I J C T A, 9(17) 2016, pp. 8499-8508

CTS: A Credit based Threshold System to Minimize the Dissemination of Faulty Data in Vehicular Adhoc Networks

Nazish Siddiqui* **and Mohd Shahid Husain***

ABSTRACT

In VANETs, vehicles broadcast messages to other nearby vehicles to exchange information among them about their surroundings. This broadcasting of messages may enhance road safety and traffic efficiency, which is possible only if the messages announced are true and could be relied upon. However, the presence of faulty and malicious messages in the network may lead to greater security threats. This paper proposes an approach called Credit based Threshold System , termed "CTS", to minimize faulty data dissemination in vehicular network to improve the security and reliability of the network. The CTS approach uses two of the most common and efficient techniques to achieve the property of message reliability- the Threshold method and the Credit-based model. Both these concepts are integrated together to design an approach that mainly focuses on message authentication. The main idea is to check for the authenticity of the message, so as to ensure the message being truthful and reliable; and consequently, reduce the propagation of malicious and faulty messages from the network. A message with a higher value of authenticity is accepted and rest are discarded. In this paper, we have also proposed, a formula for message authentication.

Keywords: VANET, CTS, Authenticity, Credits, Faulty Threshold.

I. INTRODUCTION

Efficiency of transportation and providing safety are the main driving forces for the evolution and development of vehicular ad hoc networks. In VANET, vehicles equipped with communicating and computing devices [2,15], are able to communicate with each other, as well as with the Base stations (Road side units) at different locations along the road. The information transmitted among them have the potential to increase the safety of vehicular transportation significantly. With the recent progress in various technologies employed in VANETs, it has become feasible to enhance safety by alerting vehicles in proximity to be aware of the situation, by earlier detection of potential dangers, so that appropriate actions can be taken.

Data exchanged among the nodes in VANETs often play an exclusive part in providing road safety and traffic efficiency [12]. Hence the information transmitted must be accurate and truthful, for the safety of the network. But some malicious vehicles may try to gain unfair advantage on the road or to cause some mishaps by sending false and fake information into the network. Hence the receiver must check for the authenticity of the sending vehicle, before taking any action based on the messages received from the sender. Besides, providing authentication of the sender, if the messages received could be checked for their authenticity, then the network could be made far more safe and secure to a greater extent.

This paper proposes an approach called Credit based Threshold System , termed "CTS", to minimize the faulty data dissemination in the vehicular network to improve the security and reliability of the network by ensuring that the messages announced are true and could be relied upon. Two of the most common and efficient techniques to achieve this property of message reliability are Threshold method [6,7,9] and the Credit-based model [1,3,5,8].

* Department of Computer Science & Engineering, Integral University Lucknow, India, *E-mail: nazishcs@iul.ac.in; siddiquisahil@gmail.com*

We propose in our work that the "Credit based Threshold System", is based on both threshold concept and the Credit based model with a distinction with the existing approaches, that instead of looking only for the credit score of the reporting vehicles, the density of the network, total credit score along with the threshold value of number of nodes sending the message is checked, so as to ensure that the message could be relied upon. The main idea used to implement the work is to check for the authenticity of the message, so as to reduce the propagation of malicious and faulty messages from the network. In this work, a formula for message authentication is derived and proposed. A message with high value of authenticity is accepted and rest are discarded. Simulation results shows the advantage of using this method.

The remainder of this paper is organized as follows: In Section II, we present the related works dealing with the Credit based model and the threshold method in literature. In Section III ,we present our solution based on CTS approach. Section IV presents the implementation of the work. In section V, the performance evaluation and simulations results are discussed. Finally, Section VI concludes this paper.

II. LITERATURE REVIEW

To overcome misbehaviors in VANET, various approaches have been proposed. Some of the notable work among them are discussed here .

Nadia et al. in [1] proposes an approach called VIME that stands for Vehicular incentive model with exclusion for malicious nodes. It is inspired from the signaling theory of economics, which is based on managing the credit count that each node receives at the beginning of the application. VIME[1] is based on two concepts. On one hand, a node pays an appropriate cost for each message sent by it on the network, which is seen by other nodes receiving the message as a guarantee about the truthfulness of the information from the source. On the other hand, nodes are rewarded for their cooperation in the network.

In an another approach [3],[8], the harmful presence of malicious nodes, spreading forged and false data; and the selfish nodes, that cooperate only for their own benefit in the network has been addressed by Nadia et al. in their work. To deal with this, the authors proposed a model called DTM2 [3],[8] that stands for Distributed Trust Model, which is adapted from the job market signaling model. DTM2 is based on the concept of allocating credits to nodes and managing these credits securely. To access data in the network, it requires a reception cost, thus motivating selfish nodes to participate in the network to earn credits. Moreover it also requires cost of sending; thus ensuring higher sending cost for malicious nodes, thus limiting their participation in the network.

The trust management schemes in VANETs is adversely affected by the problem of information cascading and oversampling [4], that is commonly present in social networks. To overcome this problem, Zhen et al. in [4], proposed a novel voting scheme. According to this, each vehicle has different voting weight as per its distance from the event about which the information has been broadcasted. The vehicle, more closer to the event possesses higher weight.

Another approach of dealing with the misbehavior in the network is the threshold method of authentication. Shao et al. in [6], proposed a new authentication protocol for VANET by using a new group signature scheme in a decentralized group model. It is featured with threshold authentication and efficient revocation of nodes. In the decentralized group model, instead of the centralized authority, the whole VANET is divided into several groups; with each group under the control of distinct RSU. Whereas, in the threshold authentication method, a message is accepted by the receiver, only if it has been confirmed by a threshold number of vehicles.

Liqun et al. in [7], proposed a Threshold Anonymous Announcement service (TAA) simultaneously against both authorized parties and adversaries. In this scheme, it is assumed that a vehicle is equipped with a tamper-resistant black box [7][14], [7][17], a common approach in VANET. The TAA scheme improves

the performance as a good balance is maintained between hardware and software. However, Chun et al. in [9], proposed some simple modifications on the Chen et al.'s scheme in [7].

All these approaches deals with various concerns of VANET and its security in the presence of malicious node and malicious data. However, we have integrated these approaches and proposed a new scheme called Credit based Threshold System. Our solution, CTS, is able to cope with the presence of both malicious and selfish nodes in a VANET. It is discussed in the next chapter.

III. CREDIT BASED THRESHOLD SYSTEM

This paper proposes an approach called Credit based Threshold System (CTS), to improve the security and reliability of the vehicular network, by minimizing the propagation of faulty and malicious data in the network. A Credit based Threshold System (CTS), as the name suggests, comprises the concept of the following two approaches in VANET:

- Threshold Method.
- Credit based Model.

In a threshold method, a message is believed to be reliable if a vehicle receives messages of the same content announced by a number of distinct legitimate vehicles of a certain threshold within a time interval. In other words, receivers are allowed to only accept a message that has been confirmed by a threshold number of vehicles. Whereas, in a Credit-based model, the reliability of a message is evaluated according to the total credit score of the reporting vehicles; a node pays an appropriate cost for each sent message, which is seen by the receivers as a guarantee from the source about the truthfulness of the information, higher cost reflects the likelihood a vehicle is announcing reliable messages. The Credit based system is based on the concept that each node is credited at its first connection to the network with a fixed amount of credits. For each sent message, the source pays some cost depending on different factors[1,3,5]. This represents a guarantee of trustfulness for the receivers, and an investment for the source since a corresponding reward will be given to the node if the shared data is considered as valid. Therefore, a node can only receive and send messages if it has credits left, or else it is detected and excluded from the network.

The Credit based Threshold System (CTS), scheme is based on both threshold concept and the Credit based model with the distinction with the existing approaches. Here, the message is checked for its authenticity based on certain parameters- the density of the network, total credit score and the threshold value of number of nodes sending the message. If the message is found authentic or if the message has higher authenticity it would be accepted or else discarded. For this. the authenticity of messages is checked on the scale of 0-10 with different range categorized as High, Medium and low. The messages with Higher or Medium authenticity are more likely to be genuine. Similarly the messages with authenticity Low could be discarded.

The proposed formula to check the authenticity of the message, is given below

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

3.1. CTS Based Network Model

The network model of the vehicular adhoc network by using CTS based approach comprises of several components similar in features and functionalities to a traditional vehicular network.

- Central Authority (CA) - The central authority (CA) is the central governing body that has is the trusted authority (TA) at the centre.
- Road Side Unit (RSU) – The Road Side Unit (RSU) is the local trusted authority. It is the base station at distinct locations on road.

- Vehicles –These include smart cars or other vehicles equipped with latest technology.
- On Board Unit (OBU)- It is the main processing unit present in a vehicle, equipped with a (short range) wireless communication device along with some other optional potential communication devices for efficient and safe communication.
- Tamper Proof Module (TPM)- A tamper proof module is a tamper resistant device (TRD), that cannot be attacked by the attacker. It is used to provide security in data processing by the vehicles.

3.2. CTS Process

The Credit based Threshold Method is based on the concept to ensure the authenticity of a message ,so that it could be accepted or rejected from the network. Each vehicle will first register itself with the central authority (CA). The CA will provide the vehicle with a certificate to ensure its legitimacy in the network. Along with the certificate, CA will also provide the vehicles with some credits at the beginning so that it could access the network. Now, as the vehicle joins the network of an RSU, it first verifies the certificate of the vehicle and then provide it with a random pseudo id that is provided to it by the CA.

When a sender node Vs wishes to transmit a message into the network, it sends the message "msg", along with some cost "c". This cost is actually some amount of credits that is kept on stake along with the message. This act as the guarantee for the message being truthful; higher the cost, higher will be the probability of the message being genuine and true. As the vehicle send the message its credit count will automatically decrement by an amount equal to the cost at which the message is sent.

The receiving node Vr, when receives the message will check for the following three 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 send the message.

It checks for the authenticity of the message m_{auth} based on the above parameters by the proposed formula:

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

where the value of $\alpha = -1.4$, $\beta = 1.7$, $\gamma = 0.21$ and $\mu = 3.1$ as derived through the training phase, discussed in the next section of the paper.

On obtaining and verifying the value of message authenticity m_{auth} on the scale of 0-10, the message is either accepted or rejected as per the proposed conditions. If the receiving vehicle V_r finds the message correct, it returns an acknowledgement (ACK) to the sending vehicles and as a result of sending the true message, its credit count will increment by an amount equal to double the cost at which the message is sent. While, in case the message is rejected, no such acknowledgement is sent.

3.3. Computation of the Credit Count

When the sending vehicle Vs sends the message "msg", along with some cost "c", i.e.

$$Data = msg + c;$$

The tamper proof module (TPM) present in Vs, automatically decrement its credits by the amount "c", and its new credit score will become as

$$cr_{new} = cr_{old} - c;$$

Similarly, when the message is accepted as the genuine message, then the receiver sends the ack back to the sending node. The TPM of the sending node will then increment its credits by the amount double to the cost at which the message was sent, i.e. "2c", and its new credit score will be updated as

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

3.4. Computation of Message Authenticity

The authenticity of the message is checked by the proposed formula: $m_{auth} = \alpha d + \beta n + \gamma(\Sigma c_i) + \mu$; 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;
}
```

IV. IMPLEMENTATION & RESULTS

For the implementation, of the CTS approach, the proposed formula to check the authenticity of the message has to be verified. The proposed formula for message authentication is given below:

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

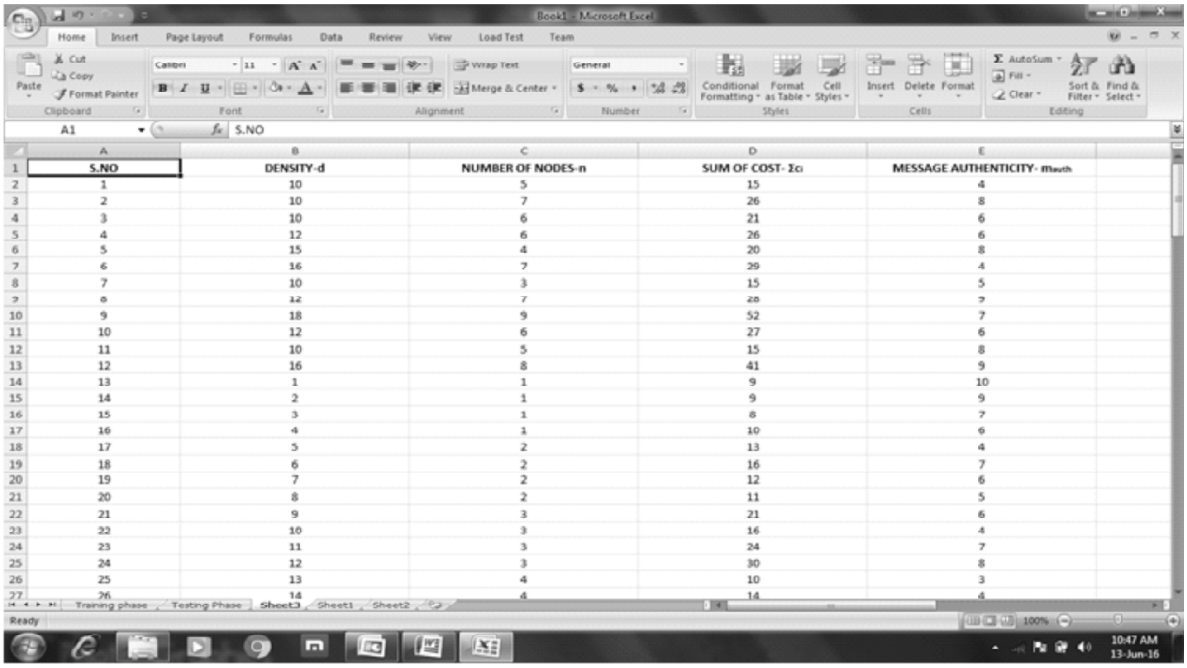
To obtain and verify the values of various constants á, â, ã and µ used in the above mentioned formula, there are three main phases, this work has undergone through-

- Training Phase
- Testing Phase and
- Simulation

4.1. Training Phase

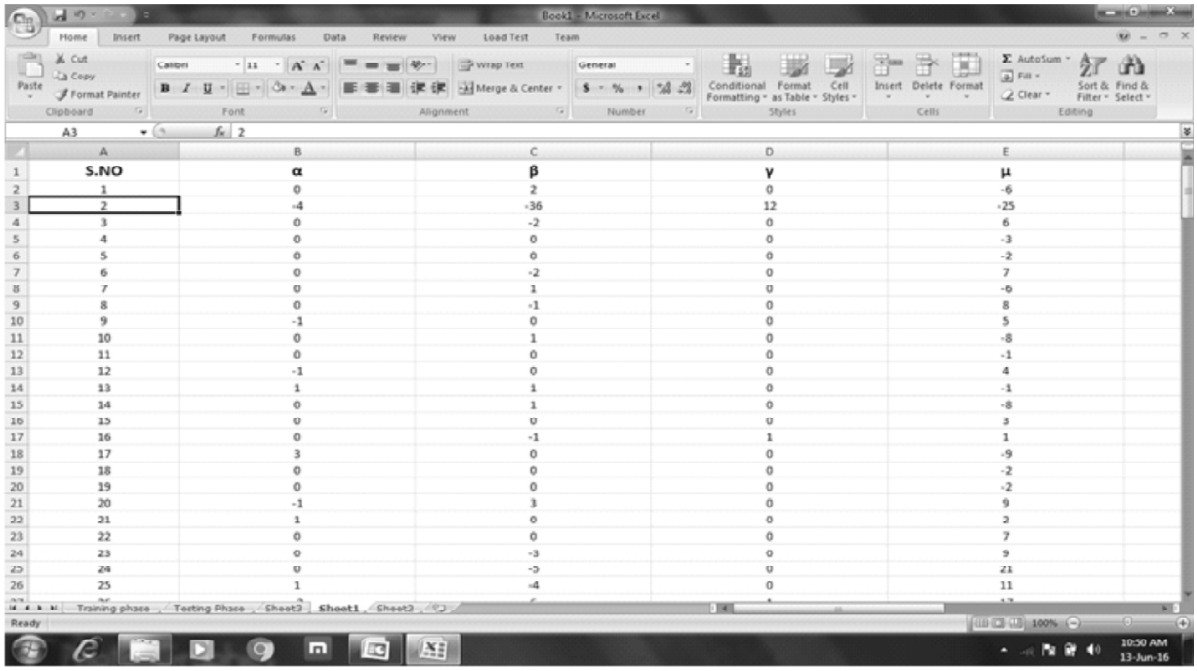
In this phase, to obtain the values of α, β, γ and μ, the values of other variables d, n, c_i and m_{auth} used in the formula are altered. For this, about 150 different linear equations based on the above proposed formula are formed and different values of the variables d, n, c_i and m_{auth} are assigned.

The table in Figure1 shows some of the assumed values of the variables d, n, c_i and $m_{auth.}$ These 150 equations are further taken into combinations of different 200 sets of 4 linear equations together to determine the values of α, β, γ and μ. After making the combination sets of 4 of these equations together, they are solved and the values are obtained. This is given below in the form of a table in Figure 2:



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	7
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: Assumed values of the variables -d, n, c_i and m_{auth}



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	3
22	0	0	0	7
23	0	-3	0	9
24	0	-9	0	21
25	1	-4	0	11

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

Once 200 values of these coefficients are obtained, their average is calculated to find the generalized values of the coefficients α, β, γ and μ which are obtained as:

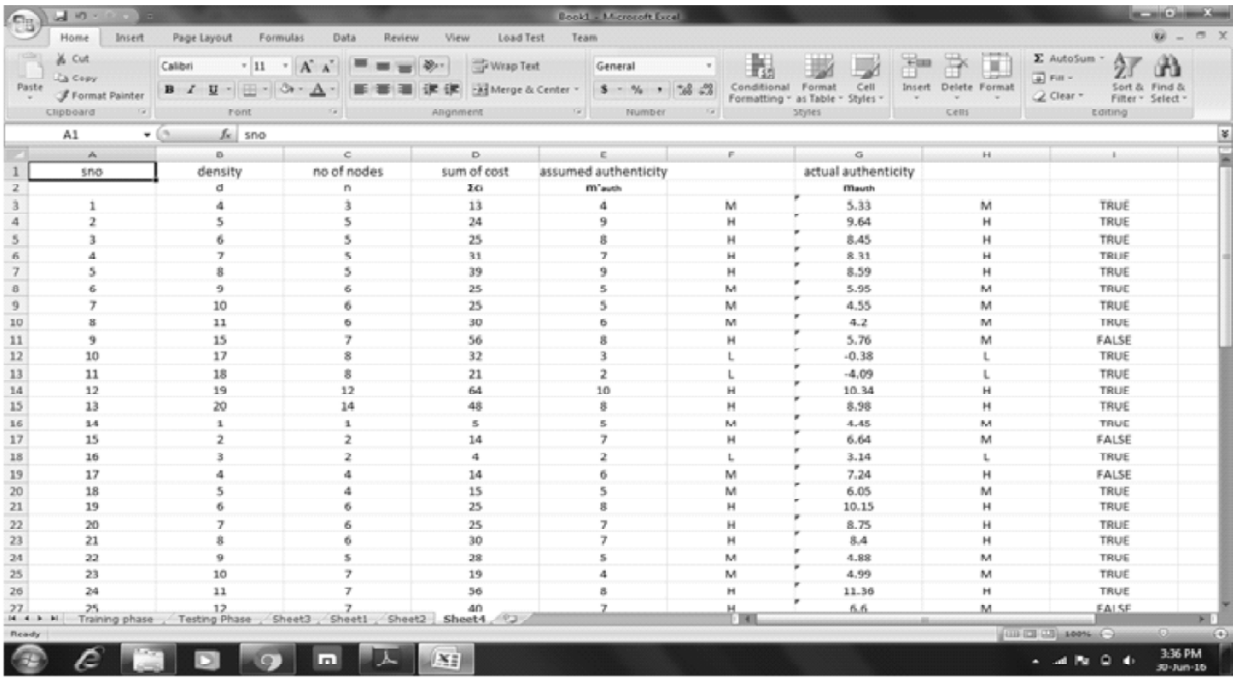
1. Coefficient of density, $\alpha = -1.4$
2. Coefficient of number of nodes sending the message, $\beta = 1.7$
3. Coefficient of summation of different cost at which message is sent, $\gamma = .21$
4. Constant, $\mu = 3.1$

4.2. Testing Phase

Testing phase deals with the testing of the obtained values of **α, β, γ and μ.** For this, about 150 different linear equations based on the above proposed formula are formed and different values of the variables **d, n, and c_i** are assigned along with the value of assumed authenticity **m'_{auth}** and the value of actual authenticity **m_{auth}** is determined by solving the equations individually. The Authenticity range of message is proposed as under:

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

On comparing the values of assumed authenticity **m'_{auth}** and the actual authenticity **$m_{auth,}$** in Figure 3, it is found that both the values are nearly same in almost most of the cases. The comparison is done on the basis of range of values, categorized as High, Medium and Low. From about 150 equations tested, it is found that only 27 results were wrong and all the other equations were found correct.



sno	density	no of nodes	sum of cost	assumed authenticity		actual authenticity		
	d	n	Σci	m'auth		mauth		
1	4	3	13	4	M	5.33	M	TRUE
2	5	5	24	9	H	9.64	H	TRUE
3	6	5	25	8	H	8.45	H	TRUE
4	7	5	31	7	H	8.31	H	TRUE
5	8	5	39	9	H	8.59	H	TRUE
6	9	6	25	5	M	5.95	M	TRUE
7	10	6	25	5	M	4.55	M	TRUE
8	11	6	30	6	M	4.2	M	TRUE
9	15	7	56	8	H	5.76	M	FALSE
10	17	8	32	3	L	-0.38	L	TRUE
11	18	8	21	2	L	-4.09	L	TRUE
12	19	12	64	10	H	10.34	H	TRUE
13	20	14	48	8	H	8.98	H	TRUE
14	1	1	5	5	M	4.45	M	TRUE
15	2	2	14	7	H	6.64	M	FALSE
16	3	2	4	2	L	3.14	L	TRUE
17	4	4	14	6	M	7.24	H	FALSE
18	5	4	15	5	M	6.05	M	TRUE
19	6	6	25	8	H	10.15	H	TRUE
20	7	6	25	7	H	8.75	H	TRUE
21	8	6	30	7	H	8.4	H	TRUE
22	9	5	28	5	M	4.88	M	TRUE
23	10	7	19	4	M	4.99	M	TRUE
24	11	7	36	8	H	11.36	H	TRUE
25	12	7	40	7	H	6.6	M	FALSE

Figure 3: Comparison of Assumed Authenticity m'_{auth} and Derived Authenticity m_{auth}

V. PERFORMANCE EVALUATION

5.1. Result Analysis

In the implementation section of the proposed work, the formula for message authentication has been derived and verified by comparing the actual values with the assumed ones. The proposed formula for checking the authenticity of a message is obtained as:

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

The above formula for message authentication m_{auth} is proposed with the idea that the authenticity of a message, depends on the following parameters- density of the network (d), number of nodes sending the message (n) and the sum of different costs at which different nodes send the message (Σc_i). From the above formula, following are the conclusions:

- The coefficient "α" of density (d) of network, has a negative value, i.e. $\alpha = (-1.4)$.
- The coefficient "β" of number of nodes sending the same message (n), has high positive value, i.e. $\beta = 1.7$.
- The summation of different costs at which different nodes send the message (Σc_i), has a coefficient "γ" with a small value, where $\gamma = 0.21$.
- Along with these parameters, the message authentication $m_{auth,}$ also depends on a constant "μ" , where $\mu=3.1$.
- From the above formula, it is also clear that the message authenticity m_{auth} is highly affected by the threshold value, i.e. the number of nodes (n) sending the message, as it has high value of its coefficient β.

Based on the above conclusions, the value of the variable m_{auth} , when calculated by varying the values of different parameters, is generally obtained between the range 0-10. Hence, the scaling of the values is done between 0-10 and it is categorized into three parts- High, Medium and Low. However, the values greater than 10 are categorized in the range of "High" and the values smaller than 0 are categorized in the range of "Low".

5.2. Performance Analysis

We evaluate the performance of our approach by observing that the number of faulty messages has been reduced in the network. The formula for authenticating the message is verified by simulating the VANET scenario with the proposed approach through ns2 simulator. On simulating the network, some data is collected to analyze the behavior of the VANET using CTS approach.

The graph in Figure 4 gives a comparison of the throughput of the vehicular adhoc network with and without using the CTS approach by varying the number of nodes in the network and it clearly shows that the throughput of the network is increased when VANET scenario is using the CTS based approach.

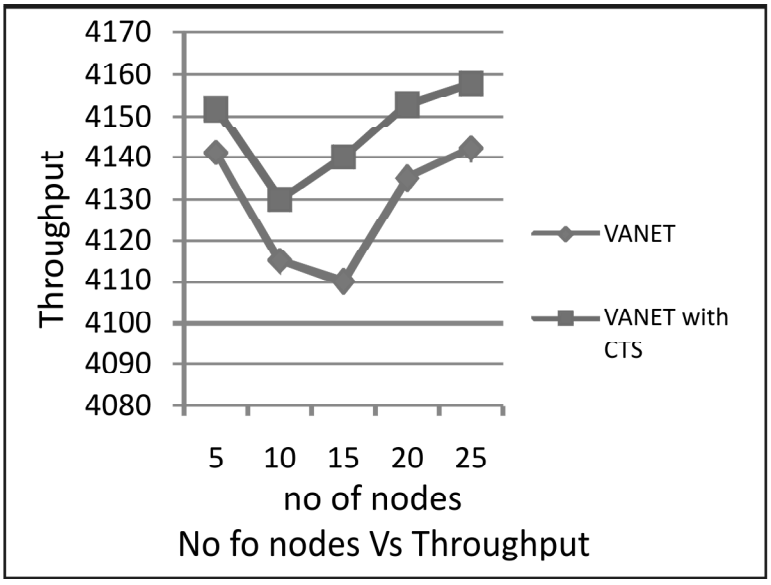


Figure 4: No of nodes Vs Throughput

Similarly, the graph in Figure 5, gives a comparison of the faulty messages present in the vehicular adhoc network with and without using the CTS approach by varying the number of nodes in the network and it clearly shows that the dissemination or presence of faulty messages in the network is decreased when VANET scenario is using the CTS based approach.

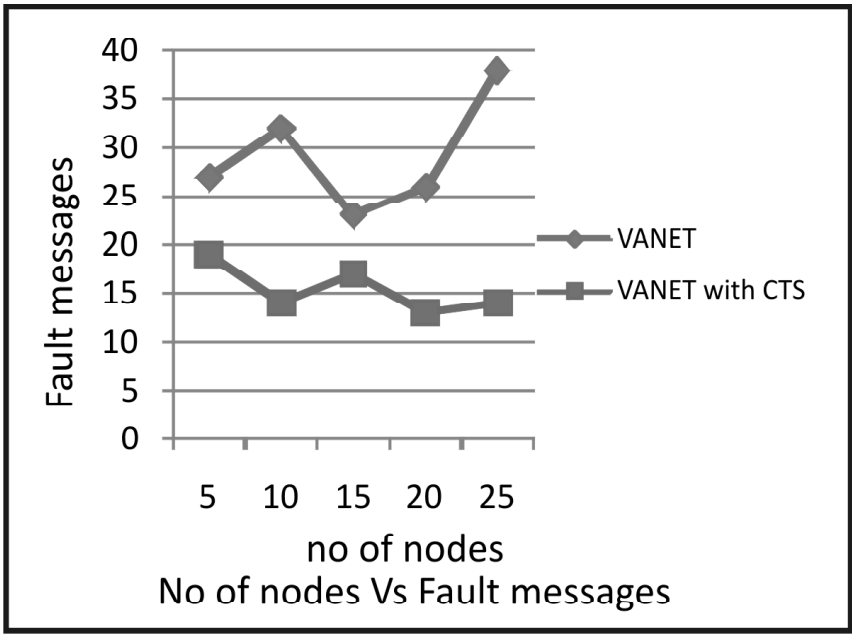


Figure 5: No of nodes Vs Fault Messages

VI. CONCLUSION

The presence of malicious and faulty messages in the network is an open challenge in a vehicular adhoc network. In this paper, we propose, a Credit based Threshold System approach to minimize the dissemination of faulty messages in the network. The main idea used is to calculate the value of message authenticity and classify it as being High, Medium & Low, so as to decide whether to accept or reject a message from being transmitted in the network. A formula for message authentication is proposed that clearly shows that message authentication depends on certain parameters- the density of the network, number of nodes sending the message and the different costs at which nodes send the message; and is thereby directly proportional to them with some amount of coefficients and a constant. The messages with authenticity High or Medium are more likely to be true and genuine , while the message with the value of authenticity low is considered as faulty or malicious and is discarded. We simulated our work using ns2 simulator. The result analysis of simulation shows that the number of the faulty messages dissemination is reduced when CTS approach is used in vehicular network. As far as the performance analysis is concerned, the proposed scheme provides better throughput as compared to the general vanet infrastructure. Hence, we propose our approach for the minimization of faulty data dissemination in Vehicular adhoc network, which on analysis is found more reliable and efficient.

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, VOL. XX, NO. XX, 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, Proceedings @ IISRC - International Journal of Information Technology & Computer Science (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, LNCS 3329, 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] Jose Maria de Fuentes, Ana Isabel Gonzalez- Tablas, Arturo Ribagorda, "Overview of security issues in Vehicular Ad-hoc Networks", Handbook of research on Mobility and Computing, 2010.