An Efficient Crash Prediction and Secured Communication of OLSR Routing Protocol uses Different Key Exchanges for VANETs

R.Gowtham[#1], M.Suguna[#2], Dr.D.Sharmila[#3]

[#1]*PG Scholar, Department of Information Technology*
SNS College of Technology
Coimbatore, India
gowtham3366@gmail.com

[#2]*Associate Professor, Department of Information Technology*
SNS College of Technology
Coimbatore, India
suguna.marappan@gmail.com

[#3] *Professor &*
Head EIE Department
Bannari Amman Institute of Technology
Sathyamangalam, India
sharmiramesh@rediffmail.com

Abstract--- A Vehicular Ad Hoc Network (VANET) is an instance of MANETs that establishes wireless connections between vehicles. The continuous exchange of routing control packets causes the appearance of network congestion, then limiting the global performance of the VANET. Thus, the quality-of-service (QoS) of OLSR significantly depends on the selection of its parameters, which determine the protocol operation and key exchange operation. Key exchange as Asymmetric encryption algorithms (public key algorithms) use different keys for encryption and decryption, and the decryption key cannot (practically) be derived from the encryption key. Automatic Vehicle Identification (AVI) used to prevent crash prediction thus avoids accidents. OLSR has a wide range of improvements by changing the configuration parameters and key files. Therefore, computing an optimal configuration for the parameters of this protocol is crucial before deploying any VANET, since it could decisively improve the QoS, with a high implication on enlarging the network data rates and reducing the network load.

Keywords-- Advanced Encryption Standard (AES), optimized link state routing (OLSR), Automatic Vehicle Identification (AVI) Vehicular Ad Hoc Network (VANET).

I. INTRODUCTION

VANET is a form of Mobile ad-hoc network, to provide communications among nearby vehicles and between vehicles and nearby fixed equipment, usually described as roadside equipment. Vehicular networks represent an interesting application scenario for not only traffic safety and efficiency but more commercial applications and entertainment support as well, such as service scheduling, content sharing, peer-to-peer marketing, and urban data collecting.

The continuous exchange of routing control packets causes the appearance of network congestion, then limiting the global performance of the VANET. Thus, the quality-of-service (QoS) of OLSR significantly depends on the selection of its parameters, which determine the protocol operation. OLSR has a wide range of improvements by changing the configuration parameters. Therefore, computing an optimal configuration for the parameters of this protocol is crucial before deploying any VANET, [3] since it could decisively improve the QoS, with a high implication on enlarging the network data rates and reducing the network load. Then, all these features make OLSR a good candidate to be optimally tuned. Here define an optimization problem to tune the [4] OLSR protocol, obtaining automatically 2the configuration that best fits the specific characteristics of VANETs. An optimization problem is defined by a search space and a quality or fitness function. The search space restricts the possible configurations of a solution vector, which is associated with a numerical cost by the fitness function. Thus, solving an optimization problem consists of finding the least-cost configuration of a solution vector.

In spite of the moderate number of configure parameters that govern OLSR , the number of possible combinations of values that they can take makes this task very hard.

Automatic vehicle identification (AVI) [15] is among other sys- terms, such as satellite positioning and mobile communications using Global System for Mobile communication, where the vehicles slow down into channeled toll lanes and, recently, where the express ETC lanes have operated at highway speeds. While traffic flow data collected from ILDs were a good safety measure in real-time proactive safety management, data collected from AVI have not been previously investigated in any safety-related study.

Due to the high complexity that these kinds of problems usually show, the use of automatic intelligent tools is a mandatory requirement when facing them. In this sense, metaheuristic algorithms [1] emerge as efficient stochastic techniques able to solve optimization problems. Indeed, these algorithms are currently employed in a multitude of engineering problems, showing a successful performance. Unfortunately, the use of metaheuristics in the optimization of ad hoc networks (and concretely in VANETs) is still limited, a specialized cellular multiobjective genetic algorithm was used for finding an optimal broadcasting strategy in urban MANETs. six versions of a genetic algorithm (GA) were evaluated and used in the design of ad hoc injection networks. A GA [6] was also employed by Cheng and Yang for solving the multicast routing problem in MANETs. Due to its specific design, Shokrani and Jabbehdari developed new routing protocols for MANETs based on ant colony optimization [7]. Particle swarm optimization (PSO) algorithm [5] has been used to manage the network resources by Huang et al, proposing a new routing protocol based on this algorithm to make scheduling decisions for reducing the packet loss rate in a theoretical [4] VANET scenarios.

II. BACKGROUND

The performance of AODV and OLSR [2] for vehicular ad hoc networks in urban environments. The traffic regulations and the vehicles characteristics handled by the Vehicular Mobility Model (VMM) used to creating a clustering effect at intersection. This effect has a remarkable properties on standard performance evaluations of ad hoc protocols. The first one is that neither the initial nor the maximum velocity has any influence on routing protocols in urban environments. Indeed, due to the interaction with the spatial environment and also other [5] neighboring cars, vehicles experience a non negligible speed decay independent of the network velocity. Then, a second property is local increase of nodes density, which clearly has a consequence on both tested ad hoc routing protocols.

They tested OLSR and AODV [2] against node density and data traffic rate. Globally, we found that OLSR outperforms AODV in VANETs. For most of the metrics we used in this paper, OLSR has better performance that AODV. Indeed, OLSR has smaller routing overhead, end-to-end delay and route lengths. And for the PDR, where OLSR may be outperformed by AODV after a certain threshold, the performance loss is limited to 10%. Accordingly, unlike a previous study for MANET which suggested that neither OLSR nor AODV could outperform each others.

Understanding the benefits of improved traffic flow (reduced congestion) is critical to the assessment of investments in infrastructure or traffic management and control[16]. Improved flow should lead to reductions in travel time, vehicle emissions, fuel usage, psychological stress on drivers, and improved safety.

A. Location Based Security

A feasible and novel geographic location based security mechanism for vehicular ad hoc network environment on the basis of concepts proposed by. Comparing with the our algorithm is efficient on the basis of simulation. The future work will integrate the model into the existing security methods. The shape of the decryption region can be extended to any shape.

The location-based encryption method that not only ensures message confidentiality, but also authenticates the identity and location of communicating peers. Our method is an extension of geo-encryption, proposed by Denning et al. Geo-encryption limits the area inside which the intended recipient can decrypt messages. Our main contributions include: 1) a detailed design of the key composition and recovery mechanism, including techniques to map the location coordinates to a unique value in order to authenticate the communicating peer's location; 2) the prediction of the decryption region in a dynamic vehicular environment. Prediction error is considered by incorporating location prediction deviation, which is dynamically updated based on real locations; 3) the modification of geo-encryption. The population of vehicle is huge and vehicles move from place to place. It is not feasible to use asymmetric cryptographic algorithms like public key infrastructure (PKI). We modify the geo-encryption scheme to adopt symmetric cryptographic algorithms. Moreover, encryption rate is improved by using symmetric cryptographic algorithms.

III. SYSTEM DESIGN

The OLSR protocol is well suited for high density networks, where most of the [3] communication is concentrated between a large number of nodes. OLSR is particularly appropriate for networks with applications that require short transmission delays.

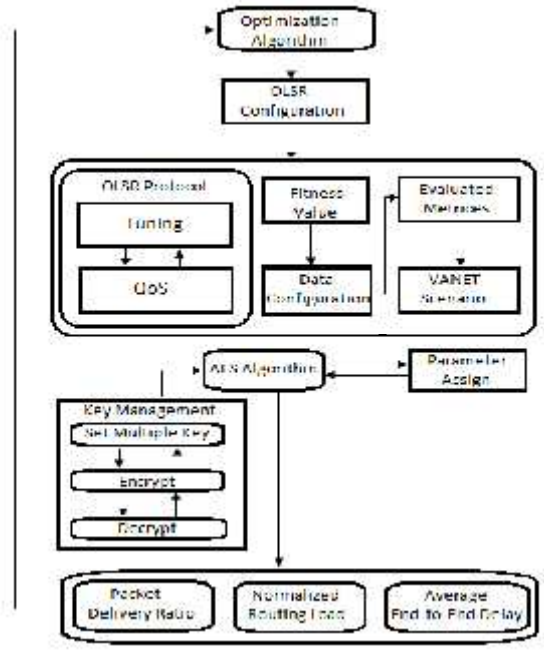

Fig.1 Work Flow Architecture of OLSR Protocol and AES Key Generation.

The OLSR parameters to define a solution vector of real variables, each one representing a given OLSR parameter. This way, the solution vector can automatically be fine tuned by an optimization technique, with the aim of obtaining efficient [2] OLSR parameter configurations for VANETs, of analytic comparisons of different OLSR configurations and their performances as those done in this paper can help the experts identify the main source of communication problems and assist them in the design of new routing protocols. OLSR is a routing protocol that follows a proactive strategy, which increases the suitability for ad hoc networks with nodes of high mobility generating frequent and rapid topological changes the links status is immediately known. it is possible to extend the protocol information that is exchanged with some data of quality of the links to allow the hosts to know in advance the quality of the network routes. This way, the solution vector can automatically be fine-tuned by an optimization technique, with the aim of obtaining efficient OLSR parameter configurations for VANETs, of analytic comparisons of different OLSR configurations and their performances as those done in this paper can help the experts identify the main source of communication problems and assist them in the design of new routing protocols.

IV. ADVANCED ENCRYPTION STANDRAD

The algorithm is designed to encipher and decipher blocks of data consisting of 128 bits under control of a 128-bit multi key. Deciphering must be accomplished by using the same key as for enciphering, but with the schedule of addressing the key bits altered so that the deciphering process is the reverse of the enciphering process. A block to be enciphered is subjected to an initial permutation Vehicles, then to a complex key-dependent computation and finally to a permutation which is the inverse of the initial permutation Vehicles. The key-dependent computation can be simply defined in terms of a function f, called the cipher function, and a function KS, called the key schedule. A description of the computation is given first, along with details as to how the algorithm is used for encrypt. Next, the use of the algorithm for decrypt is described. Finally, a definition of the cipher function f is given in terms of primitive functions which are called the selection functions Si and the permutation function P. Si, P and KS of the algorithm

A DES key consists of 64 binary digits ("0"s or "1"s) of which 128 bits are randomly generated and used directly by the algorithm. The other 8 bits, which are not used by the algorithm, may be used for error detection. The 8 error detecting bits are set to make the parity of each 8-bit byte of the key odd, i.e., there is an odd number of "1"s in each 8-bit byte. A multi key consists of three DES keys, which is also referred to as a key bundle. Authorized users of encrypted computer data must have the key that was used to encipher the data in order to decrypt it. The encryption algorithms specified in this standard are commonly known among those using the standard. The cryptographic security of the data depends on the security provided for the key used to encipher and decipher the data.

Data can be recovered from cipher only by using exactly the same key used to encipher it. Unauthorized recipients of the cipher who know the algorithm but do not have the correct key cannot derive the original data algorithmically. However, it may be feasible to determine the key by a brute force "exhaustion attack." Also, anyone who does have the key and the algorithm can easily decipher the cipher and obtain the original data.

A. Automatic Vehicle Identification (AVI)

This study uses real-time traffic flow characteristics to explain the effect of traffic performance on crash occurrence. [14] These characteristics are reflected by crash precursors. However, to explain the exclusive effect of crash precursors, crash frequency should be controlled for external factors. These external factors include road geometry and time of day (or level of congestion) which have been commonly used in the past crash prediction models. It has been logically and empirically proved that these factors have significant impacts on crash occurrence in the past studies. Also, exposure measures should be combined with crash data so that the effects of various freeway and traffic elements on crash potential can be explicitly compared within or between classifications of interest. Similar to most other crash prediction models[17], the proposed

model expresses crash frequency as a function of a variety of traffic and environmental characteristics as follows:

Crash frequency = *f* (crash precursors, external control factors, exposure)

Using this functional relationship, the model is calibrated using actual crash data and the effects of crash precursors on crash potential can be examined. In the next subsections, the calculation of crash precursors in the above function and the model specification are described. The immediate objective of this research is to determine how crashes are related to traffic flow conditions at the time of their occurrence. Crashes here are depicted in terms of the type of the collision [14](e.g., rear end, sideswipe, hit object), collision location (designated lane or off-road location), number of involved vehicles, movements of these vehicles prior to collision, and severity. Traffic flow is characterized by parameters describing temporal distributions of variables available from single inductive loop detectors, e.g., central tendencies and variations of traffic flow and density for different freeway lanes. The ultimate goal is a safety performance measurement tool that can be used to measure the effects of changes in traffic flow patterns on traffic safety. Such a tool could be used to forecast future conditions or to evaluate the effectiveness of advanced transportation management projects.

B. Applications

Data encryption (cryptography) is utilized in various applications and environments. The specific utilization of encryption and the implementation of the DES will be based on many factors particular to the computer system and its associated components. In general, cryptography is used to protect data while it is being communicated between two points or while it is stored in a medium vulnerable to physical theft. Communication security provides protection to data by enciphering it at the transmitting point and deciphering it at the receiving point.

File security provides protection to data by enciphering it when it is recorded on a storage medium and deciphering it when it is read back from the storage medium. In the first case, the key must be available at the transmitter and receiver simultaneously during communication. In the second case, the key must be maintained and accessible for the duration of the storage period. Vehicles provide approved methods for managing the multiple keys used by the algorithms specified in this standard.

V. IMPLEMENTATION

The simulation task should offer a network environment as close as possible to the real world environment. An effort to define realistic scenarios, where VANETs may be deployed. Define the urban scenario used in our simulations. Next, we present the experimental setup, taking into account the parameter settings for the ns − 2 simulation.

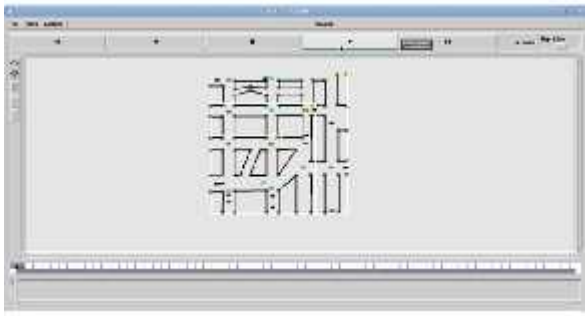

Fig.2 Shows the NS-2 road map with three different networks.

NS − 2 is a network simulator of general purpose, it does not offer a way for directly defining realistic VANET simulations, where the nodes follow the behavior of vehicles in a road, traffic lights, traffic signs, etc. we have used the Simulation of Urban Mobility road traffic simulator to generate realistic mobility models. This tool returns traces with the mobility definitions that can be used by ns – 2 [1].

Fig.3 Shows communication through the vehicles.

Fig.4 Shows Blocks the crashed vehicle and alert to all vehicles.

VI. CONCLUSION

The Optimized Link State Routing protocol by tuning soft state refresh intervals. Through simulations we can see OLSR routing performance is more sensitive to the value of HELLO intervals than the value of TC intervals. Although a smaller HELLO interval could speed up neighbor and link failure detection, the improvement is not linear with the decrease of the interval. So it may be possible to tune the operation of OLSR dynamically, during operation, by measuring metrics presented in this paper, but the mechanism for performing such a dynamic tuning requires further investigation. The main criterion for selecting crash precursors is that the distribution of precursor values for traffic conditions when crashes occurred should be significantly different from the distribution of precursor values for normal traffic condition. It may also be possible to apply such analysis and tuning to other soft-state systems, in order to improve overall system performance. The effects of the increased packet overhead (e.g. in terms of network congestion and power consumption) also need to be assessed. The optimization methodology presented in any protocol for any VANET scenario. We can now provide the experts in this area with an optimization tool for the configuration of communication protocols in the scope of VANETs.

VII. FUTURE WORK

In Future work can extend our experiments with Furthermore; we need to assess the safety benefit of an automated traffic control using the proposed crash prediction model. For one thing, the simulation can be performed before and after implementing the automated traffic control. From the simulation results, the impact of a change in driver behavior caused by this external control on the variation of traffic flow and real-time crash potential can be examined. This before-and-after study evaluates whether this automated traffic control can effectively reduce the overall crash potential on freeways for given conditions. In this line, we are tackling the problem with parallel versions of metaheuristic algorithms to solve time consuming issues derived from large simulations. We are also defining new optimized configuration schemes for other communication protocols such as WAVE, UDP, etc., which should efficiently support actual VANET design. Concerning the improvement of the QOS of the network, we are considering the use of infrastructure nodes, the Global Positioning System, security protocols, and sensing information. Finally, we are planning new real tests (using vehicles travelling through different kinds of roads) to validate our simulations.

REFERENCES

[1] Jamal Toutouch, Jose Garcia-Nieto, and Enrique Alba " Intelligent OLSR Routing Protocol Optimization for VANETs" IEEE Transactions On Vehicular Technology, Vol. 61, No.4, May 2012.

[2] Leticia Cecilia Cagninaa, Susana Cecilia Esquivela and carlos A. Coello Coello " Solving constrained optimization problems with a hybrid particle swarm optimization algorithm " Engineering Optimization Vol. 43, No. 8,August 2011, 843-866.

[3] Xue Yang University of llinois at Urbana-Champaign " A Vehicle-to-Vehicle Communication Protocol for Cooperative Collision Warning ".

[4] Gongjun Yan, Stephan Olariu Computer Science Department Old Dominion University Norfolk, VA 23529 " An Efficient Geographic Location-based Security Mechanism for Vehicular Adhoc Networks".

[5] Maxim Raya and Jean-Pierre Hubaux "Securing vehicular ad hoc networks " Journal of Computer Security 15 (2007) 39-68.

[6] H. Cheng and S. Yang, " Genetic algorithms with immigrant schemes for dynamic multicast problems in mobile ad hoc networks," Eng. Appl. Artif. Intell., vol. 23,no. 5, pp. 806-819, Aug. 2010.

[7] Jerome Haerri Institute Eur'ecomz Department of mobile Communication B.P 193 06904, Sophia Antipolis, France " Performance Comparison of AODOV and OLSR in VANETs Urban Environments under Realistic Mobility Patterns ".

[8] Lin Yi Hui Faculty of Information Technology Multimedia UniversityCyberjaya,63100,Malaysia" Simple Encryption/Decryption Application ".

[9] Naim Ajloumi Amman Arab University for Graduate Studies " A New Approach in Key Generation and Expansion in Rijndael Algorithm " The International Arab Journal Technology, Vol 3, No 1, January 2006.

[10] Subashri T Department of Electronics, MIT Campus, Anna University, Chennai-44 " Pipelining Architecture of AES Encryption and Key Generation with Search Based Memory " International journal of VLSI design & Communication Systems (VLSICS) Vol.1, No.4, December 2010.

[11] Chia-Chen Hung Department of Computer Science and Information Engineering National Central university Chung-Li 320, Taiwan, ROC "A Multi-Key Encryption Scheme for the Next Generation Wireless Network " Received 16 November 2007.

[12] *Management of Catastrophic Precursors: A Cross-Industry Analysis.* National Academy of Engineering, 2001.

[13] Lee, C., F. Saccomanno, and B. Hellinga. Analysis of Crash Precursors on Instrumented Freeways." Forthcoming in the *Transportation Research Record*, 2002.

[14] Krishnan, H., S. Gibb, A. Steinfeld, and S. Shladover. Rear-End Collision-Warning System. In *Transportation Research Record 1759*, TRB, National Research Council, Washington, D.C., 2002, pp. 52-60.

[15] Mohamed M. Ahmed and Mohamed A. Abdel-Aty "The Viability of Using Automatic VehicleIdentification Data for Real-Time Crash Prediction" IEEE Transactions on Intelligent Transportation Systems, Vol. 13, No. 2, JUNE 2012.

[16] L. A. Klein, D. Gibson, and M. K. Mills, "Traffic detector hand- book: Third edition—Volume II," Federal Highway Admin. (FHWA), Washington, DC, Rep. FHWA-HRT-06-108, 2006.

[17] M. Abdel-Aty and A. Pande, "Crash data analysis: Collective vs. individ- ual crash level approach," *J. Safety Res.*, vol. 38, no. 5, pp. 581–587, 2007.