Ilkogretim Online - Elementary Education Online, 2020; Vol 19 (Issue 3): pp. 4690-4700
http://ilkogretim-online.org
doi: 10.17051/ilkonline.2020.03.735623

Forward Decision Model For Routing In Urban Environment Of VANETS Using Improved Firefly Optimization Algorithm

[1]M.S.U laganathan , [2]Dr.SU.Suganthi , [3]Ms.Karthikayani , [4]Mr.M.Vasanth

[1],Asst Professor, Department of Computer and Communication Engineering, Sri Sairam Institute of Technology

[2],Assoc Professor &Head, Department of Computer and Communication Engineering, Sri Sairam Institute of Technology

[3],Student ,Department of Computer and Communication Engineering, Sri Sairam Institute of Technology

[4]Manager, Wipro private Ltd

Abstract— Vehicular ad hoc network (VANET) is a special form of Mobile Ad hoc Network (MANET), which plays a key role in the Intelligent Transportation System (ITS). Though many outstanding geographic routing protocols are designed for VANETs, most of the existing proposals only consider a single factor, which makes the link easy to break. In this research, we propose a Routing Protocol Based on Multi-factor Decision (RMFD), which utilizes several features. The scheme is divided into two parts, namely vehicular decision management and intersection decision management. In the vehicular component, a route is established between two adjacent static nodes by calculating a fuzzy performance score using Triangular Fuzzy Number (TFN). In the Intersection management, static nodes located at the intersection are selects to decide which road segment the data will be forwarded to

Index Terms— MANET, Intelligent Transportation System, Routing Protocol Based on Multifactor Decision, Triangular Fuzzy Number

I. INTRODUCTION

Vehicular ad hoc network (VANET) is a special form of Mobile Ad hoc Network (MANET), which plays a key role in the Intelligent Transportation System (ITS). Though many outstanding geographic routing protocols are designed for VANETs, most of the existing proposals only consider a single factor, which makes the link easy to break. In this paper, Routing Protocol Based on Multi-factor Decision (RMFD) is proposed, which utilizes several features. The scheme is divided into two parts, namely vehicular decision management and intersection decision management. In the vehicular component, a route is established between two adjacent static nodes by calculating a fuzzy performance score using Triangular Fuzzy Number (TFN). In the Intersection management, static nodes located at the intersection are selects to decide which road segment the data will be forwarded to.

The rapid increase in the number of vehicles and advancements in mobile internet has drawn the attention of experts in academia and industry towards vehicular ad-hoc networks (VANETs). VANET is a special kind of mobile ad-hoc networks (MANETs), where vehicles are the main communication participants [1,2]. VANET system communication is in two forms, namely vehicle-to-vehicle (V2V) and vehicle-to-infrastructure (V2I). In contrast to MANETs, VANETs are characterized by high mobility. Hence, the network topology of VANETs changes continuously. As a result of vehicular movements, communication link conditions among vehicles vary frequently, influencing intermittent network disconnection. Nevertheless, mobility of vehicles is predictable through GPS indicators, such as obstacles on both sides of the road segment, vehicle position, and speed.

Owing to the characteristics of VANETs, designing a suitable routing protocol remains challenging due to the requirement of a high delivery ratio at the final destination within a short time. In VANETs, data packets are transferred along road segments and routing decisions are made at intersections. Hence, if a link breaks, the packet will be retransferred to the last intersection node to determine another potential route. Hence, SNs at intersections analyze connection information of adjacent SNs to guarantee connectedness. Accordingly, vehicles select potential road segments to forward data packets. Selecting a vehicle from the candidate vehicles as the next hop between two SNs remains a key challenge to be addressed.

In topology-based routing protocols, the links' information that exists in the network is used to perform packet forwarding. They can also further be divided into proactive and reactive routing. The distinct feature of proactive routing is that the full routing information such as the next forwarding hop is maintained in the background regardless of communication requests. In reactive routing, a route will be established only when a vehicle must communicate with another vehicle. The two more famous topology-based routing protocols are ad hoc on-demand distance vector (AODV) [8] and the dynamic source routing (DSR). These two routing protocols maintain only current route information to reduce packet overhead. Nevertheless, increasing overhead size is inevitable with increasing network diameter results from vehicle mobility.

Geographic routing (GR) determines forwarding route considering destination position and the positions of the vehicle's 1-hop neighbors. Vehicles that are within a vehicle's radio range will become neighbors of the vehicle. Geographic routing assumes that not only every vehicle knows its position, but also the sending vehicle knows the receiving vehicle's position by the global positioning system (GPS) unit. Since GR neither exchanges link state information nor maintains established routes as topology-based routing protocols, it is more robust and promising compared with VANETs which are highly dynamic. GR can be sub-classified into three categories, namely non-delay tolerant network (non-DTN), delay tolerant network (DTN), and hybrid [10]. DTN considers disconnectivity, whereas non-DTN does not consider intermittent connectivity and is suitable for densely populated VANETs. Hybrid combines non-DTN and DTN routing protocols to exploit partial network connectivity.

The key objective of non-DTN is to minimize packet delivery time from source to destination. Greedy forwarding is the commonly used technique in which the fundamental principle is to forward packets to a neighbor, which is geographically closer to the destination. However, the local maximum issue could appear when a vehicle reaches closer to the destination and finds no neighbors closer to the destination than the vehicle itself. Greedy perimeter stateless routing (GPSR) is the most well-known geographic routing protocol in VANETs. A vehicle forwards a packet to a 1-hop neighbor which is geographically closest to the destination vehicle. This mode is called greedy mode, and a recovery mode is switched to when a packet reaches the local maximum. The packet is forwarded along the perimeter of a planar graph without crossing edges based on the right-hand rule. If the packet reaches a vehicle whose distance to the destination is closer than the vehicle at the local maximum to the destination, the packet resumes forwarding in greedy mode.

Greedy perimeter coordinator routing (GPCR) enhances GPSR by using the Dijkstra shortest path algorithm to determine the junctions that have to be traversed based on a static street map. A packet has to be forwarded to a vehicle that is located on the junction because junctions are the only places where routing decisions are made. Packets can be forwarded between the junctions in greedy mode. And GPCR consists of two parts. One is a restricted greedy forwarding procedure and another is a repair strategy that is based on the topology of real-world streets and junctions. Hence, GPCR not only eliminates the inaccuracy of vehicle planarization but also improves routing performance as packets travel shorter hops in the perimeter mode. More and more researchers proposed protocols considering urban traffic characteristics and intersections.

The shortest-path-based traffic-light-aware routing (STAR) protocol considers the status of traffic lights. In STAR, packets are attempted to forward to a connected road segment based on the status of traffic lights. Similarly, the intersection-based connectivity aware routing (iCAR) obtains the road connectivity proactively and decides the next intersections by evaluating the lifetime of a link based on real-time traffic information. However, both STAR and iCAR only consider the traffic conditions of the current road segment and ignore the subsequent routing. The infrastructure-based connectivity aware routing (iCAR-II) not only adopts the intersection-based connectivity-aware routing, but also makes the routing direction based on the global network topology. The strategy of iCAR-II is to construct a global network topology by predicting the network connectivity and update location servers with real-time network information. It then selects the shortest path from source to destination. Though iCAR-II enables multi-hop vehicular application, it also loses packets when roads are disconnected. Furthermore, based on the name of iCAR-II, it is known that iCAR-II is very dependent on infrastructure.

II. BACKGROUND AND RELATED WORK

A.Network Architectures:

VANET architectures are classified into: 1. The Mobile Zone 2. The Infrastructure Zone. The Mobile Zone consists all the vehicles and portable devices like smart phones and navigations devices. The Infrastructure Zone comprised of roadside components like Traffic light and management centers.

There are four types of Communication types in VANET. The figure 1 shows each function of communication.

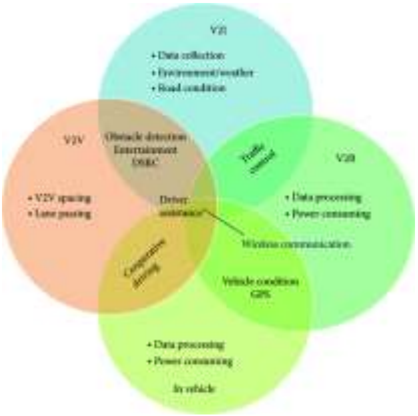

Figure 1 Functions of Communication Type

In-vehicle communication: It can detect vehicles performance. Example: Driver's drowsiness detection

Vehicle – to – Vehicle communication: It's a data transfer platform. In which information are shared among vehicles

Vehicle – to – road infrastructure: It provides weather reports and real time traffic for drivers

Vehicle – to – broadband cloud: this communication will be useful to provide driver assistance from cloud

B. ROUTING PROTOCOLS IN WIRELESS NETWORK

Table-Driven (or Proactive)

The nodes maintain a table of routes to every destination in the network, for this reason they periodically exchange messages. At all times the routes to all destinations are ready to use and as a consequence initial delay before sending data are small. Keeping routes to all destinations up-to-date, even if they are not used, is a disadvantage with regard to the usage of bandwidth and of network resources.

On-Demand (or Reactive)

These protocols were designed to overcome the wasted effort in maintaining unused routes. Routing information is acquired only when there is a need for it. The needed routes are calculated on demand. This saves the overhead of maintaining unused routes at each node, but on the other hand the latency for sending data packets will considerably increase.

DESTINATION-SEQUENCE DISTANCE VECTOR PROTOCOL

DSDV has one routing table, each entry in the table contains: destination address, number of hops toward destination, next hop address. Routing table contains all the destinations that one node can communicate. When a source A communicates with a destination B, it looks up routing table for the entry which contains destination address as B. Next hop address C was taken from that entry. A then sends its packets to C and asks C to forward to B. C and other intermediate nodes will work in a similar way until the packets reach B. DSDV marks each entry by sequence number to distinguish between old and new route for preventing loop.

DSDV use two types of packets to transfer routing information: full dump and incremental packet. The first time two DSDV nodes meet, they exchange all of their available routing information in full dump packet. From that time, they only use incremental packets to notice about change in the routing table to reduce the packet size. Every node in DSDV has to send update routing information periodically. When two routes are discovered, route with larger sequence number will be chosen. If two routes have the same sequence number, route with smaller hop count to destination will be chosen.

DSDV has advantages of simple routing table format, simple routing operation and guarantee loop-freedom. The disadvantages are (i) a large overhead caused by periodical update (ii) waste resource for finding all possible routes between each pair, but only one route is used.

On-demand Routing Protocols

In on-demand trend, routing information is only created to requested destination. Link is also monitored by periodical Hello messages. If a link in the path is broken, the source needs to rediscovery the path. On-demand strategy causes less overhead and easier to scalability. However, there is more delay because the path is not always ready. The following part will present AODV, DSR, TORA and ABR as characteristic protocols of on-demand trend.

AD HOC ON DEMAND DISTANCE VECTOR ROUTING PROTOCOL

Ad hoc on demand distance vector routing (AODV) is the combination of DSDV and DSR. In AODV, each node maintains one routing table. Each routing table entry contains:

- Active neighbor list: a list of neighbor nodes that are actively using this route entry.
- Once the link in the entry is broken, neighbor nodes in this list will be informed.
- Destination address
- Next-hop address toward that destination
- Number of hops to destination
- Sequence number: for choosing route and prevent loop
- Lifetime: time when that entry expires

Routing in AODV consists of two phases: Route Discovery and Route Maintenance. When a node wants to communicate with a destination, it looks up in the routing table. If the destination is found, node transmits data in the same way as in DSDV. If not, it starts Route Discovery mechanism: Source node broadcast the Route Request packet to its neighbor nodes, which in turns rebroadcast this request to their neighbor nodes until finding possible way to the destination.

When intermediate node receives a RREQ, it updates the route to previous node and checks whether it satisfies the two conditions:

(i) there is an available entry which has the same destination with RREQ

(ii) its sequence number is greater or equal to sequence number of RREQ. If no, it rebroadcast RREQ. If yes, it generates a RREP message to the source node. When RREP is routed back, node in the reverse path updates their routing table with the added next hop information.

If a node receives a RREQ that it has seen before (checked by the sequence number), it discards the RREQ for preventing loop. If source node receives more than one RREP, the one with greater sequence number will be chosen. For two RREPs with the same sequence number, the one will a smaller number of hops to destination will be chosen. When a route is found, it is maintained by Route Maintenance mechanism: Each node periodically sends Hello packet to its neighbors for proving its availability. When Hello packet is not received from a node in a time, link to that node is considered to be broken. The node which does not receive Hello message will invalidate all of its related routes to the failed node and inform another neighbor using this node by Route Error packet. The source if still want to transmit data to the destination should restart Route Discovery to get a new path.

AODV has advantages of decreasing the overhead control messages, low processing, quickly adapt to network topology change, more scalable up to 10000 mobile nodes. However, the disadvantages are that AODV only accepts bi-directional link and has much delay when it initiates a route and repairs the broken link.

DYNAMIC SOURCE ROUTING PROTOCOL

DSR is a reactive routing protocol which is able to manage a MANET without using periodic table-update messages like table-driven routing protocols do. DSR was specifically designed for use in multi-hop wireless ad hoc networks. Ad-hoc protocol allows the network to be completely self-organizing and self-configuring which means that there is no need for an existing network infrastructure or administration.

For restricting the bandwidth, the process to find a path is only executed when a path is required by a node (On-Demand-Routing). In DSR the sender (source, initiator) determines the whole path from the source to the destination node (Source-Routing) and deposits the addresses of the intermediate nodes of the route in the packets.

Compared to other reactive routing protocols like ABR or SSA, DSR is beacon-less which means that there are no hello-messages used between the nodes to notify their neighbors about her presence.

DSR was developed for MANETs with a small diameter between 5 and 10 hops and the nodes should only move around at a moderate speed.

DSR is based on the Link-State-Algorithms which mean that each node is capable to save the best way to a destination. Also, if a change appears in the network topology, then the whole network will get this information by flooding.

DSR contains 2 phases

- Route Discovery (find a path)

- Route Maintenance (maintain a path)

TEMPORARY ORDERED ROUTING ALGORITHM

TORA is based on link reversal algorithm. Each node in TORA maintains a table with the distance and status of all the available links. Detail information can be seen.

TORA has three mechanisms for routing:

Route Creation: TORA uses the "height" concept for discovering multiple routes to a destination. Communication in TORA network is downstream, from higher to lower node. When source node does not have a route to destination, it starts Route Creation by broadcasting the Query messages (QRY). QRY is continuing broadcasted until reaching the destination or intermediate node that have the route to the destination. The reached node then broadcast Update (UPD) message which includes its height. Nodes receive this UPD set a larger height for itself than the height in UPD, append this height in its own UPD and broadcast. This mechanism is called reversal algorithm and is claimed to create number of direct links from the originator to the destination.

Route Maintenance: Once a broken link is discovered, nodes make a new reference height and broadcast to their neighbors. All nodes in the link will change their reference height and Route Creation is done to reflect the change.

Route Erasure: Erases the invalid routes by flooding the "clear packet" through the network. The advantages of TORA are: having multiple paths to destination decreases the route creation in link broken case therefore decrease overhead and delay to the network. TORA is also claimed to be effective on large and mildly congested network. The drawbacks are requiring node synchronization due to "height" metric and potential for oscillation. Besides that, TORA may not guarantee to find all the routes for reserving in some cases.

C. FUZZY LOGIC-BASED GEOGRAPHIC ROUTING FOR URBAN VEHICULAR NETWORKS:

Vehicular ad hoc networks (VANETs) are envisioned as the future of intelligent transportation systems, which enable various kinds of applications aiming at improving road safety and transportation efficiency. Uni-cast routing is required for many of these applications. As VANET is expected to be massive in terms of number of nodes and amount of generated information, geographic routing protocols are considered the most suitable for such network owing to their scalability. Due to VANETs' extremely dynamic topology and variable channel condition, multiple metrics related to vehicles' mobility, link quality, and bandwidth availability need to be considered to make more informed and reliable routing decisions. However, some of these metrics might oppose each other. While the main forwarding strategy in geographic routing selects nodes closer to the destination to maximize distance progress, these nodes are most probably located at the border of the communication range where the probability of link breakage increases. Furthermore, the continuous selection of these nodes without considering their available bandwidth might result in higher packet delays and losses. novel routing protocol based[3] on fuzzy logic systems, which can help in coordinating and analyzing contradicting metrics. The routing protocol combines multiple metrics considering vehicles' position, direction, link quality, and achievable throughput to select the most suitable next-hop for packet forwarding.

D. CONNECTIVITY AWARE ROUTING IN VEHICULAR NETWORKS

With the high demand of mobile Internet services, Vehicular Ad hoc Networks (VANETs) become a promising technology to enable vehicular Internet access. However, the development of a reliable routing protocol to route data packets between vehicles and infrastructure gateways is still a challenging task due to the high mobility and frequent changes of the network topology. The conventional position-based routing (PBR) in VANETs can neither guarantee the existence of a routing path between the source and the destination prior to the transmission, nor provide connection duration information, which makes it unsuitable to route Internet packets. A novel infrastructure-based connectivity [4] aware routing protocol, iCAR - II, that enables multi-hop vehicular applications as well as mobile data offloading and Internet-based services. iCAR - II consists of a number of algorithms triggered and run by vehicles to predict local networks connectivity and update location servers with real-time network information, in order to construct a global network topology. By providing real-time connectivity awareness, iCAR-II improves the routing performance in VANETs by dynamically selecting routing paths with guaranteed connectivity and reduced delivery delay. Detailed analysis and simulation-based evaluations of iCAR-II demonstrate the validity of using VANETs for mobile data offloading and the significant improvement of VANETs performance in terms of packet delivery ratio and end to end delay.

III. SYSTEM METHODOLOGIES

VANETs is of the form of Vehicle-to-Vehicle communication (V2V) and Vehicle-to-Infrastructure (V2I) communication typically using Global Positioning System (GPS) to exchange messages with the RSU, and can be single-hop and/or multi-hop and broadcasting or multicasting.

Existing System:

Efficient routing in VANETs remains challenging for many reasons, e.g., the varying vehicle density over time, the size of VANETs (hundreds or thousands of vehicles), and wireless channel fading due to high motion and natural obstructions in urban environments (e.g., buildings, trees, and other vehicles). The routing protocols in VANETs can be classified into the following two major categories:

1) Topology-based routing.

2) Geographic (position-based) routing.

The common characteristic among all topology-based routing protocols is that the performance degrades as the network size increases, indicating the scalability problem.

The Geographic routing has several issues, which has inhibited its wide adoption—most important of which is that of location error. Location errors can severely degrade performance in location-based forwarding schemes, making accurate location information a necessity for most geographic routing protocols. In addition, geographic routing fails in the presence of void regions, where a closer neighbor vehicle toward the destination cannot be found.

Proposed System:

Figure 2 shows the architecture of the Proposed system.

PBAS, for vehicular is not resistant against false acceptance of batched invalid signatures sent by vehicles, and also it does not have message authentication which is the main requirement of authentication schemes for VANETs. Consequently, we show that it is not secure against impersonation and modification attacks.

Second, to tackle the aforementioned problems and have a more efficient scheme, a new identity-based authentication scheme using proxy vehicles, ID-MAP, without bilinear pairings is proposed.

Third, security analysis of ID-MAP is presented to show that it can satisfy security and privacy requirements of VANETs. In this direction, unforgeability of the underlying signature scheme against adaptively chosen-message and identity attack is proved under ECDLP in the random oracle model to guarantee resistance against modification and impersonation attacks.

Finally, its performance analysis including comparison of computation and communication overheads and simulation is presented to show that ID-MAP is more efficient than previous schemes for VANETs.

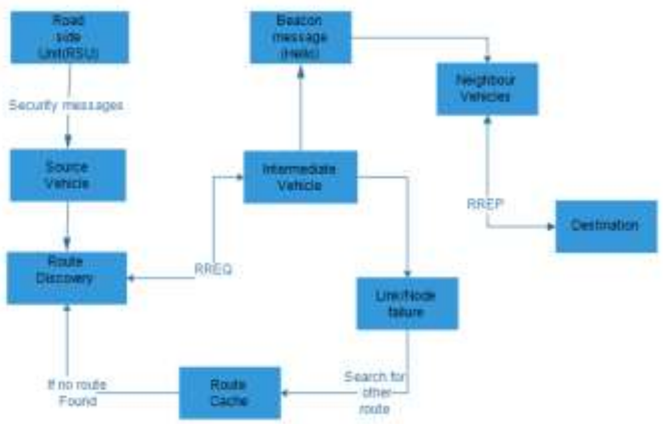

Figure 2 System Architecture

(a) Node Creation:

In a network, node is a connection point or an end point for data transmission. The first module involves the creation of nodes and road layout for simulation. The nodes and road layouts are created using the tool command language.

(b)Node-Node Routing:

The routing is the process of selecting best path in a network. This module implements the dynamic source routing (DSR) protocols for routing. It is designed specifically for use in multi-hop wireless ad hoc networks of mobile nodes. The protocol is composed of the two mechanisms of Route Discovery and Route Maintenance, which work together to allow nodes to discover and maintain source routes to destinations in the ad hoc network.

(c)Message Dissemination:

This module involves the dissemination of security messages to the nearby vehicles. The road side unit (RSU) is a computing device located on the road side that provides connectivity support to the passing vehicle. This can be effective in avoiding road accidents and traffic congestions.

(d)Simulation:

In this module, the vehicles are simulated based on the message received from the road side unit. The road side unit provides the information such as road information, traffic information and security messages.

Results:

Figure 3 Simulated Result

IV CONCLUSION

This paper is intended to provide a structured comprehensive overview of the recent advances on VANETS security, surveying the state-of-the-art on security vulnerabilities, threats and services, while focusing on important aspects that are not well-surveyed in the literature. VANET architecture and their security requirements were discussed. Then, more than 20 types of attacks of possible VANET attacks were addressed while emphasizing on their incentives. Moreover, multiple security mechanisms were discussed and the survey concluded with VANET simulation tool

REFERENCES

[1] S. K. Bhoi and P. M. Khilar, "Vehicular Communication - A Survey,"IET Networks, vol. 3, no. 3, pp. 204-217, 2014.

[2] S. Bitam, A. Mellouk and S. Zeadally, "VANET-Cloud: A Generic Cloud Computing Model for Vehicular Ad Hoc Networks," IEEE Wireless Communications, vol. 22, no. 1, pp. 96-102, February, 2015.

[3] T. W. Chim, S. M. Yiu, L. C. K. Hui and V. O. K. Li, "VSPN VANET BasedSecure and Privacy-Preserving Navigation," IEEE Trans. On Computers, vol. 63, no. 2, pp. 510-524, February, 2014.

[4] F. Wang, D. Zeng and L. Yang, "Smart Cars on Smart Roads: An IEEE Intelligent Transportation Systems Society Update," IEEE Pervasive Computing, vol. 5, no. 4, pp. 68-69, December, 2006.

[5] K. Mershad and H. Artail, "A Framework for Secure and Efficient DataAcquisition in Vehicular Ad Hoc Networks," IEEE Trans. on Vehicular Technology, vol. 62, no. 2, pp. 536-551, February, 2013.

[6] S. Woo, H. J. Jo and D. H. Lee, "A Practical Wireless Attack on the Connected Car and Security Protocol for In-Vehicle CAN," IEEE Trans. on Intelligent Transportation Systems, vol. 16, no. 2, pp. 993 -1006, 08 September 2014.

[7] J. Sun, C. Zhang, Y. Zhang and Y. Fang, "An Identity-Based Security System for User Privacy in Vehicular Ad Hoc Networks," IEEE Trans.on Parallel and Distributed Systems, vol. 21, no. 9, pp. 1227-1239, September, 2010.

[8] A. Wasef, R. Lu, X. Lin and X. Shen, "Complementing Public Key Infrastructure to Secure Vehicular Ad Hoc Networks," IEEE Wireless Communications, vol. 17, no. 5, pp. 22-28, October, 2010.

[9] S. K. Dhurandher, M. S. Obaidat, A. Jaiswal, A. Tiwari and A. Tyagi, "Vehicular Security Through Reputation and Plausibility Checks,"IEEE Systems Journal, vol. 8, no. 2, pp. 384-394, June, 2014.