International Journal of Computer Networks and Applications (IJCNA)
Volume 2, Issue 4, July – August (2015)

RESEARCH ARTICLE

Prioritized and Secured Data Dissemination Technique in VANET Based on Optimal Blowfish Algorithm and Signcryption Method

M. Selvi
Research Scholar, S.T. Hindu College, Nagercoil-2, India

Dr. B. Ramakrishnan
Associate Professor, Department of Computer Science and Research Centre,
S.T. Hindu College, Nagercoil-2, India.

Abstract –- All the way through cooperative behaviour of the vehicular nodes information dissemination in VANETs occurs. Vital information like traffic jam, emergency brake procedures, road conditions, accident warnings, bad weather conditions, etc are messages transmitted in vehicular network. Misbehaviours and false hindering is a serious issue in VANET if any vehicles maliciously send messages. Deviation from the average behaviour of other vehicular nodes in the Consecutively to make VANET a secure network, detection of misbehaviors and the malicious vehicular nodes concerned in such misconducts is tremendously imperative. In this paper we have proposed a message broadcasting and message priority assignment in vehicular networks to resolve this problem. Initially the messages are prioritized using SMTP metric. we are using the three levels of priority's those are emergency, general request and entertainment request and then finally secured information transaction via., optimal blowfish algorithm based signcryption technique. The performance of the proposed algorithm is analyzed with existing techniques.

Index Terms - VANET, data dissemination, Sybil Attack, DOS, Signcryption, blowfish, Cuckoo Search.

1. INTRODUCTION

To boost the safety and for the comfort of road traffic users Vehicular Ad Hoc Network (VANET) is envisaged by the automotive industry as one of the key to future technology. Including safety, traffic management, and infotainment, VANETs could maintain a large number of applications. Depending on the reliable working of these applications proficient transmission of diverse types of messages with required quality of service works [1]. Especially to aid safety applications in VANET broadcasting in Vehicular Ad Hoc Networks (VANET) is a technique used [2]. A proficient data transaction technique is required for a safety application to transmit data to the vehicles. Resembling emergency to vehicles, collision and reverberation, driver assistance are comes under safety applications. Likewise, data transaction and traffic related information are comes under non-safety applications. The Intelligent Transportation Systems (ITS) have been measured as a significant communication infrastructure by Vehicular Ad Hoc Networks (VANETs) [3, 4].

To improve roadway system efficiency VANET will greatly enhance driving safety and experience. Heavily based on a secure and reliable infrastructure widespread deployment VANET is used for presenting accurate traffic and road system data [5]. But too, endow with security in a vehicular network is more complex than in other networks such as WSN, because of high mobility and broad range of vehicles. Nowadays, the security issues, such as confidentiality, authentication, non-repudiation, localization and verification of data, are still the most important problem to be solved that affect the quality of service (QoS) in vehicular network. Usually Vehicular ad hoc networks are activated among vehicles moving at high speeds, therefore their communication relations can be altered often [6, 7]. In such a highly dynamic environment, traditional security solutions face many challenges in VANET caused by the complex vehicular communications system, dynamic user groups, real time constraints, etc. The privacy and confidentiality of the transmitted messages should be protected in VANET communications [8]. Necessary enhancements are needed for infotainment, driver assistance and vehicular safety applications in order to avoid some security issues.

The traffic status can help the driver making the appropriate decisions in receiving data. It allows the driver to enhance the current context, as her understanding is not controlled to what is on her field of visualization. In a bottleneck or a slippery road, the vehicular emergency warning systems cooperatively communicate with every one other when they sense a dangerous event. By the On-Board Unit (OBU), a potential warning road condition is noticed and the warning message system produces a new message and circulate it beyond the shortest transmission range. At times, the received data can change the driving task, they should be trustworthy, and in other words the received data must exactly reflect the road traffic status [9, 10, 11].

Alteration or Data forgery must be totally avoided, since there are numerous ways to execute attacks in this area. In this data creation phase, both the sensors and their connections among the OBU and the Hardware Security Module (HSM) can be effortlessly attacked therefore fake data can be produced. To manipulate the relayed data, the transmission message routing in VANET permits the intermediary nodes. In the end with the importance of stocking fake data or getting a wrong conclusion from data evaluation, the storage and evaluation phases can as well be attacked if they are not executed in a HSM [12].

2. RELATED WORKS

Esther Palomar *et al*. [12] have demonstrated that to obstruct the dissemination of false warning events in VANETs was possible and limit the quantity of messages a node can send within a specified period of time by implementing the well-known cryptographic techniques. They have presented two simple concepts namely the use of certificates and Proof-of-Work (POW) systems respectively offer accountability and combat spam and denial of Service attacks. Basically, their scheme not only depress nodes from broadcasting false event warning messages but also provides an effective non-repudiation proof for various types of dishonest behaviour inside a VANET.

Xuejiao Liu *et al*. [13] have proposed a hierarchical access control with authentication scheme for transmitted messages with security assurance over VANET. By extending cipher text-policy attribute based encryption (CP-ABE) with a hierarchical structure of multiple authorities, the scheme not only achieves scalability due to its hierarchical structure, but also inherits fine grained access control on the transmitted messages. Also by exploring attribute based signature (ABS), the scheme can authorize the vehicles that can most appropriately deal with the message efficiently.

Sofiane Zemouri *et al*. [14] have proposed a distributed dissemination protocol which was derived from a novel cooperative forwarding mechanism for safety messages in urban areas, dubbed ‘‘Road-Casting Protocol (RCP)’’. Moreover, to ensure better control of the network load an accurate definition of the Region of Interest (RoI) (i.e. the geographical scope) of each broadcasted safety message was also developed. They obtained more than 95% packet delivery ratio and minimum end-to-end delay using simulation.

Jalay S Maru et al. [15] have described the objective of the work as to enhance the delivery of a message from RSU to vehicle. Without affecting the reliability and service ratio, the message can be transferred from RSU to vehicle which is described by them based on priority based scheduling protocol.

Saurabh Kumar Gaur et *al*. [16] have described the future vehicular applications, which could be supported by the position of VANETs that indeed turn out to be the networking platform. In deciding the networking framework over, which the future vehicular applications would be deployed they have analyzed the critical factors. For making VANETs a reality in the near future a reactive research effort was needed.

Uzma Khan et al. [10] et al. presented a detailed survey on some of the important research works projected on identified malicious nodes and misbehavior in VANETs. Additionally to the details about the methods used for misbehavior detection, nature of misbehavior, their paper classifies the system for enhanced perceptive and also sketches numerous research scopes to create VANET additional reliable and secure.

Mainly due to rapid changes in network topology and frequent fragmentation, data dissemination in VANET environment is a challenging task. Moumena Chaqfeh et al. [11], along with optimization strategies under two basic models; the push model, and the pull model have surveyed the existing data dissemination techniques and their presentation modeling advancement in VANETs.

Network which doesn’t have any infrastructure and contains only the wireless equipped vehicles are called VANET. Travelling delay, congestion, Traffic related issues are inevitable in this dynamic road communication system. In order to resolve these problems and construction of more and better roads and highways and to build up safety applications like accident notification, traffic congestion avoidance and traffic congestion warning that lead to an important reduction of critical traffic events numerous measures are executed. These applications make use of a range of data obtained from the road, surrounding vehicles and the host vehicle. The information should be transmitted right away with high reliability and low delay. Vishal Kumar and Narottam Chand [17] have investigated the data scheduling approaches presented to plan the essential data considering vehicle to vehicle, infrastructure to vehicle or vehicle to infrastructure communication.

The procedure of sending a message from one node to all other nodes in an ad hoc network is broadcasting. It is a primary operation for communication in ad hoc networks as it permits for the update of route discovery, network information and other operations as well. M.Chitra and S. Siva Sathya [5] in VANET have reviewed the pros and cons of different broadcasting methods. Also, the broadcast suppression and broadcast storm problem techniques for broadcasting in Vehicular Ad hoc Networks (VANET) were discussed, since blindly broadcasting the packets cause numerous problems that influence the quality of service in VANET. Sequentially a survey of some of the existing broadcast suppression techniques in vehicular environment were done to stay away from broadcast storm problem in their paper provides.

In Vehicular Ad Hoc Network (VANET), when the driver does not respond quickly there is a possibility of event of accidents within a cluster,. To resolve this problem, S. Lakshmi and R.S.D.Wahida Banu [3] for using VANET they have projected a Prioritized Directional Broadcast Technique for Message Dissemination. Originally, message priority assignment technique was used in three levels of message priorities, in which very urgent, urgent and general messages are measured. Then for finding the candidate relay node inside the coverage area of the source binary partition phase was then presented. During emergency message dissemination, simulation results illustrate that their approach offer high reliability.

3. PROPOSED METHODOLOGY

VANET applications can be classified into several families of classifications. These classifications range from two to several categories according to the degree of accuracy. VANET is composed of vehicles that are equipped with computing, sensing, and communication capabilities. Most important and major problem with VANET is, there is a chance of accident within a cluster if the driver does not react quickly.

In order to overcome this issue, we have proposed a Secured and prioritized message dissemination technique in VANET. Based on the number of messages, a priority should be assigned in terms of some keywords. The types of the messages will be emergency request, general request and entertainment request and then finally secured information transaction.

3.1. Message Prioritization

In this research, the Priority based Directional Broadcast is proposed to avoid the accidents. Initially, message priority assignment is used. In message priority, the three types of priorities such as emergency request, general request and entertainment request are used. If a very urgent request is received, then the highest priority will be assigned and the message is served as an emergency and processed immediately.

Initially the keywords which are used to identify the message priority is stored in a separate document. Once the message arrived, the priority of the message is automatically assigned. The keywords are categorized for each message priority such as emergency, general request and entertainment request. Message priority can be assigned based on the similarity calculation between messages and keywords already stored. A similarity measure is presented namely SMTP (similarity measure for text processing) for the two messages. Several characteristics are embedded in this measure. It is a symmetric measure.

There are 3 cases to measure the similarity between the messages such as (a) The feature appears in both messages, (b) the feature appears in only one message and (c) the feature appears in none of the messages. Based on the preferable properties mentioned above, we present a similarity measure, S_{SMTP} for t_1 and t_2 is,

$$S_{SMTP}(t_1,t_2)=\frac{F(t_1,t_2)+\gamma}{1+\gamma}$$

Where, F is the function, which is defined for the two messages $t_1 =< t_{11},t_{12},...,t_{1m} >$ and $t_2 =< t_{11},t_{12},...,t_{1m} >$ and as follows:

$$F(t_1,t_2)=\frac{\sum_{j=1}^{l} N*(t_{1j},t_{2j})}{\sum_{j=1}^{l} N_{\cup}(t_{1j},t_{2j})}$$

Where,

$$N*(t_{1j},t_{2j})=\begin{cases} 0.5\left(1+\exp\left\{\left(\frac{t_{1j}-t_{2j}}{\sigma_j}\right)^2\right\}\right) & ,if\ \ t_{1j}t_{2j}>0 \\ 0 & ,\ if\ t_{1j}=0\ \ and\ \ t_{2j}=0 \\ -\gamma & ,\qquad Otherwise \end{cases}$$

$$\sum_{j=1}^{l} N_{\cup}(t_{1j},t_{2j})=\begin{cases} 0 & ,if\ t_{ij}=0\ and\ t_{2j}=0 \\ 1, & \qquad otherwise \end{cases}$$

As mentioned in the above eqn. for case (a); the lower bound was set to 0.5 where σ_j is the standard deviation of all non zero feature values for the keyword z_j. For case (b) $-\gamma$ is set to represent the non zero feature value. Based on the similarity measure, the message can be prioritized and the high priority messages are served first.

3.2. Secured Data Dissemination using Hybrid signcryption Algorithm

Transferring high sensitive data between the vehicles is a risky job in VANET. Possibility for hackers to extract the messages. It is essential to secure the secret messages from adversaries in applications such as military, air force etc. In order to avoid such circumstances, we need a secure message dissemination technique. VANETs generally use a combination of broadcast, multicast, uni-cast dissemination messages between the vehicles, depending on the type of packets that we need to send. Vehicle can broadcast messages to all vehicles in all directions, or can be directed to a group of vehicles or one vehicle behind it. Every vehicles dynamically update the information while transaction. Each and every vehicle knows about this information broadcasting and updation.

Here we are proposed an optimal signcryption [18] based on KEM and DEM, the KEM is executed based on the Key Derivation Function (KDF) by means of the secure pseudo random number generation technique. The KEM technique is used to transfer the secret key along with some additional keys which are necessary for encryption process

The additional information's are extracted from the secret key by means of pseudo random number functions. Advanced Encryption Standard (AES) algorithm is used inside a DEM process in Signcryption algorithm. In our suggested method, the AES algorithm is replaced by optimal Blow fish algorithm based on Cuckoo search algorithm. Figure 1 symbolizes the block diagram of the secured data transaction technique.

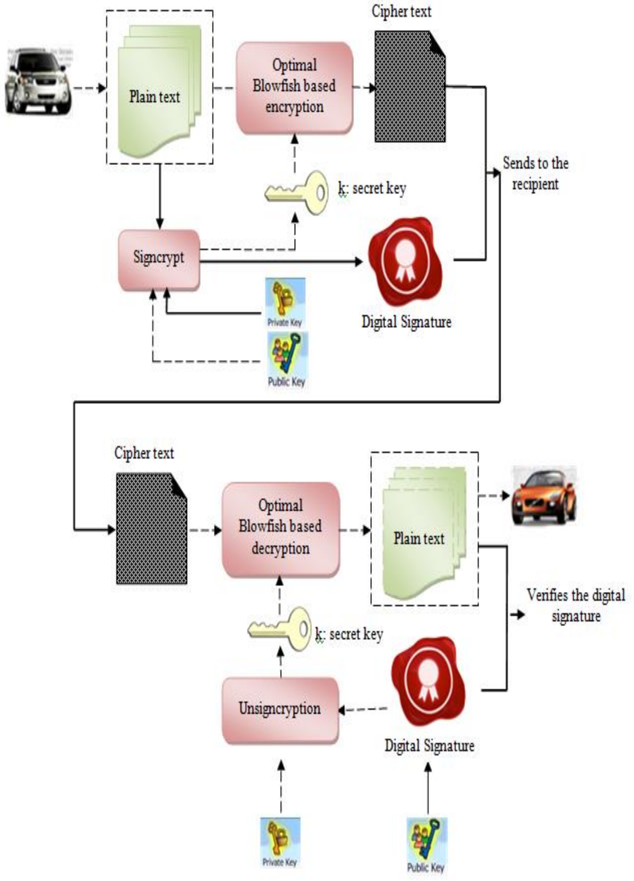

Figure 1: Proposed Optimal Signcryption algorithm

3.3. Signcryption algorithm

Sender's Signcryption
Select x uniformly and randomly from $1 \le x \le q-1$. Calculate $k = hash(y_b^x (\bmod p))$. Split k into k_1 and k_2 of appropriate length. Calculate $r = KH_{k2}(m)$. $s \equiv x/(r + x_a)(\bmod q)$ $: SCS1$ $s \equiv x/(1 + x_a . r)(\bmod q)$ $: SCS2$ $c = E_{K_1}(m)$ Send the signcrypted text (c,r,s).
Receiver's Unsigncryption
Recover k using r,s,g,p,q,y_a,x_b $k = hash((y_a . g^r)^{s.x_b} (\bmod p))$ $: SCS1$ $k = hash((y_a^r . g)^{s.x_b} (\bmod p))$ $: SCS2$ Split k into k1 and $k_{2.}$ $m = D_{k1}(c)$ Calculate KH_{k2}(m) and accept m as a valid message if KH_{k2}(m)= r.

3.4. Optimal Blow Fish Algorithm

In our proposed method Hybrid Blow Fish algorithm is applied for both encryption and decryption. Blow fish algorithm is employed for symmetric key cryptography. Blow fish algorithm encloses 64 bit block size and key length from 32 bit to 448 bits. There is P-array and four 32 bit S-boxes. P-array encloses 18 of 32 bit sub keys and each S-box contains 256 entries. Blow fish algorithm contains two parts namely key expansion and data encryption. To change the input key (448 bit) into sub key (4168 bytes) arrays, key expansion is applied. Data encryption is employed 16 round feistel network. Each round contains a key dependent permutation and a key dependent substitution. All functions are XOR's and additions on 32 bit words in blow fish algorithm.

3.5. Sub keys of Blow Fish algorithm:

Huge number of sub keys is applied in Blow fish algorithm. These sub keys are must be precomputed before the encryption and decryption process.

- P-array consist of 18 of 32 bit sub keys

  P_{y1}, P_{y2}……P_{y18}.

- four 32 bit S-box contains 256 entries

  $S_{b1,0}$, $S_{b1,1}$……$S_{b1,255}$.

  $S_{b2,0}$, $S_{b2,1}$……$S_{b2,255}$.

  $S_{b3,0}$, $S_{b3,1}$……$S_{b3,255}$.

  $S_{b4,0}$, $S_{b4,1}$……$S_{b4,255}$.

3.6. Encryption:

Encryption is the procedure of changing plain text into cipher text. In our proposed method, the input is 64 bit data. The input data is splitted into two 32 bit halves at first round. That is indicated as left halves (LH) and right halves (RH). In blow fish algorithm the first 32 bit left halves and P-array executes the XOR operation and the result is fed to the function (Ft). Next the output of left halves and the next 32 bit right halves perform the XOR operation. Then both the result is swapping then the rest of the round goes on till it reaches 16 round. The specified process is revealed in Figure 2.

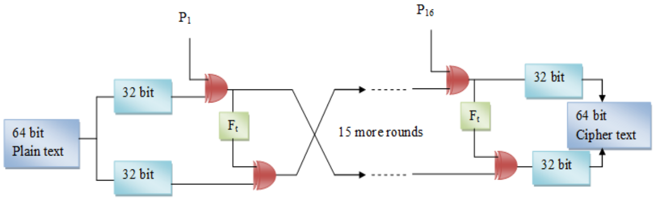

Figure 2: The detailed encryption process of Blowfish

3.7. Working of F_t function:

Ft function employs four 32 bit S-boxes and each S-box encloses 256 entries. In blow fish algorithm, the first 32 bit left halves is separated into four 8 bit blocks m, n, o and p.

The formula using F_t function is shown in below,

$$F_t(L_H) = ((S_{b1,m} + S_{b2,n} \bmod 2^{32}) \oplus S_{b3,o}) + S_{b4,p} \bmod 2^{32}$$

3.7.1. Decryption:

The decryption process of blow fish algorithm is similar process of encryption however here the P-array employed reverse.

GA based Cuckoo search algorithm for Optimal key generation in Blow fish algorithm

Cuckoo search algorithm is a meta-heuristic algorithm which was inspired by the breeding behaviour of the cuckoos and ease to implement. In cuckoo search, there are a number of nests. Every cuckoo lays one egg at a time, and leaves its egg in a randomly selected nest. The best nests with high superiority of eggs will put back to the next generation. Each egg in a nest represents a solution, and a cuckoo egg represents a new solution. The number of available host's nests is allocated, and the egg laid by a cuckoo is found by the host bird. The process performs on some of the worst nest sets and the obtained solutions are leaved from out of calculations. In the proposed method, combined CS-GA algorithm finds the optimal combination of the generator units based on the multi-objective function, which is possible by taking the generation limits of the generator as the input. Here, the solution updating process can be done by the CS algorithm's levy flight search and GA algorithm's crossover and mutation processes. From the attained updated solutions, the best solution can be selected by using the multi-objective function. The algorithmic procedure to find the optimal generator combination is described as follows.

Steps to optimize the key combinations

Step1: Initialize the input host nest and cuckoo parameters such as generation limits of thermal generators X_i .

Step 2: Generate the random population of *n* host nests using the following equation.

$$X_i = [X_1, X_2 \mathrm{K}\ X_n]$$

Step 3: Set the iteration count k=1.

Step 4: Determine the fitness of the nests by means of the fitness equation.

$$fitness = \max(matched\ data)$$

Step 5: Determine the maximum and minimum fitness of the initial population. The minimum values are stored as the best solutions.

Step 6: Generate the new solution X_i^{t+1} using levy flight search, crossover and mutation, which can be represented as follows

Step 6.1: Levy flight search

$$X_i^{t+1} = X_i^t + \alpha \oplus Levy(\lambda)$$

Where, $\alpha > 0$ is the step size, which should be related to the scale of the problem of interest and the product $\oplus$ means element-wise multiplication. In this work, we consider Levy flight in which the step-lengths are distributed according to the following probability distribution

$$Levy(\lambda) = t^{-\lambda},\ 1 < \lambda \le 3$$

Discover the worst nests based on the probability (p_a) and substitute the worst nests by new set of solutions.

Step 6.2: Crossover and mutation

The crossover operation is achieved between the two chromosomes that lead to generate new set of chromosomes. The mutation process is achieved by using the mutation probability; the method mutates a new child at each chromosome. The best solution can be determined from the attained new chromosomes.

Step 7: The updated results from levy fight search and GA's crossover and mutation process are compared. The best solutions are identified using the multi-objective function.

Step 8: Test the termination criteria. Go to step 9 if it is met, otherwise go to step 3.

Step 9: Terminate the process.

Once the process is completed, the network is ready to give the optimal key generations which is suitable for different attacks.

4. RESULTS AND DISCUSSION

The proposed methodology for secured data transaction in a network is implemented in Java with user defined network. Here we organized a network with some vehicles in which the message prioritization and data dissemination to be held. Here Table 1 represents some of the Messages and Assigned Prioritization and Table 2 represents the keywords.

Messages	Urgent	General	Entertainment
Accident! Ambulance needed	✓		
Nearest Petrol bulk location		✓	
Nearest shopping Mall			✓
Road Blocked. Heavy Traffic jam	✓		

Table 1: Message Prioritization Process using SMTP

Urgent	General	Entertainment
Accident Ambulance Traffic jam	Petrol Bulk	Shopping mall Music park

Table 2 Keywords

While transfering the data, hackers or unauthorized node may try to hack the data. We analyzed 2 types of attacks such as DOS and Sybil. The Hackers will try to break the secret keys to get the data.

4.1 Comparative Analysis:

Here Table 3 represents the encryption time of various cryptographic encryption algorithm with various lengths. Our proposed blowfish algorithm outperforms the existing algorithms with less encryption time.

Encryption algorithm	Encryption time (in ms)		
	Urgent Msg.	General Msg.	Entertainment Msg.
AES	321	386	597
RSA	323	356	587
ECC	291	358	491
Proposed Method	275	342	479

Table 3 Encryption time analysis of various cryptographic algorithms

The proposed optimal blowfish algorithm encrypts the urgent messages in minimum time when compared to the existing algorithm. Here in Table 3, the encryption algorithms are tested with varying length text messages mentioned in Table 1. Our proposed security system is analyzed with various attacks such as Daniel of Service (DOS) and Sybil attack. While using these attacks, the security of the system is evaluated in terms of key breaking time, and similarity of the hacked text.

Algorithm	Similarity (in %)	
	DOS attack	Sybil attack
AES	24.6358	21.8544
RSA	21.8544	18.6635
ECC	18.6635	15.3846

Proposed Method	14.231	13.5632

Table 4 Key similarity

From this Table 4, we observed that, our proposed algorithm outperforms the existing algorithm, i.e., during the hackers attack, the key breaking time is high for the existing algorithm. This key breaking time is used for a fitness in CS-GA.

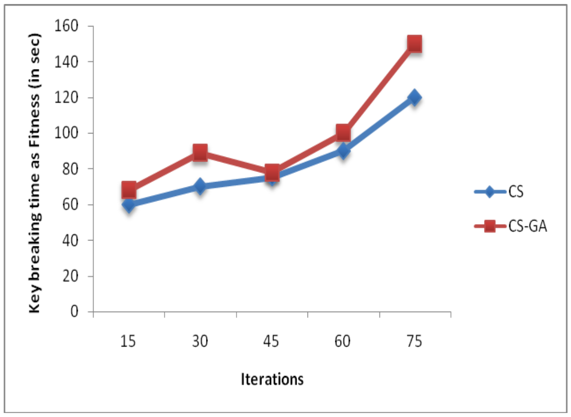

Figure 3: Fitness convergence comparison

While using the optimization algorithm the fitness convergence plays the major role. Here in CS-GA, The key breakingtime is used as the fitness, ie., how long itwill take to break the key. This is the maximization problem so the fitness converges towards maximum. Figure 3 represents the convergence graph for both conventional CS and CS-GA. Our CS-GA has maximum fitness when compared to CS.

Algorithm	Time (in ms)
Conventional Signcryption	474
Signcryption with ECC	461
Signcryption with optimal blowfish based on CS	411

Table 5 Computational Time analysis with existing techniques

In information security, encryption time plays a vital role in terms of sensitive message transaction. The complexity of the algorithm depends upon the encryption time. Here table 5 describes the computational time of our proposed Signcryption with optimal blowfish based on CS algorithm with other existing techniques. In VANET, the optimal blowfish algorithm based signcryption technique is for secured message transaction which is observed from the results and discussion.

5. CONCLUSION

Message Prioritization and data dissemination plays a major role VANET. Here we proposed SMTP based Message Prioritization technique and Hybrid blowfish algorithm based signcryption technique for data dissemination. Message Prioritization technique can identify the false hindering messages and our proposed technique can offered a secured message transfer under various attacks such as Sybil and DOS From the Results and discussion part, we observed that, our proposed method outperforms the existing techniques.

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.

Authors

Mrs. M. Selvi received her B.Sc Computer Science degree from S. T. Hindu college affiliated Manonmanium Sundaranar University, Tirunelveli, India and MCA degree from Anna University, India. Presently she is a research scholar in Department of Computer Science, S. T. Hindu College, Nagercoil, India. She has three years of research experience and authored six research papers in reputed international journals and conferences. His research interests include Data Mining, Information Security, Vehicular Adhoc Network and Network Security.

Dr. B. Ramakrishnan is currently working as Associate Professor in the Department of Computer Science and research Centre in S.T. Hindu College, Nagercoil. He received his M.Sc degree from Madurai Kamaraj University, Madurai and received Mphil (Comp. Sc.) from Alagappa University Karaikudi. He earned his Doctorate degree in the field of Computer Science from Manonmanium Sundaranar University, Tirunelveli. He has a teaching experience of 28 years. He has twelve years of research experience and published more than forty research articles in reputed international journals. His research interests lie in the field of Vehicular networks, mobile network and communication, Cloud computing, Green computing, Ad-hoc networks and Network security.