ASSOCIATIVE RECEPTIVE SENSOR NETWORK ROUTING PROTOCOL FOR VANETs

Shushmita S, Adarsh Ojha, Sibi Amaran, Balachander T, Indhu G

SRM INSTITUTE OF SCIENCE AND TECHNOLOGY, CHENNAI

Abstract—The Vehicular Ad hoc Networks are a different type of ad hoc network, which contain communicating entities that are in motion with different velocity along with lacking in infrastructure. Hence, this work needs the establishment of more consistent end-to-end communicating pathways and efficiently transferring data. We have presented a new security-aware routing algorithm called Deep learning-based prediction. The presented scheme is more efficient and reliable against different kinds of attacks such as black hole and malicious node penetration attempts to the entire network. It basically depends upon route link error recover and shortest path by using Dijkstra’s algorithm. The aim of this scheme is to identify malicious data and black hole nodes. The simulation results of eDC-NC are compared with already existing techniques called COPE in terms of Energy consumption (EC), throughput and network lifetime (NLT). This helps to achieve better performance and filter unwanted data by applying deep learning filtering technique.

Keywords—Enhanced Distributed Coding and Network Coding (eDC-NC) Vehicular Ad hoc Network (VANET), COPE

1. INTRODUCTION

Vehicular Ad hoc Network (VANETs) is a concept of transmission of data between Vehicles. Many Scientists are working on this concept of Vehicular Ad Hoc Network to make it better and easy to transfer data. The transmission or transfer of data takes place between vehicle to vehicle while moving on road as they are not at constant place. They use the help of road side units for data transmission.

Communication between vehicles takes place using Wireless Sensor Network (WSN). Since the transmission is through WSN there is a threat of attackers to steal the data. As the Vehicles keeps on changing in a particular range there is a chance of attacker vehicle to come inside the range of network.

Several Research papers proposed various types of techniques in Wireless sensor network and VANET. But nowhere the precaution of the attacker vehicle has been mentioned and also there is high energy consumption is done while transferring data using COPE.

We proposed a scheme where there is minimal Energy consumption using eDC-NC technique that gives best performance and filters the data using deep learning filter. The attacker is known and prevented using deep learning-based detection methods. Route link error recovery and shortest path algorithm is used for black hole prevention. These techniques also improve traffic efficiency.

2. PREVIOUS WORK

Some researchers studied security challenges associated to VANETs. Here, we make a short study of current and relevant everything Nabeel I. Sulieman, Richard D. Gitlin had proposed Diversity and Modified Triangular Network Coding (eDC-NC) to enable very fast recovering from wireless link or node failure and offer low computational and energy cost which are very vital metrics for WSNs.

They applied eDC-NC coding to Wireless Sensor Network where both the direction wireless links are linked with the device node and the gateway nodes to everyone using the mesh topology. There is an uplink point-to-multipoint topology models in network. The distribution of the three data packets from the device node A1
to the two gateways Ga1 and Ga2. Thus it is presumed that the corresponding two gateways conveying in either active/stand-by (ACT/STBY) method to eradicate only facts of failure and thus to make certain the essential data is received from the device nodes which means that even if anyone gateway flops due to any cause, the received data will still reach the user.

Furthermore, not alone DC-NC coding improves several link/node failures eDC-NC coding in the WSN example network. Two in-between node/link failures like A2 and A3 can be abided mean while this links to the four immediate link/node failures where separately every pair is related with diverse destination node.

Likewise, if these are the only failures, when failures occur at S4 and S5, c3 and c4 only may be lost i.e. security of the network yet, positive data transfer can be reached. Here it is not necessary to simulate the results in this existing paper because the link failure is measured autonomously of the failure mode which statistically proves how eDC-NC improves and protects the WSN network. Certainly, the retrieval time is lesser limited by detection time of any failure. Thus intrusion of the attacker into the network can be prevented in the future.

3. PROPOSED WORK

A. Network simulator

In network simulator is a software which is used for testing the network components. This is a easy way to implement and through which it can be easily verified. This is a discreetworkingsimulator used in networks.

It provides support for Simulation of TCP, Routing. Enormous number of protocols reaching from wired to wireless networks, Provisions the addition of new entities like agent, packet, application, queue, protocol, routing, etc.

NS2 is not a refined or a finished product. In this errors/Bugs are being exposed and corrected. Network simulator architecture is said to consists of C++ (Internally), OTCL (User Interface) and anTclCL (Interface between C++ and OTCL). The simulation trace file of this consists of NAM(animation) and X-graph(plotting).

B. Diagrammatic Representation

![Diagram](image-url)

Fig.1: Attacker enters a VANET Network

C. Shortest Distance using Dijkstra’s Algorithm

Dijkstra’s algorithm, which was first created by the Dutch computer scientist Edsger Dijkstra in 1959 is used on weighted graph. Either directed graph or undirected graph can be applied. One
Thus we use two type of sets, one set has a list of vertices comprised in the shortest path tree, while the other set contains vertices that has not been involved in shortest path tree. At each step of this algorithm, we will find a vertex which is present in the other set (not included set) and has least distance from the source node.

**Dijkstra’s Algorithm- Example**

- Initialize an array lessweight in such a way lessweight[a]=weight[vertex,a]=0
- Now set the lessweight[vertex]=0
- Now find the vertex, a, which is closest to vertex for which the shortest way hasn’t been determined.
- Now mark a as the (immediate) vertex for which the less weight has been found.
- For each vertex b in M, the shortest way from the vertex to b has still not been found and an edge (a, b) exists, if weight of that path to b via a is less than its present weight, update the weight of b to weight of a + weight of the edge (a,b).

```
Algorithm 1: Dijkstra’s algorithm

Method Dijkstra (distance, initial node):
initialize node set K
for each vertex x in Graph: // Initial declaration
    distance[x] ← INFINITY // Unknown distance from source to x
    previous[x] ← UNDEFINED // Previous node in optimal path from source
    add x to K // All nodes initially in K (unvisited nodes)
    distance[source] ← 0 // Distance from source to source
while K is not empty:
y ← vertex in K with min distance[b] // with the least distance will be selected first
    Remove y from K
    for each neighbour of y: // where y is still in K.
        alt ← distance[y] + length(y, x)
        if alt<distance[x]: // A shorter path to v has been found
            distance[x] ← alt
            previous[x] ← y
return distance[], previous[]
```

Using this algorithm two shortest path are found between the source and destination.

**D. Algorithm for eDC-NC**

In order to check the availability of the nodes in the network, each node sends a beacon message. After receiving the vehicle status, it sends a RTS/CTS message to check the channel status. It then enters into the channel scheduling phase where each node is assigned with a time slot.

Channel selection is done based on two main factors, one is the
shortest distance, the other one is the node with energy greater than the threshold energy. Packets are then arranged based on the priority. Transmission begins with the congestion avoidance. Every node is authenticated before sending the packet. This authentication process takes place by verifying the id and password. The attacker node however will have a different id and password. Using eDC-NC technique this is avoided.

There maybe even some disturbance after eDC-NC technique, thus we have included the machine learning technique which involves deep learning and filtering process. This enhances the throughput thus preventing the attacker into the network.

**Algorithm 2: eDC-NC**

| Step   | Description                                                                 |
|--------|-----------------------------------------------------------------------------|
| Step:1 | Each vehicle sends a beacon message for checking the vehicle status.         |
| Step:2 | Vehicle status defines whether the vehicle is sleep vehicle or wake up vehicle (nid). nid->neighbor id |
| Step:3 | It sends the RTS/CTS message for getting the channel status.                |
| Step:4 | After it forms the frame in terms of bandwidth and slot time TX.            |
| Step:5 | Maximum allowed queue process to be utilized at every transmission slots at T-sec. T-sec->Transmission seconds |
| Step:6 | Tr->propagation variance of delay when transmitter receiver distance is rx.  |
|        | Tri->Transmission rate of the node                                          |
|        | rxi->reception rate of the node                                             |
| Step:7 | Probability of delivered rate of new entity in (nb) access slots.           |
|        | nb->neighbor vehicle                                                        |
| Step:8 | Then it enters the channel scheduling for assign the channel to communicate. |
| Step:9 | Channel scanning is done by number of neighbor selection.                   |
| Step:10| Attacker reroute the packet by twisting the path.                          |
| Step:11| Energy level is beyond a specified threshold time schedule of helper is not affected. |
| Step:12| Receiver vehicle have higher than transmitter vehicle then co-operative transmission will be applied. |
| Step:13| Packets are assigned into priority level.                                   |
| Step:14| Packet transmission begins with congestion avoidance.                      |
| Step:15| Each vehicle should be testified by the security level and filter the process in the network. |
| Step:16| Data should be collected by the neighbor vehicle and cooperate transmission takes place. |
| Step:17| Packet balancer classify the vehicle based upon the load.                  |
| Step:18| Then the load should be categorized as heavy, medium, low.                  |

E. Block Diagram

In this proposed work, individual vehicle’s GPS and the distance optimization is verified. Each individual vehicle in every network can do both communicate and receive data packets. Neighbor selection is done mainly based on two main criteria. One of which is triangular coding which verifies for any network failure thus improving the network reliability.
Other one is the energy assumption which orders for the ideal energy, then minds and communicates energy which is based on which neighbor node for transmission is selected.

F. Flow chart

G. RESULTS

(a) Simulation_Time Vs Throughput
Throughput has been considerably increased when compared to the existing system as data is transmitted without any intervention of attackers.

Energy consumed by the nodes is reduced by 20% when compared to the existing system.

In the existing system, Network lifetime increases slightly when compared to the proposed system.

**4. CONCLUSION**

Hence in this paper we have proposed and eDC-NC deep learning with filtering mechanism. The results of our proposed technique will ensure less packet loss without the intrusion of Attackers. Energy consumption, throughput, Network Lifetime will be calculated and outputs will be shown.
using graphs. The Performance will be analyzed based on these parameters using mathematical and simulation means.

5. REFERENCES

[1] Wasantwaej, Muhammad khan,” network performance evaluation of M2M with self organizing cluster head to sink mapping”, IEEE seniors journal, vol 17, no 15, 2017.

[2] Nabeel , Sulieman, Richard D. Gitlin,” Ultra-reliable and energy efficient wireless sensor networks”, IEEE 19th Wireless and Microwave Technology Conference (WAMICON), 2018

[3] Jesisha Jayarajan, Sapna Prabhu,” Comparison of Energy Minimization Techniques in Wireless Sensor Network”, Comparison of Energy Minimization Techniques in Wireless Sensor Network, 2016.

[4] Gurudattulkulkaran, Rupali shelek, Prasad Khatwakar “wireless sensor network security threats”, IET.

[5] E. Ayanoglu, C.-L. I, R. D. Gitlin, and J. E. Mazo, “Diversity Coding for transparent self-healing and fault-tolerant communication networks,” IEEE Trans. Commun., vol. 41, pp. 1677–1686, Nov. 1993.

[6] J. Qureshi, C. H. Foh, and J. Cai, "Optimal solution for the Index Coding problem using Network Coding over GF(2)," IEEE Communications Society Conference on Sensor, Mesh and Ad Hoc Communications and Networks (SECON), Seoul, South Korea, June 2012.

[7] G. E. Arrobo and R. D. Gitlin, "Minimizing energy consumption for cooperative Network and Diversity coded sensor networks," IEEE Wireless Telecommunication Symposium, Washington, D.C., April 2014.

[8] N. Sulieman, K. Davaslioglu, and R. D. Gitlin, “Link failure recovery via Diversity Coding in 5G fronthaul wireless networks,” IEEE Wireless and Microwave Technology Conference, Cocoa Beach, FL, April 2017.

[9] N. Sulieman, K. Davaslioglu, and R. D. Gitlin, “Diversity coded 5G fronthaul wireless networks,” IEEE Wireless Telecommunication Symposium, Chicago, IL, April 2017.

[10] J. Qureshi, C. H. Foh, and J. Cai, "Optimal solution for the Index Coding problem using Network Coding over GF(2)," IEEE Communications Society Conference on Sensor, Mesh and Ad Hoc Communications and Networks (SECON), Seoul, South Korea, June 2012.

[11] R. Ahlswede, N. Cai, S.-Y. R. Li, and R. W. Yeung, “Network information flow,” IEEE Trans. Inform. Theory, vol. 46, no. 4, pp. 1204–1216, July 2000.

[12] N. I. Sulieman, E. Balevi, K. Davaslioglu, and R. D. Gitlin, “Diversity and Network coded 5G fronthaul wireless networks for ultra reliable and low latency communications,” IEEE International Symposium on Personal, Indoor and Mobile Radio Communications, Montreal, QC, Canada, Oct. 2017.

[13] N. Sulieman, E. Balevi, and R. D. Gitlin, “Near-instant link failure recovery in 5G wireless Fog-base-fronthaul networks,” IEEE Wireless Telecommunication Symposium, Phoenix, AZ, April 2018, in press.