Privacy preserving approach for VANETs using Mutation technique of genetic algorithm

Sheetal Singh, Bhawna Chaudhary

Abstract— Vehicular ad-hoc networks are particularly useful and well-suited for critical scenarios including road-accidents and in emergency situations. When operating in vicious or suspicious enviornment, VANET requires communication security and privacy,especially location privacy.Most of the applications in VANET like warning messages, collision avoidance messages require exact location of the vehicle. This information available in the network can be used by an adversary to track a vehicle.We need a preventive approach because lack of privacy may act as barrier in the acceptance of VANETs.This paper presents an algorithm inspired from a concept of genetic algorithms to compute the validity of the algorithm and gauge the performance of work.We analyze privacy in and performance of the algorithm by computationally finding the correlation factor. Result has shown that this approach achieved sufficient degree of privacy in the network.

Index Terms— Genetic Algorithms, Location Privacy, Mutation, Pseudonyms, VANETs.

1 INTRODUCTION

The vehicular ad-hoc network has set the vision of computers on wheels to a reality. Such networks consist of cars in a network talking to each other through GPS or wireless enabled devices fitted in their cars [1]. The term VANETs is gaining popularity nowadays because of their applications in road safety and travel convenience. The advanced wireless technologies enable direct and instant Vehicle-to-Vehicle (V2V) communication and Vehicle-to-Infrastructure (V2I) Communication.Vehicles communicating with each other and the other Road Side Units enable a range of applications such as providing information regarding the traffic jams, road accidents and other information on the road. The cars in the VANETs are connected to themselves in a self organizing and decentralized manner [2]. VANETs have recently become a favorable technology for increasing the efficiency and the safety levels of transportation systems. In the recent years, there has been a significant interest and development in the field of Vehicular Ad-hoc Networks. The vehicles in the VANET are supposed to broadcast their status consisting of their current location, speed and direction they are heading towards. The information received is then used in safety enhancing applications [3].

Despite of several great advantages, VANETs also face some challenges in security and privacy. The open essence of wireless communications and faster mobility of the vehicles in the network puts the security and privacy of the vehicles to a stake. The messages transmitted by the vehicles can be easily eavesdropped by anyone within the network. These messages can then be used by the adversaries to trace the location of the vehicles and the adversaries can easily spy on the people in the network [6].Location privacy is one of the major concerns in the field of VANETs. It is basically related to protecting ones real identity and location information. Adversaries should be fended off from recognizing the real identity of the driver and the specific location of that vehicle [7]. One possible solution to provide location privacy to the vehicles in VANETs is the pseudonym scheme. In this scheme, each vehicle in the network is assigned a pseudonym for communicating with the other vehicles which is changed either after a specified time or at random time spans.

In this paper, we propose a scheme for enhancing location privacy based on the pseudonyms. The proposed scheme relies on generating pseudonyms using a search heuristic called Genetic Algorithm.As the scheme is based on the optimization technique, the fittest solutions are chosen to create a new generation. We achieve salient location privacy for VANETs by combining the proposed pseudonym generation scheme with the mutation method of genetic algorithms.

This paper is organised as follows.In Section II, we shortly review the previously proposed work and Sec. III present the concept of genetic algorithm used in our work.Sec. IV provides the proposed algorithm and the findings of the work. Finally in Sec. V, we will conclude the paper and discuss its future aspects.

2 RELATED WORK

In order to achieve location privacy in VANETs, a number of schemes have been presented. In [8] AMOEBA was proposed which makes use of entropy and the maximum tracking time as metrics to provide unlinkability between the vehicles.The

- *Sheetal singh is currently working as Assistant Professor at Ramanujan College,University of Delhi.Email id: sheetal.2109@yahoo.in*
- *Bhawna Chaudhary is currently pursuing her PhD from School of Computer Systems& Sciences, JNU. Email id: bhwna.0101@gmail.com*

AMOEBA scheme makes use of a silent interval to determine the area of vehicles in VANET by enforcing the vehicle to remain silent for a randomly chosen period of time. The effectiveness of AMOEBA improves as the silent interval increases.Another mechanism for preserving privacy called CARAVAN was proposed by [10]. They proposed that combining the neighboring vehicles into groups can reduce the number of times a vehicle needed to broadcast a message, which in turn provides longer silent period thereby enhancing anonymity. CARAVAN also suggested an anonymous protocol for addressing the threats to privacy caused by LBS applcations.

In [9], anonymity-based approach is discussed in which a randomly changing identifier, called the pseudonym is used to trace the location of a target vehicle. The idea behind this approach is to generate pseudonyms in such a way that the adversaries are not able to link a new pseudonym to the existing ones of the same vehicle. Pseudonyms can either be a set of public keys, network layer addresses, or link layer addresses.Since pseudonyms follow the anonymity based approach, they cannot be linked to each other and hence, can provide a certain degree of privacy [8, 9].Whenever the vehicle changes its public key or any of the layer's addresses the value of the pseudonym changes accordingly. This anonymity based approach prevents tracking between two successive locations of the target.

In [11], a strategy called PCS (Pseudonym Changing at Social spots) is proposed which measured the level of anonymity by using the size of the anonymous set of pseudonyms used. The social spot which is meant to be a mix zone of predefined fixed size is used to bewilder the relationship of vehicles entering and leaving the network. JulienFreudiger [12] proposed a trigger based approach to provide location privacy by using the age of the pseudonym and the number of neighbors of the vehicle by considering the temporaland spatial factors. RPCs have proved to be beneficial in providing location privacy. An analytical model proposed by [6] is the RPC scheme in which whenever each vehicle broadcasts a message, it chooses any one of the pseudonym from the preloaded set pseudonyms and changes its value after a random period. Wasef et al.[13] proposed an efficient certificate scheme for VANET (ECMV) based on public key infrastructure. In ECMV, each vehicle has short-lifetime certificate (requires frequent validation from authority), which can be renew from any RSU.But this scheme demands continuous updation of certificates to provide privacy-preserving authentication.
Based on the above observations, we propose our GA based technique for pseudonym generation in this paper. To the best of our knowledge, our work is the first study that will be able to generate pseudonyms using mutation method. Our algorithm ensures that the pseudonym generation cannot be linked to the previous generation, to achieve unlinkability.

3 GENETIC ALGORITHMS

Genetic algorithm is a search heuristic that imitates the process of natural selection which is routinely used as an optimization technique to generate useful solutions to search problems [4]. A Genetic Algorithm chooses a parent from a random population of chromosomes to generate an offspring using crossover and mutation. The fitness of the chromosomes is tested on the basis of the value of their fitness function, which in turn is used to decide the elimination of unfit chromosomes from the population. The selection of chromosomes is done on the principle of "SURVIVAL OF THE FITTEST". The fitter chromosomes are kept to generate a new population and the less fitter are discarded [5]. The following figure depicts a typical genetic process :

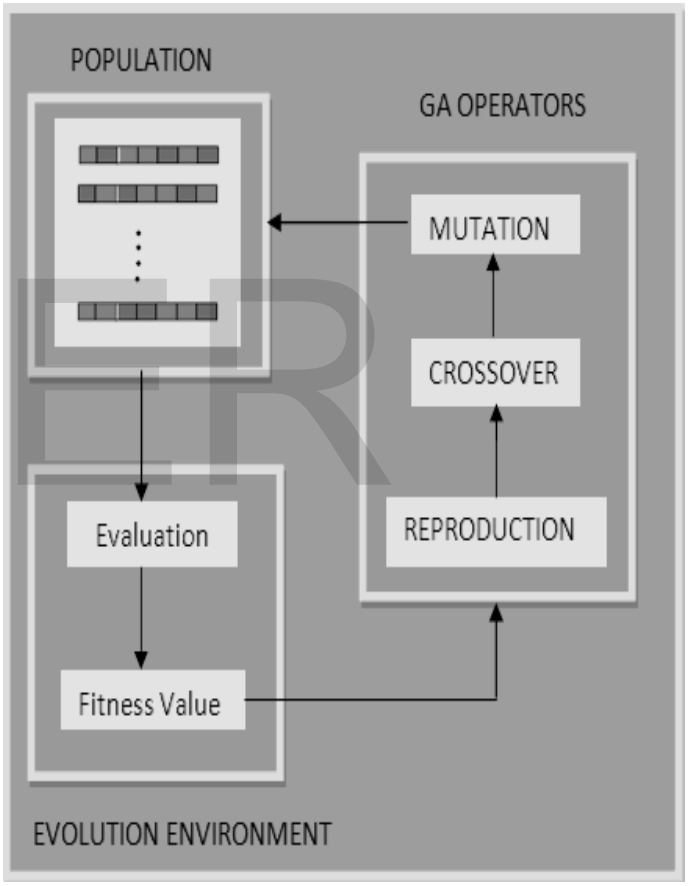

FIG1: A TYPICAL GENETIC PROCESS

As we have seen, Genetic Algorithms have earlier been used in VANETs. In this paper, we propose a scheme for generation of pseudonyms based on mutation probability of the Genetic Algorithms. A random population is used to select parent pseudonyms and a generation of offspring is generated. Experimental results show that the proposed scheme significantly improves randomization and independent pseudonym generation.

4 PROPOSED WORK

In this paper, we present an approach for generating the pseudonyms using the mutation method of genetic algorithms. The mutation method flips the random number of bits in the parent pseudonym and hence a mutated offspring is generated. The offspring produced is then again mutated and another offspring is generated. Following this approach we are able to create a new generation of the pseudonyms and these pseudonyms can then be assigned to the vehicles in the network.

4.1 Mutation based generation of Pseudonyms

The random flip based mutation method flips a random number of bits in the given pseudonym to generate the offspring. To generate a random series, we are using Fibonacci series to flip the bits. We randomly chose a pseudonym to illustrate this mutation based on Fibonacci numbers. The table below shows the mutation process. The new offspring generated is then again mutated to generate another offspring and so on.

Pseudo code for generating pseudonyms using Genetic Algorithm:

1. Generate a random population P with x chromosomes.
2. Evaluate the fitness of each chromosome x in the population P using a fitness function f(x).
3. {
   Creating a New population: P′

   While P′ <= n

   Do

   {

   a. The random pseudonym is chosen as a parent for performing mutation.
   b. The Fibonacci sequence is generated.
   c. The function f(x) = Fn Modulo 15 is calculated, where Fn is the Fibonacci number from the sequence.
   d. The pseudonym P is then mutated by performing the 8 bit flip operation.
   e. The f(x)th bit is flipped in the parent pseudonym.
   f. A total of 8 flips are performed on the pseudonym and the offspring is generated.
   g. Insert the offspring generated to the new population P′.

   }
4. Use the new generated population to repeat the algorithm until the termination condition is satisfied.
5. Return the best solution in the current population.

On the basis of the above pseudocode, we illustrate the scheme as follows. The table shows the pseudonyms and their offspring. The scheme works as follows. The random pseudonym is chosen from a population to generate the offspring using mutation. The function f(x) is calculated using the formula f(x) = Fn Modulo 15 where Fn is the Fibonacci number from the sequence 1, 2, 3, 5, 8, 13, 21, 34, 55 and so on. The function f(x) results in an integer value between 0-15. This function gives the bit positions to be flipped in the mutation process. Each pseudonym is mutated by flipping 8 bits from the parent based on the function f(x). According to the described procedure, we get the following results as shown in the table I:

TABLE-I

OFFSPRING'S AFTER FLIPPING THEIR POSITIONS

Parent	F(x), Bit positions to be flipped	Offspring
101010000100100	1, 2, 3, 5, 8, 13, 6, 4	010101010100000
010101010100000	10, 14, 9, 8, 2, 10, 12, 7	000101101101010
000101101101010	4, 11, 0, 11,11,7,3,10	001001001011010
001001001011010	13, 8, 6, 14, 5, 4 , 9, 13	001110010011000
001110010011000	7, 5, 12, 2, 14, 1, 0, 1	011100110010100

The newly generated offspring after mutation is further used as parent for the next mutation. The parent pseudonym is again mutated by flipping the 8 bits on the next 8 bit positions generated by the function f(x) generated from the Fibonacci modulo. This process is repeated until a generation of pseudonyms is created or the termination condition is satisfied. We can generate n number of pseudonyms using this scheme.

4.2 Calculating Average Correlation between Pseudonyms

To show that the parent pseudonym and the offspring generated are distinct from each other, the correlation average is calculated. We compare the parent pseudonym with the off-

spring produced. To show the comparison between the two strings, we will perform an exclusive nor function on the two bit strings, whenever the two inputs are same, the output logic is 1. For instance, consider the following bit sequence:

Parent 1 101010000100100

Child 1 010101010100000

X-NOR 000000101111011

The output string has 7 ones out of 15 bit string which on an average is 0.47 meaning that approximately half of the string is different from the parent. Similarly, we can compare the entire parent pseudonyms with the offspring produced after mutation.The average function here gives the number of output 1s' signifying the percentage of difference in two strings. Likewise, we can find out the correlation between other generations by performing the X-NOR function and the result will be shown below in the given table-II.

TABLE-II

CORRELATION AVERAGE BETWEEN PARENT AND CHILD USING X-NOR FUNCTION

Parent	Child	X-NOR
Parent1	Child1	.47
Parent2	Child2	.60
Parent3	Child3	.667
Parent4	Child4	.60
Parent5	Child5	.667

After finding the correlation average between the parent and their respective child, we can plot graph that shows there is no relation between the previous two outcomes. We calculated the similarity (in percentage) among the offspring and parent; which gives an average of 0.5, i.e. the offspring generated is approximately 50% different than its parent (See Fig 2).

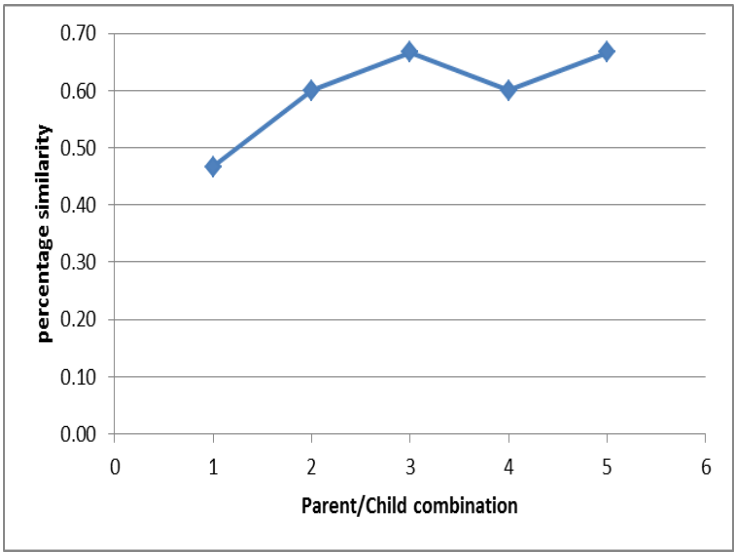

FIG2: RELATION BETWEEN PERCENTAGE SIMILARITY AND PARENT AND CHILD COMBINATIONS

5 CONCLUCSION AND FUTURE WORK

In this paper, we studied the efficacy of pseudonyms in providing location privacy for vehicles in vehicular ad-hoc networks. The number of techniques of changing the pseudonyms at regular intervals to enhance location privacy has been proposed earlier. We defined a new algorithm to generate pseudonyms based on the Genetic Algorithm by considering a random population to produce offspring from the parent pseudonyms using the random flip bit mutation operator of genetic algorithm. We also defined a function f(x) to generate random numbers series to find out the bit positions to be flipped in the parent pseudonym. In addition to this function, in spite of selecting random parent for each iteration, we considered the newly generated offspring as the parent for the next mutation iteration; thereby reducing the probability of generating identical offspring and the parent pseudonym.

In this paper, we assumed that the frequency with which the pseudonyms are changed is high enough so that every vehicle surely changes pseudonym while present in the network. In our future work, we intend to simulate the work by considering a strong adversary.

References

[1] AgataGrzybek, MarcinSeredynski, Gr´egoireDanoy and Pascal Bouvry, Aspects and Trends in Realistic VANET Simulations
[2] Florian D¨otzer, Privacy Issues in Vehicular Ad Hoc Networks
[3] Albert Wasef , Xuemin (Sherman) Shen, REP: Location Privacy for VANETs Using Random Encryption Periods
[4] Louis Mayaud, Lionel Tarassenko , Gari D. Clifford; Genetic Algorithm for feature selection: application to prediction of mortality during hypotensive episodes in patients with sepsis and severe sepsis, October 11, 2012

[5] WEN-YANG LIN, WEN-YUAN LEE, TZUNG-PEI HONG, Adapting Crossover and Mutation Rates in Genetic Algorithms, January 24, 2003.

[6] Yuanyuan Pan, Jianqing Li, Li Feng , Ben Xu, An analytical model for random pseudonym change scheme in VANETs, Springer Science+Business Media New York 2013

[7] Albert Wasef, Xuemin (Sherman) Shen, Location Privacy for VANETs Using Random Encryption Periods, 27 May 2009

[8] Krishna Sampigethaya, Mingyan Li, Leping Huang, and RadhaPoovendran, AMOEBA: Robust Location Privacy Scheme for VANET,

[9] Joo-Han Song, Vincent W.S. Wong, Victor C.M. Leung, Wireless Location Privacy Protection in Vehicular Ad-Hoc Networks, Springer Science + Business Media, LLC 2009

[10] Krishna Sampigethaya , Leping Huang , Mingyan Li , Radha-Poovendran , Kanta Matsuura , Kaoru Sezaki, CARAVAN: Providing Location Privacy for VANET

[11] Lu, R., Li, X., Luan, T.H., Liang, X., Shen, X.: Pseudonym changing at social spots: an effective strategy for location privacy in vanets. IEEE Trans. Veh. Technol. 61(1), 86–96 (2012)

[12] Freudiger, J., Manshaei, M., Boudec, J.Y.L., Hubaux, J.P.: On the age of pseudonyms in mobile ad hoc networks. In: Proceedings of the 29th IEEE International Conference on Computer Communications (IEEE INFOCOM 2010), San Diego, California, USA, pp.1–9 (2010)

[13] Wasef, A., Jiang, Y., & Shen, X. S. (2008, November). ECMV: efficient certificate management scheme for vehicular networks. In Global Telecommunications Conference, 2008. IEEE GLOBECOM 2008. IEEE (pp. 1-5). IEEE.

IJSER