RESEARCH ARTICLE OPEN ACCESS

Light Weight Cryptography for Secure Data Transmission

Dr. Manoj Priyatham
Professor, Department Of Electronics And Communication Engineering, Rr Institute Of Technology, Bengaluru, Karnataka-India

ABSTRACT

Vehicular Ad Hoc Networks (VANETs) is an imperative communication paradigm in recent mobile computing for transferring message for either condition, road conditions. A protected data can be transmitted through VANET, LEACH protocol based clustering and Light Weight cryptographically Model is considered. At first, grouping the vehicles into clusters and sorting out the network by clusters are a standout amongst the most widespread and most adequate ways. This in mechanism gives a solution to control the assaults over the VANET security. This security demonstrates actualized in NS2 simulator with a simulation parameter, and furthermore, our proposed secure data transmission contrasted with existing security methods.

Keywords: VANET, Clustering, Secure data Transmission, Optimization, security, and Cryptography.

I. INTRODUCTION

Vehicular Ad-Hoc Network (VANET) is a developing zone in networking, other than the discern security applications and driver support that frame the fundamental reason for which the VANET has risen; there are applications for traveler comfort and online stimulation [1-10]. Vehicles specifically speak with various vehicles and send information in regards to car influxes, cautioning messages with Road-Site Unit (RSU) which is fasten hardware in roads [11-20]. Clustering is the technique for creating coherently gatherings of the network by some appropriate standard and control in vehicles [21-39]. The Security is increasingly essential in VANETs because of the absence of centralization, dynamic topology [40]. Because of this, it is hard to recognize noxious, acting up and broken nodes or vehicles in the network. Primarily trust models depend on confirming vehicles and give fitting trust value to all vehicles [41].

In existing security model in Beacon based trust framework (RABTM) utilized, that is roundabout event based trust utilized for trust foundation and signal message and occasion message to decide the reliability estimation of that event [42-49]. The goal of VANET is giving road safety [7], improving traffic productivity yet it is a network, so VANET additionally has difficulties about security and is inclined to assault, we will consider reliability investigation in created VANET structure [50-55].

II. LITERATURE SURVEY

In 2018 Rajdeep Kaur et al, [56] have recommended the VANETs remote discussion between cars in this manner attackers rupture secrecy, security, and genuineness properties which affect further insurance. It's exhibited the safety challenges and existing threads in the VANET framework. The reliability of such applications was approved through genuine portability information from an expansive vehicular testbed were presently sent [57] Enhance the steering execution in terms of transmission time and better availability [58]. The FF algorithm on the VANET improves the execution of routing by effective packets transfer from the source vehicle to goal vehicle. Inter-vehicle communication has pulled in consideration since it tends to be relevant not exclusively to elective networks yet in addition to different correspondence frameworks, Fuzzy-based cluster head selection was utilized by Kosuke Ozera et al. [60]. In 2014 Mohamed Nidhal Mejri et al. [61] has been proposed the protection and security challenges that should be defeated to make such networks safety usable practically speaking. It recognizes all current security issues in VANETs and orders them from a cryptographic perspective. It regroups studies and thinks about additionally the different cryptographic plans that have been independently recommended for VANETs, assesses the proficiency of proposed arrangements [62].

III. METHODOLOGY FOR WSN SECURITY

VANET network security in WSN, Lightweight cryptographically model is utilized. For the most part in security examination, the attackers are physically caught to the real sensor vehicles, the real vehicles have not strong security, so the assailants effectively supplant the phony nodes and access all data. So our enhanced security model initially distinguished the reliability nodes by an optimization procedure that is Random Firefly (RFF) Approach with clustering. From this reliability of vehicle nodes and remote connections, in packet forwarding of the sensors are addressed adequately in an orderly way with the assistance of a trust-based frame ceaselessly. In the wake of finding the reliability nodes in network topology, the LWC model used to secure the data transmission in sender to a beneficiary with expecting routing model.

3.1 Routing Scenario with Clustering Model

Cluster formation processes the cluster heads to choose the vehicle nodes in each cluster. The node transmits to the cluster head clearly and in multi-hop of all vehicle node will send their information through the neighbor node. For a cluster based sensor network, the cluster arrangement plays a key part to the cost shrink, where cost alludes to the outlay of setup and support of the sensor networks. This cluster formation model, the routing protocol is extremely critical, in our work LEACH protocol is used. It's to decrease energy consumption by conglomerating data and to lessen the transmissions to the base station.

3.2 Security analysis

Lightweight cryptography is a cryptographic algorithm or protocol custom-made for usage in obliged conditions. Lightweight cryptography adds to the security of VANET networks in light of its effectiveness and little impression. LWC can be characterized by lightweight block ciphers, lightweight hash functions, and lightweight public key cryptography. In our proposed investigation, the security for VANET process utilized Light Weight Hash Function (LWHF) to secure the data. A hash function takes messages of self-assertive information sizes and delivers yield messages with a fixed size. Here, we consider any one of the hash function HF:

Collision resistance: It is hard to discover two distinct messages; for instance let us accept two messages, for example, f_1 and f_2; with the end goal $H(f_1)=H(f_2)$ this requires at any rate $2^{n/2}$ work

Preimage- resistance: The known hash value $H(f)$, it is hard to discover f, this involves $2n$ work.

Second Preimage-resistance: specified f_1, it is complex to locate a diverse input f_2 such that $H(f_1)=H(f_2)$ and this involves at least $2n$ work.

IV. RESULT ANALYSIS

In this result part talked about the performance of the enhancement strategies; some performance measures are utilized and contrasted and existing systems. The proposed framework is actualized in the Java programming language with the JDK 1.7.0 in a windows machine containing the configurations, for example, the Intel (R) Core i5 processor, 1.6 GHz, 4 GB RAM, and the operating system platform is Microsoft Window7 Professional.

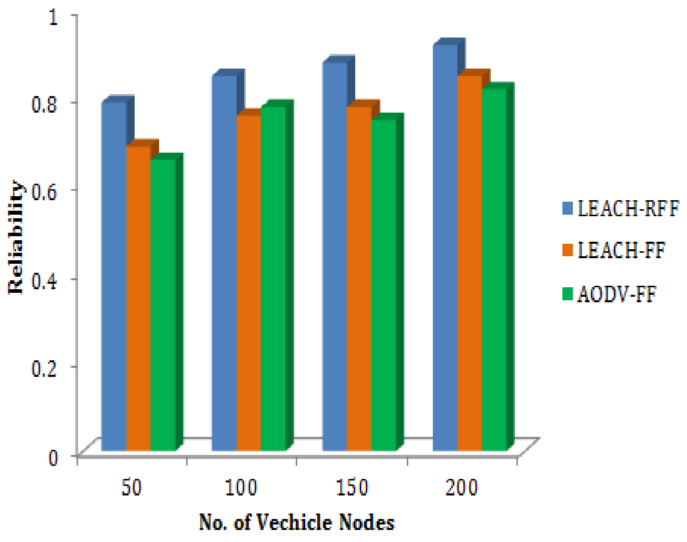

Fig.1: Reliability analysis

Figure 1 shows the reliability analysis for various vehicle nodes. This analysis compares with proposed (LEACH-RFF) into LEACH-FF and AODV-FF. Here, we take 50-200 vehicle nodes for reliability analysis. The analysis depicts that the proposed model (LEACH-RFF) finds out best reliability nodes compared to other techniques.

Table 1: Measures for Proposed VANET security

Number of Vehicles	***PDR (%)***	***NLT(hrs)***	***EC (J)***	***Security (%)***
50	96	119	105	94.67
100	94	124	127	87.67
150	88	126	128	82.45
200	83.56	145	134	90

Table 1 shows the performance measures such as PDR, NLT and EC results for proposed model are illustrated based on a number of vehicles. And also, encryption, decryption time, clustering level and security obtained percentage are shown in this table. The encryption time and decryption time are lower for less number of vehicles.

V. CONCLUSION

In this paper, we analyzed the LWC-Hash function model for improving the security of vehicles that are communicating with the VANET. The data which transmitted safely and the misbehaviors likewise identified effectively.. The fundamental advantages of LWC in VANET are low interest for asset and for power consumption and the execution time as low. From the implementation results, our proposed work (LEC-LEACH) is compared with AES, DES strategy with some execution measure like NLT, PDR, and EC. In future, weighted clustering model with mobility vehicles is utilized to enhance the security of data transmission process alongside the correspondence of traffic controller.

REFERENCE

[1] Anand Nayyar, Vikram Puri, Nhu Gia Nguyen, Dac Nhuong Le, Smart Surveillance Robot for the Real Time Monitoring and Control System in Environment and Industrial Applications, Advances in Intelligent System and Computing, pp 229-243, Springer

[2] Ezhilarasu, P., & Krishnaraj, N. (2015). Applications of Finite Automata in Lexical Analysis and as a Ticket Vending Machine–A Review. Int. J. Comput. Sci. Eng. Technol, 6(05), 267-270.

[3] Agrawal, U., Arora, J., Singh, R., Gupta, D., Khanna, A., & Khamparia, A. (2020). Hybrid Wolf-Bat Algorithm for Optimization of Connection Weights in Multi-layer Perceptron. ACM Transactions on Multimedia Computing, Communications, and Applications (TOMM), 16(1s), 1-20.

[4] Prasanna, S., & Ezhilmaran, D. (2016). Association rule mining using enhanced apriori with modified GA for stock prediction. International Journal of Data Mining, Modelling and Management, 8(2), 195-207.

[5] Pustokhina, I. V., Pustokhin, D. A., Gupta, D., Khanna, A., Shankar, K., & Nguyen, G. N. (2020). An effective training scheme for deep neural network in edge computing enabled Internet of medical things (IoMT) systems. IEEE Access, 8, 107112-107123.

[6] Shankar, K., Zhang, Y., Liu, Y., Wu, L., & Chen, C. H. (2020). Hyperparameter tuning deep learning for diabetic retinopathy fundus image classification. IEEE Access, 8, 118164-118173.

[7] Joshi, G. P., Perumal, E., Shankar, K., Tariq, U., Ahmad, T., & Ibrahim, A. (2020). Toward Blockchain-Enabled Privacy-Preserving Data Transmission in Cluster-Based Vehicular Networks. Electronics, 9(9), 1358.

[8] Saračević, M. H., Adamović, S. Z., Miškovic, V. A., Elhoseny, M., Maček, N. D., Selim, M. M., & Shankar, K. (2020). Data Encryption for Internet of Things Applications Based on Catalan Objects and Two Combinatorial Structures. IEEE Transactions on Reliability.

[9] Namasudra, S., & Roy, P. (2017). Time saving protocol for data accessing in cloud computing. IET Communications, 11(10), 1558-1565.

[10] Elsir, A., Elsier, O., Abdurrahman, A., & Mubarakali, A. (2019). Privacy Preservation in Big Data with Data Scalability and Efficiency Using Efficient and Secure Data Balanced Scheduling Algorithm.

[11] Ezhilarasu, P., Krishnaraj, N., & Babu, S. V. (2015). Applications of finite automata in text search-a review. International Journal of Science, Engineering and Computer Technology, 5(5), 116.

[12] Huyen, D.T.T., Binh, N.T., Tuan, T.M., Nguyen, G.N, Dey, N., Son, L.H, Analyzing

trends in hospital-cost payments of patients using ARIMA and GIS: Case study at the Hanoi Medical University Hospital, Vietnam, Journal of Medical Imaging and Health Informatics, 7(2), pp. 421-429.

[13] Prasanna, S., & Maran, E. (2015). Stock Market Prediction Using Clustering with Meta-Heuristic Approaches. Gazi University Journal of Science, 28(3).

[14] Pustokhina, I. V., Pustokhin, D. A., Rodrigues, J. J., Gupta, D., Khanna, A., Shankar, K., ... & Joshi, G. P. (2020). Automatic Vehicle License Plate Recognition using Optimal K-Means with Convolutional Neural Network for Intelligent Transportation Systems. IEEE Access.

[15] Namasudra, S. (2018). Cloud computing: A new era. Journal of Fundamental and Applied Sciences, 10(2).

[16] Uthayakumar, J., Elhoseny, M., & Shankar, K. (2020). Highly Reliable and Low-Complexity Image Compression Scheme Using Neighborhood Correlation Sequence Algorithm in WSN. IEEE Transactions on Reliability.

[17] Deepalakshmi, P., & Shankar, K. (2020). Role and Impacts of Ant Colony Optimization in Job Shop Scheduling Problems: A Detailed Analysis. Evolutionary Computation in Scheduling, 11-35.

[18] Ashwin, M., Kamalraj, S., & Azath, M. (2019). Multi objective trust optimization for efficient communication in wireless M learning applications. Cluster Computing, 22(5), 10687-10695.

[19] Ezhilarasu, P., & Krishnaraj, N. (2015). Double Substring based Classification for Nondeterministic Finite Automata. Indian Journal Of Science And Technology, 8, 26.

[20] Amira S. Ashour, Samsad Beagum, Nilanjan Dey, Ahmed S. Ashour, Dimitra Sifaki Pistolla, Gia Nhu Nguyen, Dac-Nhuong Le, Fuqian Shi (2018), Light Microscopy Image De-noising using Optimized LPA-ICI Filter, Neural Computing and Applications, Vol.29(12), pp 1517–1533, Springer, ISSN: 0941-0643.

[21] Prasanna, S., Govinda, K., & Kumaran, U. S. (2012). An Evaluation study of Oral Cancer Detection using Data Mining Classification Techniques. International Journal of Advanced Research in Computer Science, 3(1).

[22] Sankhwar, S., Gupta, D., Ramya, K. C., Rani, S. S., Shankar, K., & Lakshmanaprabu, S. K. (2020). Improved grey wolf optimization-based feature subset selection with fuzzy neural classifier for financial crisis prediction. Soft Computing, 24(1), 101-110.

[23] Namasudra, S., & Deka, G. C. (2018). Introduction of DNA computing in cryptography. In Advances of DNA computing in cryptography (pp. 1-18). Chapman and Hall/CRC.

[24] Mubarakali, A., Srinivasan, K., Mukhalid, R., Jaganathan, S. C., & Marina, N. (2020). Security challenges in internet of things: Distributed denial of service attack detection using support vector machine-based expert systems. Computational Intelligence.

[25] Le Nguyen Bao, Dac-Nhuong Le, Gia Nhu Nguyen, Vikrant Bhateja, Suresh Chandra Satapathy (2017), Optimizing Feature Selection in Video-based Recognition using Max-Min Ant System for the Online Video Contextual Advertisement User-Oriented System, Journal of Computational Science, Elsevier ISSN: 1877-7503. Vol.21, pp.361-370.

[26] Ezhilarasu, P., Thirunavukkarasu, E., Karuppusami, G., & Krishnaraj, N. (2015). Single substring based classification for nondeterministic finite automata. International Journal on Applications in Information and Communication Engineering, 1(10), 29-31.

[27] Bhateja, V., Gautam, A., Tiwari, A., Nhu, N.G., Le, D.-N, Haralick features-based classification of mammograms using SVM, Advances in Intelligent Systems and Computing, Volume 672, 2018, Pages 787-795.

[28] Latha, A., Prasanna, S., Hemalatha, S., & Sivakumar, B. (2019). A harmonized trust assisted energy efficient data aggregation scheme for distributed sensor networks. Cognitive Systems Research, 56, 14-22.

[29] Krishnaraj, N., Elhoseny, M., Lydia, E. L., Shankar, K., & ALDabbas, O. (2020). An efficient radix trie-based semantic visual indexing model for large-scale image retrieval in cloud environment. Software: Practice and Experience.

[30] Namasudra, S., Roy, P., Vijayakumar, P., Audithan, S., & Balusamy, B. (2017). Time efficient secure DNA based access control model for cloud computing environment. Future Generation Computer Systems, 73, 90-105.

[31] Lakshmanaprabu, S. K., Shankar, K., Rani, S. S., Abdulhay, E., Arunkumar, N., Ramirez, G., & Uthayakumar, J. (2019). An effect of big data technology with ant colony optimization based

routing in vehicular ad hoc networks: Towards smart cities. Journal of cleaner production, 217, 584-593.

[32] Namasudra, S., & Deka, G. C. (Eds.). (2018). Advances of DNA computing in cryptography. CRC Press.

[33] Mubarakali, A., Ashwin, M., Mavaluru, D., & Kumar, A. D. (2020). Design an attribute based health record protection algorithm for healthcare services in cloud environment. Multimedia Tools and Applications, 79(5), 3943-3956.

[34] Dey, N., Ashour, A.S., Chakraborty, S., Le, D.-N., Nguyen, G.N, Healthy and unhealthy rat hippocampus cells classification: A neural based automated system for Alzheimer disease classification, Journal of Advanced Microscopy Research, 11(1), pp. 1-10

[35] Krishnaraj, N., Ezhilarasu, P., & Gao, X. Z. Hybrid Soft Computing Approach for Prediction of Cancer in Colon Using Microarray Gene Data. Current Signal Transduction Therapy, 11(2).

[36] Namasudra, S., Deka, G. C., Johri, P., Hosseinpour, M., & Gandomi, A. H. (2020). The revolution of blockchain: State-of-the-art and research challenges. Archives of Computational Methods in Engineering.

[37] Goel, N., Grover, B., Gupta, D., Khanna, A., & Sharma, M. (2020). Modified Grasshopper Optimization Algorithm for detection of Autism Spectrum Disorder. Physical Communication, 101115.

[38] Prasanna, S., Narayan, S., NallaKaruppan, M. K., Anilkumar, C., & Ramasubbareddy, S. (2019). Iterative Approach for Frequent Set Mining Using Hadoop Over Cloud Environment. In Smart Intelligent Computing and Applications (pp. 399-405). Springer, Singapore.

[39] Le, D.-N.a, Kumar, R.b, Nguyen, G.N., Chatterjee, J.M.d, Cloud Computing and Virtualization, DOI: 10.1002/9781119488149, Wiley.

[40] Raj, R. J. S., Shobana, S. J., Pustokhina, I. V., Pustokhin, D. A., Gupta, D., & Shankar, K. (2020). Optimal Feature Selection-Based Medical Image Classification Using Deep Learning Model in Internet of Medical Things. IEEE Access, 8, 58006-58017.

[41] Namasudra, S., & Deka, G. C. (2018). Taxonomy of DNA-based security models. In Advances of DNA Computing in Cryptography (pp. 37-52). Chapman and Hall/CRC.

[42] Mubarakali, A., Ramakrishnan, J., Mavaluru, D., Elsir, A., Elsier, O., & Wakil, K. (2019). A new efficient design for random access memory based on quantum dot cellular automata nanotechnology. Nano Communication Networks, 21, 100252.

[43] Ramakrishnan, J., Mavaluru, D., Sakthivel, R. S., Alqahtani, A. S., Mubarakali, A., & Retnadhas, M. (2020). Brain–computer interface for amyotrophic lateral sclerosis patients using deep learning network. NEURAL COMPUTING & APPLICATIONS.

[44] Van, V.N., Chi, L.M., Long, N.Q., Nguyen, G.N., Le, D.-N, A performance analysis of openstack open-source solution for IaaS cloud computing, Advances in Intelligent Systems and Computing, 380, pp. 141-150.

[45] Sinha, A., Shrivastava, G., Kumar, P., & Gupta, D. (2020). A community-based hierarchical user authentication scheme for Industry 4.0. Software: Practice and Experience.

[46] Namasudra, S., Devi, D., Kadry, S., Sundarasekar, R., & Shanthini, A. (2020). Towards DNA based data security in the cloud computing environment. Computer Communications, 151, 539-547.

[47] Mubarakali, A., Durai, A. D., Alshehri, M., AlFarraj, O., Ramakrishnan, J., & Mavaluru, D. (2020). Fog-Based Delay-Sensitive Data Transmission Algorithm for Data Forwarding and Storage in Cloud Environment for Multimedia Applications. Big Data.

[48] Reshmi, T. R., & Azath, M. (2020). Improved self-healing technique for 5G networks using predictive analysis. Peer-to-Peer Networking and Applications, 1-17.

[49] Namasudra, S., Chakraborty, R., Majumder, A., & Moparthi, N. R. (2020). Securing multimedia by using DNA based encryption in the cloud computing environment. ACM Transactions on Multimedia Computing Communications and Applications.

[50] Patro, K. K., Reddi, S. P. R., Khalelulla, S. E., Kumar, P. R., & Shankar, K. (2020). ECG data optimization for biometric human recognition using statistical distributed machine learning algorithm. The Journal of Supercomputing, 76(2), 858-875.

[51] Rajagopal, A., Joshi, G. P., Ramachandran, A., Subhalakshmi, R. T., Khari, M., Jha, S., ... & You, J. (2020). A Deep Learning Model Based

on Multi-Objective Particle Swarm Optimization for Scene Classification in Unmanned Aerial Vehicles. IEEE Access, 8, 135383-135393.

[52] Chakchai So-In, Tri Gia Nguyen, Gia Nhu Nguyen: Barrier Coverage Deployment Algorithms for Mobile Sensor Networks. Journal of Internet Technology 12/2017; 18(7):1689-1699.

[53] Mubarakali, A., Bose, S. C., Srinivasan, K., Elsir, A., & Elsier, O. (2019). Design a secure and efficient health record transaction utilizing block chain (SEHRTB) algorithm for health record transaction in block chain. Journal of Ambient Intelligence and Humanized Computing, 1-9.

[54] Devaraj, A. F. S., Murugaboopathi, G., Elhoseny, M., Shankar, K., Min, K., Moon, H., & Joshi, G. P. (2020). An Efficient Framework for Secure Image Archival and Retrieval System Using Multiple Secret Share Creation Scheme. IEEE Access, 8, 144310-144320.

[55] Mubarakali, A. (2020). Healthcare Services Monitoring in Cloud Using Secure and Robust Healthcare-Based BLOCKCHAIN (SRHB) Approach. MOBILE NETWORKS & APPLICATIONS.

[56] Namasudra, S. (2019). An improved attribute-based encryption technique towards the data security in cloud computing. Concurrency and Computation: Practice and Experience, 31(3), e4364.

[57] Kathiresan, S., Sait, A. R. W., Gupta, D., Lakshmanaprabu, S. K., Khanna, A., & Pandey, H. M. (2020). Automated detection and classification of fundus diabetic retinopathy images using synergic deep learning model. Pattern Recognition Letters.

[58] Govinda, K., & Prasanna, S. (2015, February). Medical dialysis prediction using fuzzy rules. In 2015 International Conference on Soft-Computing and Networks Security (ICSNS) (pp. 1-5). IEEE.

[59] Sujatha, R., Navaneethan, C., Kaluri, R., & Prasanna, S. (2020). Optimized Digital Transformation in Government Services with Blockchain. In Blockchain Technology and Applications (pp. 79-100). Auerbach Publications.

[60] Govinda, K., & Prasanna, S. (2015, February). A generic image cryptography based on Rubik's cube. In 2015 International Conference on Soft-Computing and Networks Security (ICSNS) (pp. 1-4). IEEE.

[61] Anand Nayyar, Vikram Puri, Nhu Gia Nguyen, BioSenHealth 1.0: A Novel Internet of Medical Things (IoMT) Based Patient Health Monitoring System, Lecture Notes in Networks and Systems. Springer, 2019

[62] Prasanna, S., & Narayanan, V. (2017). A Novel Approach for Generation of All-Optical OFDM Using Discrete Cosine Transform Based on Optical Couplers in a Radio-Over-Fiber Link. International Journal of Advanced Research in Engineering and Technology, 8(3).

[63] Sanjeevi, P., Prasanna, S., Siva Kumar, B., Gunasekaran, G., Alagiri, I., & Vijay Anand, R. (2020). Precision agriculture and farming using Internet of Things based on wireless sensor network. Transactions on Emerging Telecommunications Technologies, e3978.

[64] Rathi, V. K., Chaudhary, V., Rajput, N. K., Ahuja, B., Jaiswal, A. K., Gupta, D., ... & Hammoudeh, M. (2020). A Blockchain-Enabled Multi Domain Edge Computing Orchestrator. IEEE Internet of Things Magazine, 3(2), 30-36.

[65] Khanna, A., Rodrigues, J. J., Gupta, N., Swaroop, A., & Gupta, D. (2020). Local mutual exclusion algorithm using fuzzy logic for Flying Ad hoc Networks. Computer Communications.