WWW.IJRPR.COM

International Journal of Research Publication and Reviews

Journal homepage: www.ijrpr.com ISSN 2582-7421

SECURED COMMUNICATION AND ENERGY EFFICIENT FOR VANET USING LOCATION DEPENDENT KEY MANAGEMENT

C .K. Morarji[a], Dr.N.Sathish Kumar[b], C.Isha[c]

[a]Research Scholar, Anna University, Chennai, India.
[b]Professor, Sri Ramakrishna Engineering College, Coimbatore, India.
[c]PG Student, Rohini College of Engineering & Technology, Kanyakumari, India.

ABSTRACT:

In the Vehicular Ad hoc Networks (VANET), performance is the key factor for the development of a standard routing protocol. The general characteristics of VANET are dynamic vehicle network topology and mobility. The choice of a better next forwarding hop vehicle among the available neighboring vehicles will lead better use of the route and also minimize the delays. However, there is a need for an efficient decision making in selecting the route for successful packet delivery. This project proposes a new routing algorithm called "Fuzzy assisted Cuckoo Search Algorithm". This algorithm uses a fuzzy logic technique that helps in better decision making to select the next hop for packet forwarding. Metrics like distance, direction, velocity, density and position of next hop vehicle are placed into the fuzzy logic system. In order to make the communication more secured location based key management is utilized. Under LBK, Lagrange based crypto systems are used for the generation and the management of keys. The performance of the proposed algorithm and the simulation results highlights that it is more effective in selecting the better forwarding hop for improved performance. Also the communication is secured when compared to other encryption techniques.

Keywords: VANET, Fuzzy assisted CS algorithm, Lagrange based crypto system

Introduction:

An important component of an intelligent transportation system (ITS) is the vehicular communication network (VANET) that enables information exchange among vehicles. A VANET is a special case of a Mobile Ad Hoc Network (MANET) in which vehicles equipped with wireless and processing capabilities can create a spontaneous network while moving along roads [1]. Communication in a VANETs allows vehicles to share different kinds of information such as safety information for the purpose of accident prevention, post-accident analysis or traffic congestion [2]. Each vehicle, in VANET, is equipped with a sensor whereby vehicles are able to communicate with each other via inter-vehicle communication (IVC) as well as with road side equipment via Roadside to Vehicle Communication (RVC).This communication can be used for a broad range of safety and non-safety applications, allow for value added services such as vehicle safety, automated toll payment, traffic management, enhanced navigation, location-based services such as finding the closest fuel station, restaurant or travel lodge and infotainment applications such as providing access to the Internet [3].

Problem statement

In the existing systems, ad hoc on demand distance vector routing (AODV) protocol and modified AODV is implemented in finding the shortest path to deliver the packets. The major problem with these protocols is that, they do not have memory. Once an intrusion is detected in the system, it does not have memory to store the information regarding the problem. So each time the process gets repeated until an intrusion is detected. Thus the energy of nodes is being increased producing considerable losses.

In order to ensure security, an end to end authentication scheme is used. Once the communication entities are verified, the data is transmitted in the encrypted form and thus security is ensured in the system. End to end authentication increased the risk of overhead communication and leads to slow data transmission. Also, location dependent key management was implemented in the existing system without using deployment knowledge so, the shortest path was not determined.

Proposed System

Identification and location of vehicles with the absence of packet loss and security problems becomes biggest threat in the existing systems. In the developed work, Fuzzy assisted cuckoo search optimization technique is utilized to determine the shortest and the best route. The proposed Fuzzy Assisted Cuckoo Search Algorithm allows the network service providers to implement a more customer-centric network infrastructure thus improving their spectral efficiency. The network can automatically adapt to dynamic customer needs and capacity demand fluctuations of mobile users in VANETs. Key system is utilized for securing the data transmission in between vehicles. In the developed work the VANET system is differentiated into a number of groups according to their distribution of location. It is observed that the vehicle nodes which belong to same region will be neighboring nodes. Henceforth location dependent key management (LDK) technique is utilized. It helps the members of same region to produce group keys. The keys are generated using Lagrange based crypto system. Lagrange based crypto systems generates key based on group theory and moreover, the generated keys are 128 bit and so packet threat is lower when compared to other systems.

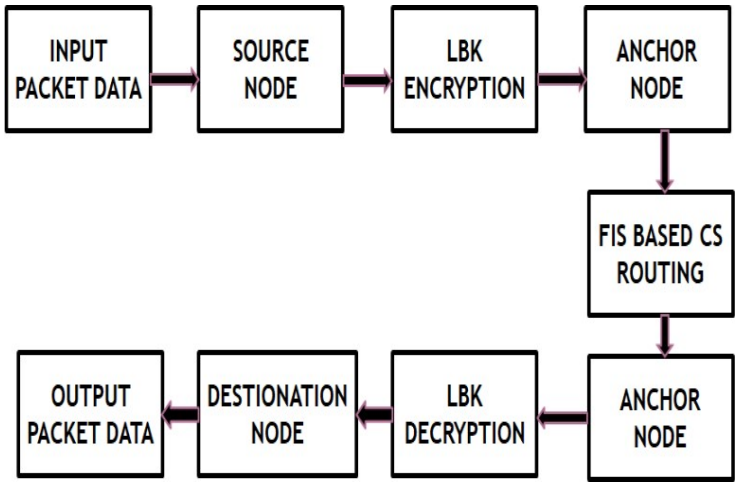

Fig. 1 - Block Diagram

Fuzzy Assisted Cuckoo Search Algorithm

The CS algorithm was inspired by the obligate brood parasitism of some cuckoo species by laying their eggs in the nests of host birds. Some cuckoos have involved in such a way that female parasitic cuckoos can imitate various colors and patterns of the eggs of a few chosen host species. This reduces the probability of the eggs being abandoned so re-productivity increases. It is important to mention that several host birds engage direct conflict with intruding cuckoos. If host birds discover the eggs are not their own, they will either throw them away or simply abandon their nests and build new ones. Parasitic cuckoos often choose a nest where the host bird just laid its own eggs. In general, the cuckoo eggs hatch slightly earlier than their host eggs. Once the first cuckoo chick is hatched, his first instinct action is to evict the host eggs by blindly propelling the eggs out of the nest. This action results in increasing the cuckoo chick's share of food provided by its host bird. Moreover, studies show that a cuckoo chick can imitate the call of host chicks to gain access to more feeding opportunity. The breeding behavior of cuckoo can be applied to various optimization problems. Levy Flights mechanism is used instead of simple random walk to improve the performance of CS by Yang and Deb.

Each egg in a nest represents a solution, and a cuckoo egg represents a new occurred solution. The aim is to employ the new and potentially better solutions (cuckoos) to replace not-so-good solutions in the nests. In the simplest form, each nest has one egg. The algorithm can be extended to more complicated cases in which each nest has multiple eggs representing a set of solutions (Yang 2009; Yang 2010). The CS algorithm is based on three idealized rules:

- Each cuckoo lays one egg at a time, and dumps it in a randomly chosen nest.
- The best nests with high quality of eggs (solutions) will carry over to the next generations.
- The number of available host nests is fixed, and a host can discover an alien egg with probability pa $\varepsilon[0,1]$. In this case, the host bird can either throw the egg away or abandon the nest to build a completely new nest in a new location (Yang 2009).

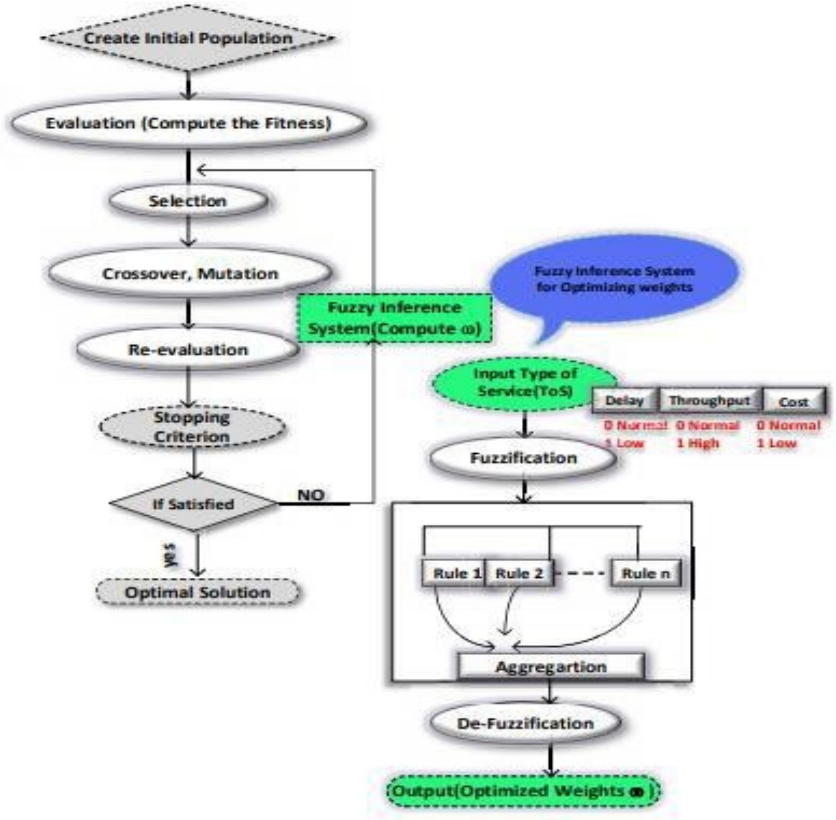

Fig. 2 - Cuckoo Search Algorithm

Cuckoo Search Based Route Discovery Process

The route discovery can be done by cuckoo search algorithm. The detailed clarification of selection process is offered in subsections.

Initialization

At first, N number of solutions or nests is randomly generated in the initialization process. Here, "0" and "1" are randomly initialized for each nest.

Fitness Selection

The selection of the fitness is a crucial aspect in cuckoo search algorithm. It is used to evaluate the aptitude (goodness) of candidate solutions. Here, minimum distance is selected as the best fitness to find the optimal route. To evaluate an individual, an objective function (i.e., fitness function) is applied that considers the shortest path from the source to the destination as the best one. In other words, the fitness fi of the individual 'i' is the sum of the distance (dis) between each two adjacent nodes 'nj' and 'nj+1' in the path from the source node 's' to the destination node 'd', calculated by the following formula:

$$Fitness\left(nest_n^k\right) = \sum_{j=s}^{d} dis\left(n_j, n_{j+1}\right)$$

New Solution Generation Using Levy Flight

To generate novel solution, levy flight method is applied at this point. It is a type of random walk. It will arbitrarily search for length to produce novel solution which has a heavy-tailed distribution. Levy flight has a huge coverage range in search space. Both, original and adapted codes employ random step sizes. We employ different function set for computing this step size compared to the original code. In the original code, step size is computed by subsequent code expression:

The difference between cuckoo and modified step size cuckoo is that levy flight is used in both cases but step size of levy f light is changed in modified

$$S_i^{t+1} = S_i + stepsize \oplus N(0,1)$$

cuckoo. Like this, higher fitness solutions contain small benefit over solutions with lower fitness. At this point, every iteration, worst nests based on the probability are substituted with a novel set of solutions. The algorithm stops its implementation only if maximum number of iterations is attained and the nest which is containing the best fitness value is chosen and it is given as best route to route discovery.

Route Repairing Phase

The periodic sending of beacon packets in the transmission range between the node and its neighbors helps to ensure the stability of the connections. If there is connectivity problem, the node detects the broken link and any route passing through this broken link is considered as disconnected

Location Dependent Key Management

The basic element for secured information transmission is key management. Key management is the process by which the keys are distributed to nodes on the network and how they are further updated if required, erased when the keys are compromised, etc. A large part of the cryptographic system relies on the basic secured, vigorous key management system. When employing cryptographic schemes, a key management service is always required

In the developed work the VANET system is differentiated into a number of groups' according to their distribution of location. It is observed that the vehicle nodes which belong to same region will be neighboring nodes. Henceforth location dependent key management (LDK) technique is utilized. It helps the members of same region to produce group keys.

Lagrange Based Crypto System

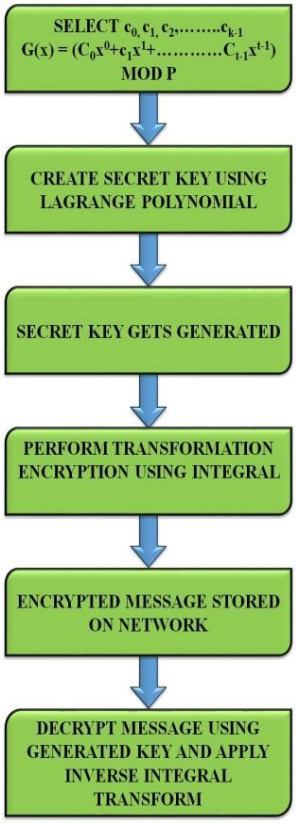

Fig. 3 - Flowchart of LBK

Phase 1: Secret Key Generation

Create node id by using a random number generator. By making use of this node id, produce a secret key. Recreate secret key using a fixed threshold number of node id. Select c0, c1, c2.
Consider a polynomial equation GF(p)

Select C0, C2, ……., Ck-1

$G(x) = (C0X^0 + C1X^1 + \ldots\ldots\ldots\ldots Ct\text{-}1X^{t-1}) \bmod p$

Here, G (0) = C0

After this, the sign-in id is offered with its partial key.

Si=F(idi)

Compute polynomial by using Lagrange interpolation. It is computed as follows,

$F(x) = \sum_{i=1}^{k} y_i \prod_{1\le j\le k} , j\neq i$

$= \frac{x-x_j}{x_i-x_j}$

If G (0) =C0=S, the shared key can be represented as,

$K = \sum_{i=1}^{k} D_i Y_i$

$D_i = \prod_{1\le j\le k, j\neq 1} \frac{x_j}{x_j-x_i}$

The secret key is created by using a minimum threshold using,

$(0) = a0 mod\ p = secret\ key$

Phase 2: Encryption

Using Lagrange polynomial, a secret key gets generated. The generated key is used in integral transform to encrypt the information. Finally, an encrypted message is generated. Encryption is performed by using Integral transformation. It helps to protect the data from third party users. The integral function is defined for $0\leq t< \infty$ is the normal calculus integration.

$\{f(t)\} = (s) = (t)e^{-st}dt$

$L^{-1}\{F(s)\} = f(t)$

Where L^{-1} represents the inverse integral transform.

In this proposed work, integral transformation takes place to provide confidentiality, security during the transmission of information from the server to the client. Then by making use of exponential function it can be solved,

$$e^{kx} = 1 + \frac{kx}{1!} + \frac{(kx)^2}{2!}\frac{(kx)^3}{3!}\ldots,$$

K represents any real number.

Multiply both sides by x,

$$xe^{kx} = x\left(1 + \frac{kx}{1!} + \frac{(kx)^2}{2!} + \frac{(kx)^3}{3!} + \cdots\right)$$

$xe^{kx} = x1 + \frac{kxx}{1!} + \frac{x(kx)^2}{2!} + \frac{x(kx)^3}{3!} + \cdots$ K is a secret key produced by Lagrange polynomial.

Phase 3: Decryption

This process transforms the encrypted message back to its original form by using some operation. By using shared partial information, create a secret key. Using inverse integral, decrypt the message back to the original information. Decryption operation decrypts the encrypted text to its normal form. To perform this operation some mathematical computations were performed. It is expressed as follows,

$G_i = c_i + 26d_i$

Where 'i' ranges from 0 to n using di create all Gi.

$$L\{f(x)\} = \left(\frac{G_0}{s_1} + \frac{G_1}{s_3} + \frac{G_2}{s_4} + \frac{G_3}{s_5} + \frac{G_4}{s_6}\right)$$

Taking inverse transform on both the sides using Lagrange interpolation produce session key and create $p0, p1, p2 \ldots \ldots \ldots pn$

Results and Conclusion

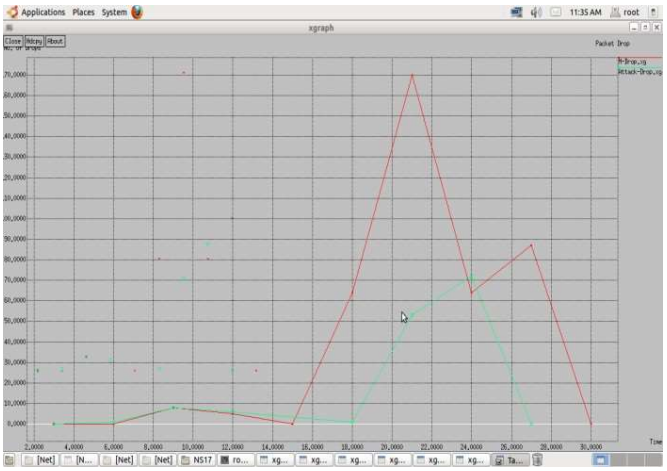

Fig. 4 - Packet Drop Comparison

The simulation results of the proposed algorithms in comparison with the existing algorithms proved to be effective in case of packet loss, throughput and packet delivery ratio. The proposed algorithms have overcome the drawbacks of the existing algorithm techniques. Since fuzzy has memory, fuzzy assisted cuckoo search optimization technique is more effective. The packet drop ratio is also less when compared to other techniques. Security is also ensured by using Lagrange based crypto systems. Thus the packets are delivered to the destination with less energy and high security.

REFERENCES:

1. F.D. Da Cunha, A. Boukerche, L. Villas, A.C. Viana, A.A. Loureiro, Data communication in VANETs: a Survey, Challenges and Applications. (Research Re-port) RR-8498, INRIA Saclay, INRIA, 2014, https://hal .inria .fr /hal -00981126 /document.
2. P.M. Khilar, S.K. Bhoi, "Vehicular communication: a survey," in IET Networks, vol. 3, 2014, pp. 204–217.
3. Sherali Zeadally, Ray Hunt, Yuh-Shyan Chen, Angela Irwin and Aamir Hassan. Vehicular ad hoc networks (VANETS): status, results, and challenges. Telecommunication Systems. Springer, 217–241 (2010).
4. Xin-She Yanga, Xing-Shi Heb, "Bat algorithm and cuckoo search algorithm",Chapter 2.
5. Gulshan Kumar, Rahul Saha, Mritunjay Kumar Rai, And Tai-Hoon Kim, "Multidimensional Security Provision For Secure Communication In Vehicular Ad Hoc Networks Using Hierarchical Structure And End-To-End Authentication".