LOCATION BASED KEY MANAGEMENT FOR SECURE COMMUNICATION IN VEHICULAR AD HOC NETEORKS WITH END-TO-END AUTHENTICATION

Balamani Athina Navin Sin[1] ,P.S. Jhonu Rathna[2],P.J. Beslin Pajila[3]

[1]Department of Computer Science and Engineering, FX Engineering College, Vannarapetti 627003, India

[2]Department of Computer Science and Engineering, FX Engineering College, Vannarapetti627003, India

[3] Assistant Professor, Department of Computer Science and Engineering, FX Engineering College, Vannarapetti 627003, India

ABSTRACT:

Vehicular adhoc network (VANETs) is the safety application to reduce accident and reduce traffic, a network adhoc create a adhoc connection where, different moving vehicles and other connecting devices come to contact over a wireless medium and exchange useful information to one another Vanet security using end to end authentication to avoid intrusion in the vanet. Therefore, this paper proposes an end-to-end transfer rate adjustment mechanism in the application layer for VANET.

Keywords: Authentication, certificate, hierarchical, multidimensional, security, VANETs.

INTRODUCTION:

In todays world increasing demand for enhancing the lifestyle leads to the rapid line up of private vehicles on roads such as alarming to the death tolls and other hazards. VANETs allows to share the information such as safety information for purpose of accident prevention, post-accident analysis or traffic congestion. Some non-safety information such as car related information can also be gathered for detecting criminal activities. due to the fact that data transmitted are diffused in an open access environment.

However, highest of drivers want to maintain their information discreet and protected, and they do not want to share their confidential information. So, the private information of drivers who are distributed in this network must be protected against various threats that may damage their privacy.That is why, confidentiality, integrity and availability are the important security requirements in VANET. This project focus on security threat in vehicle network especially on the availability of this network. It regard the rational attacker who decides to lead an attack based on its adversary's strategy to maximize its own attack interests.

Our aim is to provide reliability and privacy of VANET system, by preventing attackers from violating and endangering the network.To increase the security of the data transmission in VANET system using Location Based Key management system.

To reduce the packet, drop and energy consumption in data transmission for VANET system.

To make the security system for IoT enabled Vehicle application.so reduce the communication overhead problem in VANET system.

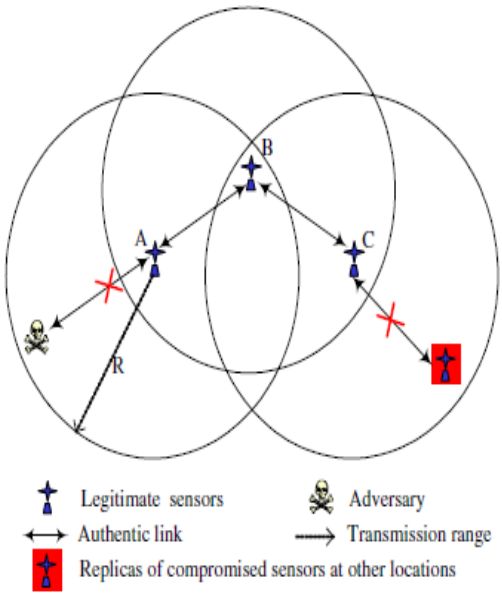
EXISTING WORK

Many researches they are worked on VANETs for secure communication

In existing works energy consumption of movable nodes are high. External attackers thread the data's which is to be transferred. Highoverhead communication problem.

Data transmission rate is very less and high packet drop due to attacker problem. Cryptographic keys not secured in VANET applications. Privacy between the owner and Vehicle drivers is not secured.

LOCATION BASED MANAGEMENT KEY

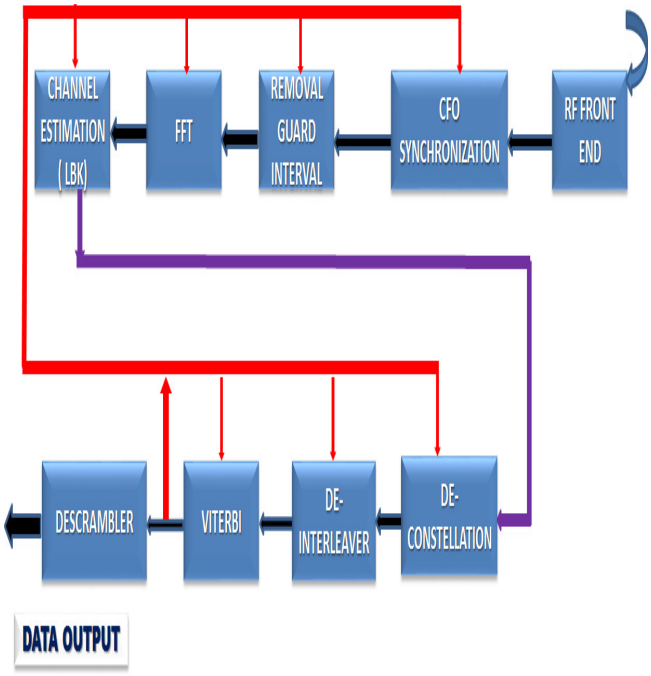


Allowing greater confidence The system exposes several factors which enable contractors to improve their performance.

Current production systems include allowance for a great deal of non-productive time (waste) which inflates costs and duration. By careful management of sub-contractors, the project is able to release much of this to improve the project performance.Working out of sequence, a common occurrence in common production systems, leads to increased risk of damage, waste, incomplete work and consequential rework. The LBMS (Location based management system)plans and controls for continuity in work crews, greatly reducing the risk of delays, costs and problems associated with rework.

Current planning systems tend to alert clients to problems too late for control action. The LBMS uses locations to calculate current production rates and in particular to control sub-contractor performance, such that an clear and accurate picture of project performance is achievable progressively and in time.

PROPOSED SYSTEM DIAGRAM



PROPOSED SYSTEM:

We propose a comprehensive routing solution that delivers messages in VANETs via a self-organized moving-zone based architecture formed using pure vehicle-to-vehicle communication.

Our approach integrates moving object modeling and indexing techniques to vehicle management.Moving object techniques allow us to provide a realistic

cluster-based representation, in that vehicles are grouped together according to their actual moving patterns**.**

ADVANTAGES OF PROPOSED SYSTEM

Routes maintained only between nodes who need to communicate reduces overhead of route maintenance.

Route caching can further reduce route discovery overhead

A single route discovery may yield many routes to the destination, due to intermediate nodes replying from local caches.

Using fewer wires means it costs less to set up a network, particularly for large areas of coverage.

The more nodes you install, the bigger and faster your wireless network becomes.

They rely on the same WiFi standards (802.11a, b and g) already in place for most wireless networks.

PROPOSED ALGORITHM

Dual Queue Scheduling Algorithm(DQSA)

Dual scheduling algorithm that uses rate control and queue length based scheduling to allocate resources for a generalized switch. first consider a saturated system in which each user has infinite amount of data to be served.

the asymptotic optimality of the dual Scheduling algorithm for such a system, which says that the vector of average service rates of the scheduling algorithm maximizes some aggregate concave utility functions.

Problem statement:

In existing works energy consumption of movable nodes are high.

External attackers thread the data's which is to be transferred.

High overhead communication problem.

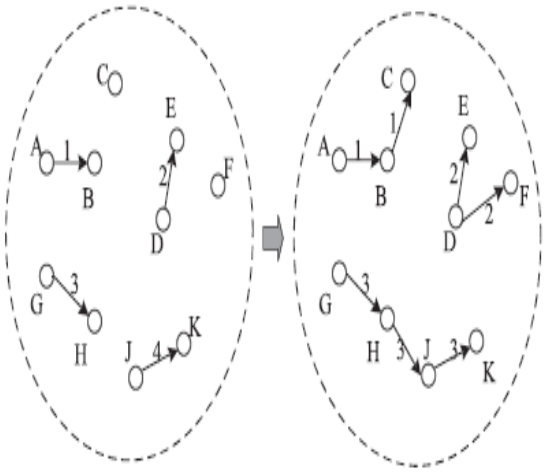
Data transmission rate is very less and high packet drop due to attacker problem.

Cryptographic keys not secured in VANET applications.

Privacy between the owner and Vehicle drivers is not secured.

PROPOSED METHODOLOGY(AODV):

ADOV (**AD HOC ON DEMAND DISTANCE VECTOR**) it's used for builds routes between nodes only if they request by the source node.it don't create in extra traffic for communication this protocol designed for wireless and mobile adhoc networks then it support for both unicast and multicast routing it was developed by NOKIA RESEARCH CENTER, THE UNIVERSITY OF CALIFORNIA.It'sa self-staring and loop free protocol.



Node creation: Before starting to create a node, determine the following:

the name, address, and location of the node are known. the location and type of units physically present in the NE are known. the main unit must be assigned before the interfaces associated with this unit can be assigned. For example, a tributary port unit must be assigned before the ports for this unit can be assigned**.**

Packet Drop: It might get lost by accident, but packets can also be lost because a router receives it and specifically decides not to pass it on to the next hop. This deliberate loss of a packet is called dropping. (Thereare legitimate reasons for dropping a packet: for example, if the router is overloaded, or if the router believes the packet is part of a DOS attack.

RELATED WORK

It proposal withstands for (DOS) denial of service and also decrease the length of nodes request messages. its support both asymmetric and symmetric cryptographic algorithm then the computational complexity with create the delay in transmission. authentication scheme is depending on key agreement approach such as system setup phase, user registration phase, user login and authentication phase and password changes phase

TITLE: Security analysis of vehicular ad hoc networks based on attack tree

AUTHOR AND YEAR: MeriemHOUMER et al.2018

ADVANTAGES: It focus on security threat in vehicle network especially on the availability of this network. Then it regards the rational attacker who decides to lead an attack based on its adversary's strategy to maximize its own attack interests

DRAWBACK Cryptographic keys not secured. High energy consumption due to attackers.

TITLEMultidimensional Security Provision for Secure Communication in Vehicular Ad Hoc Networks Using Hierarchical Structure and End-to-End Authentication

AUTHOR AND YEAR:GULSHAN KUMAR et al.2018

ADVANTAGES: In this paper, provided a solution for the VANETs security using end to end authentication to avoid intrusion in the VANETs

After verifying the communicating entities, the data are transmitted in encrypted form thus the proposed approach CIA security services to VANETs communication

DRAWBACK: Overhead communication is high. Slow data transmission

TITLE: Distributed key management scheme based on ECC for Heterogeneous Sensor Networks

AUTHOR AND YEAR: Jiu-ru Wang et al.2014

ADVANTAGES: Taking advantages of distributed routing protocol, the scheme achieves to reduce communication cost and improve adaptive capacity. In the key agreement process, the scheme utilizes identity-based Encrypt to reduce storage requirement.

DRAWBACK: The data loses are frequently occurs. Data is not verifiable and sleep mode is occurred this will reduce the life time of sensors.

TITLE: Secure and Efficient Broadcast

Authentication in Wireless Sensor Networks

AUTHOR AND YEAR: Taekyoung kwon et al.2016

ADVANTAGES: A specific design of one way chains using a block cipher is given for efficiency i.e., without additional encryption. Dos attacks are resisted without requiring large buffers or strict commitment delivery guarantee, both of which were required for multilevel TESLA**.**

DRAWBACK: The data losses are frequently occurs. Data is not verifiable and sleep mode is occurred this will reduce the life time of sensors.

TITLE: Location dependent key management in sensor networks without using deployment knowledge**.**

AUTHOR AND YEAR: F. Anjum et al,2010**.**

ADVANTAGES: The communication overhead between nodes during shared key discovery is dramatically reduced. Our scheme guarantees message authentication and integrity with respect to fake or tampered message during communication. The performance analysis and simulation results show that our scheme performs better than previous.

DRAWBACK: Stillsome communication overhead problem isthere. Did not tracked the shortest path between the nodes.

CONCLUSION

This open network of vehicles is referred as VANET which gives numerous applications so as to make the road travel experience more efficient, safe, easy and pleasant by decreasing traveling time, road congestion, increasing road capacity, avoiding congested areas and emergency situations and we have used a hierarchical architecture of message transmission using end to end authentication to provide message integrity and authentication.

REFERENCES:

[1] P. M. Khilar and S. K. Bhoi, ``Vehicular communication: A survey," *IET Netw.*, vol. 3, no. 3, pp. 204217, 2014.

[2] J. A. C. GuerreroIbáñez, C. Flores-Cortés, and S. Zeadally, ``Vehicular ad-hoc networks (VANETs): Architecture, protocols and applications,'' in *Next-Generation Wireless Technologies*. London, U.K.: Springer, 2013, pp. 4970.

[3] W. Liang, Z. Li, H. Zhang, Y. Sun, and R. Bie, ``Vehicular ad hoc networks: Architectures, research issues, methodologies, challenges, and trends," *Int. J. Distrib. Sens. Netw.*, vol. 11, no. 8, pp. 102113, 2015.

[4] S. Al-Sultan, M. M. Al-Doori, A. H. Al-Bayatti, and H. Zedan, ``A comprehensive survey on vehicular ad hoc network," *J. Netw. Comput. Appl.*, vol. 37, pp. 380392, Jan. 2014.

[5] G. Karayiannis*et al.*, ``Vehicular networking: A survey and tutorial on requirements, architectures, challenges, standards and solutions," *IEEE Commun. Surveys Tuts.*, vol. 13, no. 4, pp. 584616, 4th Quart., 2011.

[6] S. Sen, N. Santhapuri, R. R. Choudhury, and S. Nelakuditi, ``Successive interference cancellation: A back-of-the-envelope perspective," in *Proc. 9th ACM SIGCOMM Workshop Hot Topics Netw. (Hotnets-IX)*, 2010, Art. no. 17.

[7] P. Fazio, F. De Rango, and C. Sottile, ``Anewinterference aware on demand routing protocol for vehicular networks," in *Proc. Int. Symp. Perform. Eval. Computer. Telecomm. Syst.*, The Hague, The Netherlands, 2011, pp. 98103.

[8] G. KUMAR and Saha “Multidimensional security provision for secure communication in vehicular adhoc networks using hierarchical structure and end to end authentication”

[9] Prentice hall “adhoc and mobile wireless network”

[10] L. Fan, X. Lei, N. Yang, T. Q. Duong, and G. K. Karagiannidis, ``Secrecy cooperative networks with outdated relay selection over correlated fading channels," *IEEE Trans. Veh. Technol.*, vol. 66, no. 8, pp. 75997603, Aug. 2017