous Authentication Protocol for VANETs", IEEE Transactions on vehicular technology, 20(20), 2015.

[7] Liqun Chen, Siaw-Lynn Ng, Guilin Wang, "Threshold Anonymous Announcement in VANETs", IEEE Journal on Selected Areas in Communications, 29 (3), pp.605-615, 2011.

[8] Nadia Haddadou, and Abderrezak Rachedi, "DTM2: Adapting Job Market Signaling for Distributed Trust Management in Vehicular Ad Hoc Networks", IEEE Press. IEEE ICC'2013, pp.1827- 1832, 2013.

[9] Chun-Ta Li, Yan-Ming Lai, and Cheng-Chi Lee , "Enhanced Threshold Anonymous Announcement in VANETs" , International Conference on Computing , E-Learning and Emerging Technology & International Conference on Advances in Computer , Electrical and Electronic Engineering - Sydney, Australia, Proceedings available @ IISRC -IJITCS , 12(2), pp-16-23, 2013.

[10]Isamu Teranishi, Jun Furukawa, and Kazue Sako. "k-times anonymous authentication" (extended abstract). In the Proceedings of ASIACRYPT 2004, pp.308–322. Springer, 2004.

[11]Uzma Khan, Shikha Agrawal and Sanjay Silakari, "A Detailed Survey on Misbehavior Node Detection Techniques in Vehicular Ad Hoc Networks", © Springer India J.K. Mandal et al. (eds.), Information Systems Design and Intelligent Applications, Advances in Intelligent Systems and Computing , 2015.

[12]Nazish Siddiqui, Mohd Shahid Husain, Mohammad Akbar, "Analysis of Security Challenges in Vehicular Adhoc Network", in the proceedings of international conference on advancement in computer engineering & information technology , IJCSIT, pp. s87-s90, 2016.

[13]M. Raya, P. Papadimitratos, I. Aad, D. Jungels, and J.-P. Hubaux, "Eviction of Misbehaving and Faulty Nodes in Vehicular Networks", IEEE journal on selected areas in communications, 25(8), october 2007.

[14]Hu Xiong, Zhi Guan, Jianbin Hu and Zhong Chen , "Anonymous Authentication Protocols for Vehicular Ad Hoc Networks: An Overview", Applied Cryptography and Network Security, Dr. Jaydip Sen (Ed.), InTech, pp. 53-71, March 2012.

[15]Sherali Zeadally, Ray Hunt, Yuh-Shyan Chen, Angela Irwin, Aamir Hassan, Vehicular ad hoc networks (VANETS): status, results and challenges, © Springer Science+Business Media, LLC, pp. 217-238, December, 2010.

[16]Preetam Suman; Amrit Suman, An Enhanced TCP Corruption Control Mechanism For Wireless Network, HCTL Open International Journal of Technology Innovations and Research, Volume 1, January 2013, Pages 27-40, ISSN: 2321-1814, ISBN: 978-1-62776-012-6.

[17]Prashant Tiwari; Varun Prakash Saxena; Raj Gaurav Mishra; Devendra Bhavsar, Wireless Sensor Networks: Introduction, Advantages, Applications and Research Challenges, HCTL Open International Journal of Technology Innovations and Research (IJTIR), Volume 14, April 2015, eISSN: 2321-1814, ISBN (Print): 978-1-62951-946-3.

This article is an open access article distributed under the terms and conditions of the Creative Commons Attribution 4.0 International License (https://creativecommons.org/licenses/by/4.0/).

© 2016 by the Authors. Licensed by HCTL Open, India.