**Indonesian Journal of Electrical Engineering and Computer Science**
Vol. 9, No. 1, January 2018, pp. 111~114
ISSN: 2502-4752, DOI: 10.11591/ijeecs.v9.i1.pp111-114


# Data Spread among Vehicular Networks with Minimal Cost and Privacy

**Atul Kulkarni[1], Dr. Debajyoti Mukhopadhyay[2]**
[1]Research scholar, Information Technology, AMET University, Chennai
[2]Department of Computer Science, Maharashtra Institute of Technology, Chennai

**Article Info**

***Article history:***

Received Jul 7, 2017
Revised Nov 28, 2017
Accepted Dec 17, 2017

***Keywords:***

Global positioning system
Migration cost
Shortest path
VAN router

**ABSTRACT**

Currently, choosing a node to carry the files via network is inefficient due to multiple end-users are requesting for packets at the same time. The problem is to identify the shortest path, traffic cost is high, and hackers enter the network to access the file. Whenever user requesting for packets to service provider, it has been carried out via router to provide security and effective way of transmission without any hackers. We proposed a VAN router that manages the transmission process. Once the packet enters router follows: (i) identifies the shortest path to transmit the packets, (ii) analyze the migration cost, (iii) when a hacker enters the network, the details of the hacker is send to the GPS to identify hackers location, (iv) provides the user requested packets back to the user without any modification. GPS work is to identify the hacker location in which node they are trying to access the files and that information has been sent to the user where hacker enters the network. Each packet sent by the service provider via router to end-user, the router intimates service provider with a confirmation message. Finally, VAN router provides security to the end-user by avoiding hackers to access the file and minimizes traffic cost, finds shortest path.



***Corresponding Author:***

Atul Kulkarni,
Research scholar, Information Technology,
AMET University, Chennai

## 1. INTRODUCTION

In environment, different way of transportation evolves to satisfy people to travel one place to other with variety of choice. Some cases, malfunction of vehicles leads disappearance from the current route [1]. Drones are developed for search and rescue mission where the man couldn't step on fields, the drone can easily fly over there and capture surrounding and sends that to the base station [2].

Between the diffusion, connection is important to spread data from one area to other without any interference and data loss. At the same time privacy need to be a vital role where no other users should interfere and modify[3]. Those data packets sent from thedrones are forwarded to base station where the service providers send those to the end users with the help of routers [4-5].

Most of them lead data to a shortest base station to reduce time delay and cost wise of network where congestion is more due to increase of packets on the same channel with Underwater vehicle for surveillance with navigation and swarm network communication [6]. Even though we all solve this issue of data interference, the attacker may interfere and convert those into malicious which interacts false information among end users. Privacy proceedings are major issue to securely spread data on router with protocols that manages attackers on way and forward it to the routers to change the path of data diffusion of Enhancement of fuel consumption and efficiency of the vehicles, International Journal of Mechanical Engineering and Technology [7]. To increase the accuracy of forecast data at the base station is the main approach; therefore coding schemes based relative difference was proposed [8].

## 2. PROPOSED WORK

In proposed work, implementation of VAN router increase efficiency of data spread from one city to other with the help of service provider as well as logger where the malicious user enters the premises as shown in figure 1.

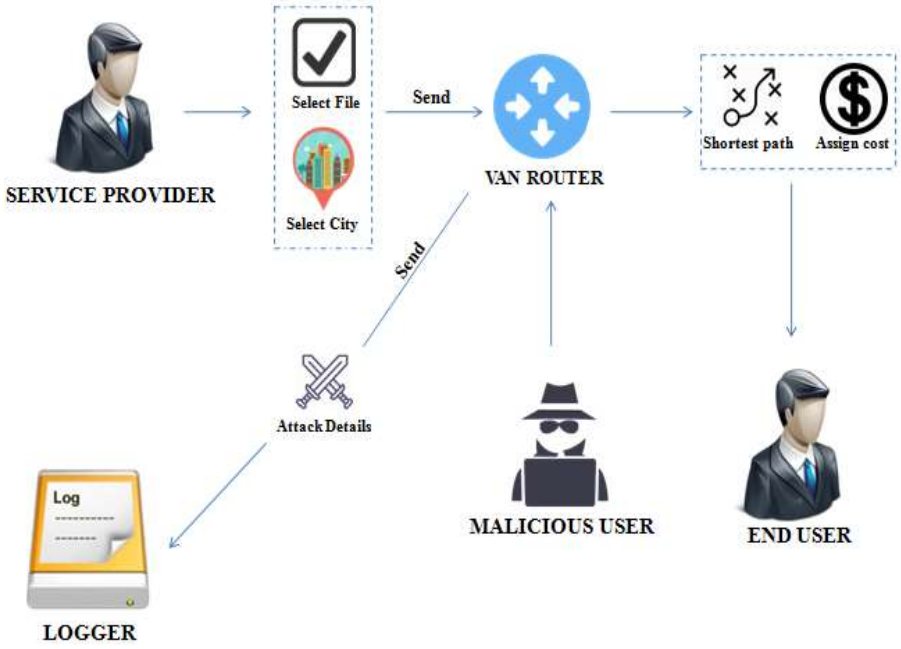


Figure 1. Architecture of Proposed Work

### 2.1. Service Provider

Service providers receive data packets from the drone and via base station. They choose the file need to be transmit and select city where the file to be forwarded. Assign router path where the service provider need to enter the router address of the end user to prevent data from un-authorized users.

### 2.2. Van Router

VAN router plays a vital role in this method, where it assigns the cost for the path and finds shortest path to forward the packets without any data loss. Here, we implemented honeypots to analyze the tricks of the malicious user from which node, they trying to attack. Finally, the details of the attacker is analyzed and sent to logger where it checks the node details and swap the path from the attacked node.

### 2.3. Malicious User

Malicious user enters the network and attack the node which carries data packets and modifies it without any knowledge to both the service provider and router.

### 2.4. Logger

Logger is a kind of tracking device which checks the entry of malicious user on the attacking node and intimates it back to the router to change the path of data spread. Here, the service provider can check the details of the attacker on what time on which node they tried to attack. It will be useful to further update of protocols to securely carry data packets from one station to other city without any data loss.

### 2.5. End User

End user have only one option where they can receive file, view files and store it on a location which is convenient for them. Intimation is send back to the service provider that they got the packets and received successfully.

## 3. RESULT AND DISCUSSION

Figure 2 & 3 shows the result of our proposed system concludes the efficiency of data spread via VAN router reduced time delay and data loss of packets during data diffusion through Service provider select city and end user router address and attacker process.

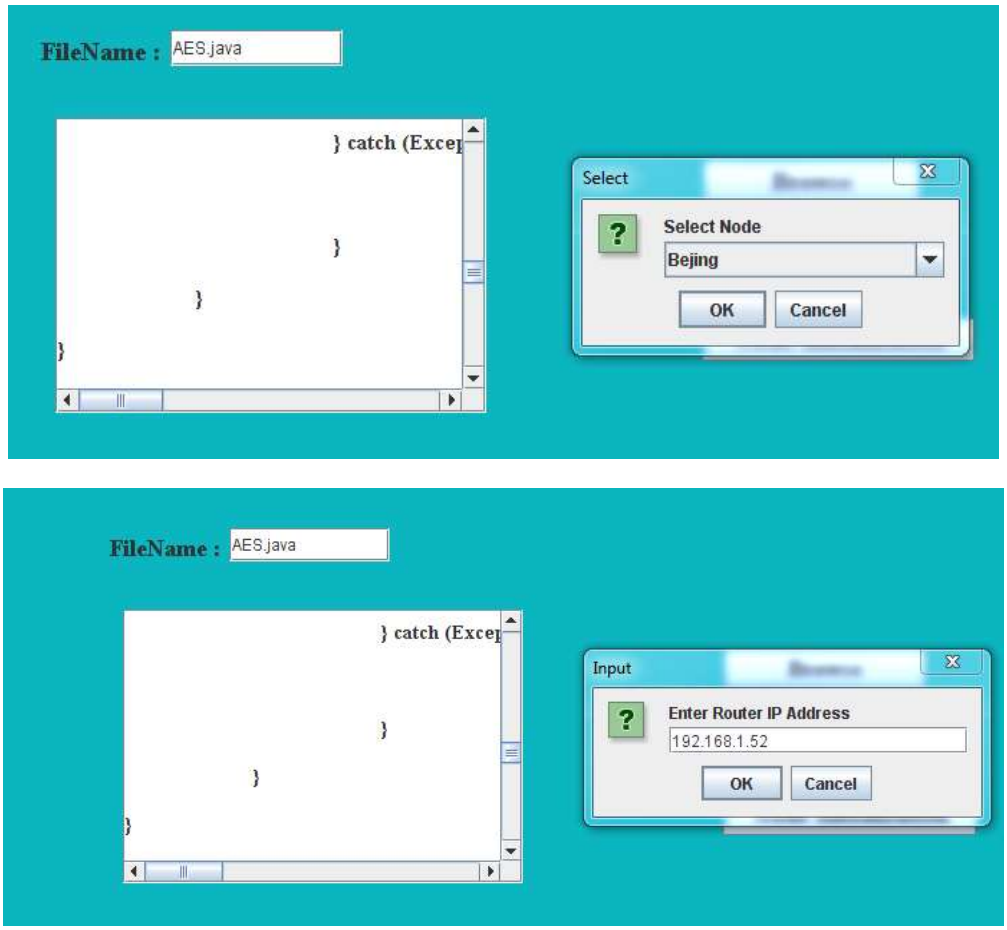


Figure 2. Service Provider Select City and End User Router Address


Figure 3. Attacker Process

## 4. CONCLUSION

Hereby, our proposed system concludes the efficiency of data spread via VAN router reduced time delay and data loss of packets during data diffusion. Interference of data packets is avoided with the help of honeypots discovering malicious users while diffusion as well logger helps to identify on which node the data has been attacked. The method of logger improvises privacy among data.

## REFERENCES

[1] Van den Bergh B, Vermeulen T, Pollin S. (, May). Analysis of Harmful Interference to and from Aerial IEEE 802.11 Systems. In *Proceedings of the First Workshop on Micro Aerial Vehicle Networks, Systems, and Applications for Civilian Use*. ACM. 2015: 15-19.

[2] Asadpour M, Van den Bergh B, Giustiniano D, Hummel K, Pollin S, Plattner B. Micro aerial vehicle networks: An experimental analysis of challenges and opportunities. *IEEE Communications Magazine*. 2014; 52(7): 141-149.

[3] Andre T, Hummel K A, Schoellig A P, Yanmaz E, Asadpour M, Bettstetter C, Zhang S. Application-driven design of aerial communication networks. *IEEE Communications Magazine*. 2014; 52(5): 129-137.

[4] Won M, Stoleru R, Chenji H, Zhang W. On *optimal connectivity restoration in segmented sensor networks*. In European Conference on Wireless Sensor Networks. Springer, Berlin, Heidelberg. 2013: 131-148.

[5] Muzaffar R, Yanmaz E. *Trajectory-aware ad hoc routing protocol for micro aerial vehicle networks*. 2014

[6] Karthik S. Underwater vehicle for surveillance with navigation and swarm network communication. *Indian Journal of Science and Technology*, 2014; 7(S6): 22-31.

[7] Elavarasi R, Senthil Kumar P K. Enhancement of fuel consumption and efficiency of the vehicles. *International Journal of Mechanical Engineering and Technology*. 2017; 8(4): 456-460.

[8] N. A. M. Alduais, J. Abdullah, A. Jamil. Enhanced Payload Data Reduction Approach for Cluster Head (CH) Nodes, *TELKOMNIKA Telecommunication, Computing, Electronics and Control*, 15(3), 2017.