A Secure and Efficient System for Ambulance Vehicular Social Network Based on Re-Fragmentation and Swarm

Tianhan Gao* and Marwan Kadhim Mohammed Al-shammari
Software College, Northeastern University, Shenyang, China
gaoth@mail.neu.edu.cn, alkaseralshamary@gmail.com

Abstract

Efficient and secure treatment for the patient is associated with many health risks, including patient's life. The purpose of this study is to investigate the relationship between Vehicular Social Network (VSN) and ambulance system. A new secure and efficient system for ambulance vehicular social network is proposed in this paper. The security scheme based on Re-Fragment mechanism is suggested to secure the communication between ambulance and hospital. Moreover, the intelligence swarm approach is introduced to improve network efficiency. According to the performance analysis, the proposed system is able to find the best network node by using ant colony swarm intelligence. Furthermore, the system provides a secure session between ambulance and hospital.

Keywords: VSN, WMN, SWARM, Re-Fragmentation

1 Introduction

The rapid and secure arrival for the patient to the nearest hospital is most important priorities and principles in the medical field. Therefore, the modern medical harnesses the telemedicine and Internet of Vehicles (IOV) to achieve maximum benefit from these technologies. Year by year, the vehicular social network (VSN) technology has emerged as an ideal solution for ambulances to reduce the rapid increase of the road accidents and traffic congestions which obstacle the safe and effective arrival for ambulances. VSN is the combination of Vehicular Ad-Hoc Network (VANET) and social network, where each ambulance driver can share data with hospitals and other ambulances quickly and efficiently [13]. However, there are still many challenges raised by the society, especially in the issues of privacy and security. It is possible that the leak of the identity of the paramedic comes up with risk for the life of patients, who may be an influent person [6]. From the above, the problem can be defined as a mixture of two essential parts. The first part represents achieving the fastest arrival of the ambulance to the nearest hospital. The second part focuses on privacy and security issues of the ambulance driver while contacting with the nearest hospital [11].

A group of studies contributed to solve the problem adopted an urban planner with the aid of estimating the arrange of bus fraction and random arrival-time [8]. Other studies relied on the effective location of ambulances and suggested an effective spatial coverage model [3]. Tabu Model, was a suggested solution to solve the problem of the optimal time for ambulances [4]. An ambulance application was also introduced to achieve social trust [7]. And swarm techniques were adopted to speed up the transmission of data on the cloud network [14]. Utilizing VSN to send initial health record about the patient's status before reaching hospital was also proposed [10].

The purpose of this paper is to find out and elaborate on various challenges associated with the development of ambulance. A wireless mesh network with related middleware has been suggested to address those challenges. The proposed system is composed of three phases. The first phase employs a wireless

IT CoNvergence PRActice (INPRA), volume: 6, number: 3 (September 2018), pp. 1-8
*Corresponding author: NO. 3-11, Wenhua Road, Heping District, Shenyang, P. R. China, Tel: +86-24-83678115

mesh network, equivalent to a VSN network, and divides it into Virtual Local Area Networks (VLANs) where each LAN represents an independent wireless network. The second phase is the preparation of Middleware, which manages this network and calculates the nearest point-to-point convenient access point by using an appropriate theory. Thirdly, we implement this Middleware to send the identity number (ID) of the ambulance driver in encrypted form to ensure the privacy issue. In addition, the ant colony theory, one of the SWARM theories, has been suggested as an appropriate hypothesis for rapid access to the network. In terms of security, Re-Fragment of different sequence in the Network Layer has been chosen as a suitable authentication approach.
The rest part of the paper is organized as below. Basic knowledge about the proposed system is summarized in section 2. The proposed system is elaborated in section 3 and section 4. The performance analysis of the system is given in section 5. Finally, the paper is concluded in section 6.

2 Preliminaries

2.1 VSN services based on WMNs

Wireless mesh networks (WMNs) have emerged as a core technology for the next-generation wireless Ad-Hoc networks. WMNs are undergoing rapid progress and inspiring numerous applications, e.g. VSN in Telemedicine field [1].
WMNs are defined as interactive wireless networks consisting of several mobile access points (APs) that are controlled simultaneously through the access controller (AC). WMNs can be integrated with minimal mobility networks to achieve an incorporated network. WMNs are the backbone for the improvement of Ad-Hoc networks where VSN services can be achieved [2].

2.2 SWARM and Ant Colony

SWARM Intelligence is an approach aimed to use the behavior of a swarm of animals as a theory to improve the efficiency of a certain system [9]. The ant colony is one of these theories that employ the intelligence of the swarm in the area of networks. The theory summarizes the ants' strategy of reaching food in less time. As a result, the network that adopts this approach is able to deliver information as soon as possible. The ant colony theory is convenient for flexible networks since such networks have no infrastructure or centralized management. Ad-Hoc networks are therefore suitable for this temporary network connectivity [5].

2.3 Re-Fragmentation

Re-Fragmentation is one of the Networks security mechanism employed to protect the integrity and usability of data access in a specific network. This kind of protection is designed to change the sequence of standard fragments. Effective Re-Fragmentation can against a variety of threats and prevent the intruders from receiving true information. Re-Fragmentation combines two layers of TCP/IP network protocol at the edge of each access point in the network, Transport and Network layers. The two layers carry out policies and controls to authorized users with true fragments sequence while blocks the malicious actors. In addition, to keep out potential attackers from attacking the network, each terminal device of the user must have an identity id and block the noncompliant identity. Wireless networks are not as secure as wired ones without stringent security measures. Changing the sequence of the fragments in the Network layer of TCP/IP protocol is one of the powerful strategies to protect the wireless networks [12].

3 The Proposed System

The main objective of the system is to propose a fast and safe access to the nearest hospital in the region of the ambulance and to take the advantage of VSN technology. As shown in Figure1, the system is divided into two interactive networks. The ambulance is equipped with the middleware, which sends test packets to the surround hospitals and calculates the throughput. Then, the middleware calculates the fastest respond and decides the nearest hospital to assist the patient. This strategy is called SWARM to improve network traffic efficiency. In order to ensure privacy between the ambulance driver and the hospital, the middleware sends the ID of the ambulance driver, which includes four samples that are protected by the Re-Fragmentation mechanism. The fragments are sent in a pre-agreed sequence between hospitals and ambulances, which are different from the standard sequence. Thus, the ambulance will be able to locate the nearest hospital without the driver's identity being detected.

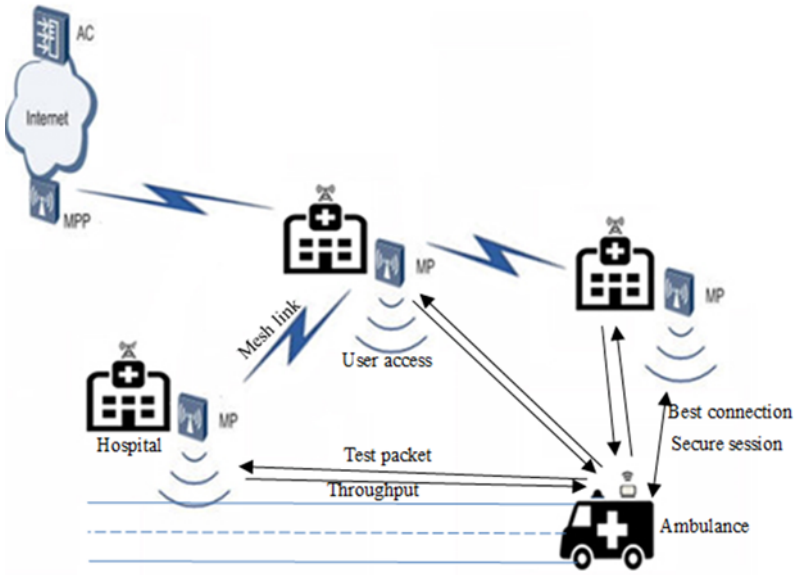

Figure 1: Overall Ambulance Vehicular Social System based on WMN with SWARM

3.1 Network architecture

The nodes in WMN can be categorized into the following categories based on the nodes' functionality. MP is mesh point equipped with IEEE802.11 physical layer protocol in the wireless network. MP is capable of automatic route discovery and packet forwarding. MPP is mesh portal point connected with WMN or other types of networks. MPP enables mesh nodes to communicate with external networks. AC is access controller to ensure uninterrupted packet forwarding and high reliability. STA represent any station can connect with the mesh network. As shown in figure 2, the WMN consist from four MPs to provide access to the three wireless STA, One MPP to provide connection to the Internet and One AC to establish high bandwidth and highly-stable Internet connection.

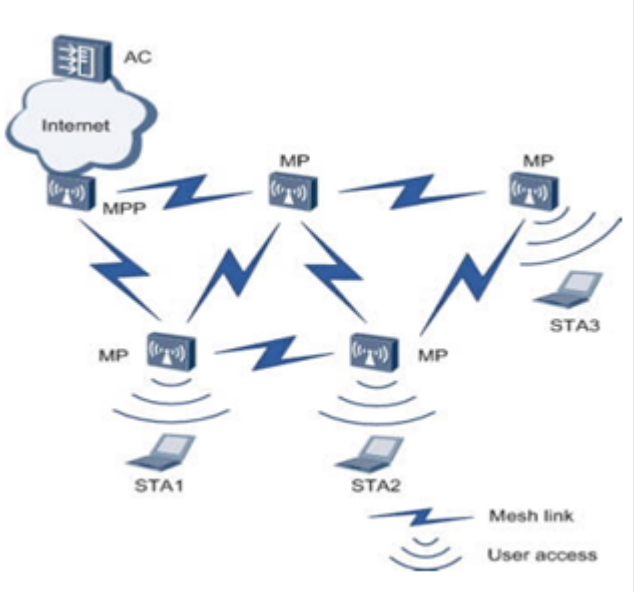

Figure 2: Network architecture.

3.2 Packets transmission with SWARM

The proposed system borrows the theory of Ant Colony, one of the SWARM theories. This theory is applied in the client middleware. Before presenting the subroutine implementation, the mechanism of this theory should be explained. The Ant Colony theory is a colony that sends the ants in all directions to get food. After the ants return, the colony calculates the least time for each ant back with food then redirects all the ants in the colony to this shortest path. To achieve this process, ants use a specific chemical liquid at different concentrations. Similar as the ant colony, the proposed system adopts throughput rather than chemical liquid as a gauge to find the best route in the network.
First, the system sends a signal in all directions then calculates the lowest throughput. Depending on the throughput, the system estimates the packets receiving time and chooses the shortest path for ambulances. Then the system redirects the entire packets to the lowest throughput path between the ambulance and the chosen hospital.

3.3 Network security based on Re-Fragmentation

The maximum transmission unit (MTU) is the maximum limits of the packet and cannot be exceeded during transmission. On this basis, the packet is divided into segments. The segments are assembled at the other end. Each segment needs its own index to be arranged according to an agreed context between the sender and the recipient so that the information is reorganized correctly. The segment and its ID are called fragment. The sending of the fragments and their receipt at the other end is called fragmentation. Figure 3 shows the sequence of fragments under TCP/IP for nodes. There are special libraries to change

this sequence between sender and receiver through Re-Fragmentation. It could also employ encryption methods to improve security.

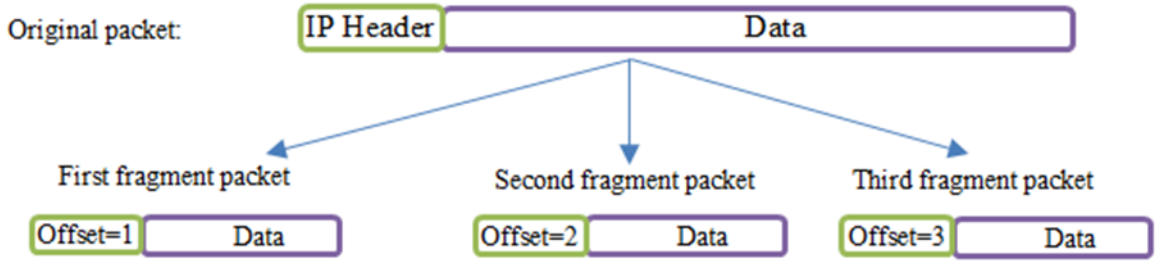

Figure 3: IP packet fragmentation in the network hidden layer in Vehicular Social Network.

4 Implementation

As shown in Figure 4, the system consists of three wireless routers (Huawei AP6010DN-AGN), one Access controller (Huawei AC6605), and a middleware. The middleware is written by Python that manages the network. The middleware is made up of two integrated parts. The client is embedded into ambulances and the server resides in hospitals. The access controller manages overall mesh network. The nodes information in WMN updates every 30 seconds. AP1 (China1) connects WMN and sends the control network messages of VLANs from the access controller. AP2 (China2) and AP3 (China3) provide access service for the terminals in the WMN. In the end, China2 and China3 are placed in hospitals and provided with a server middleware. While the client middleware is embedded into ambulances within Ad-Hoc network. The access controller and access points are configured using CTL as shown in table 1. About programming, the middleware first configures the connection session (software port number and IP) by socket() library commands (socket(AF INET, SOCK STREAM), conn.bind(), conn.listen(), conn.send() and conn.recv()). Then, the middleware sends a test packet for both China2 and China3 networks. Finally, the middleware calculates the throughput for each network through the commands in (OS, SYS and Time) libraries. Depending on the better throughput, the middleware determines which network is suitable for communication and which hospital is closer to treat the patient. The results are shown in Figure 5.
In the proposed system, Re-Fragmentation is carried out in accordance with a special agreement between the client-middleware and server-middleware in order to protect the identity privacy of the ambulance driver. This function is programmed using the Scapy() library and the results are shown in Figure 6.

Table 1: Configuration of the mesh network.

Device	Type	My Net	Radio	Configuration
AP1	AP6010DN	192.168.1.1/24	China1	Channel 40mhz-plus 157
AP2	AP6010DN	192.168.2.1/24	China2	Ap-region 102,102,103
AP3	AP6010DN	192.168.3.1/24	China3	Forward mode
AC	AC6605	Vlan 100	mesh1	p/w: 12345678

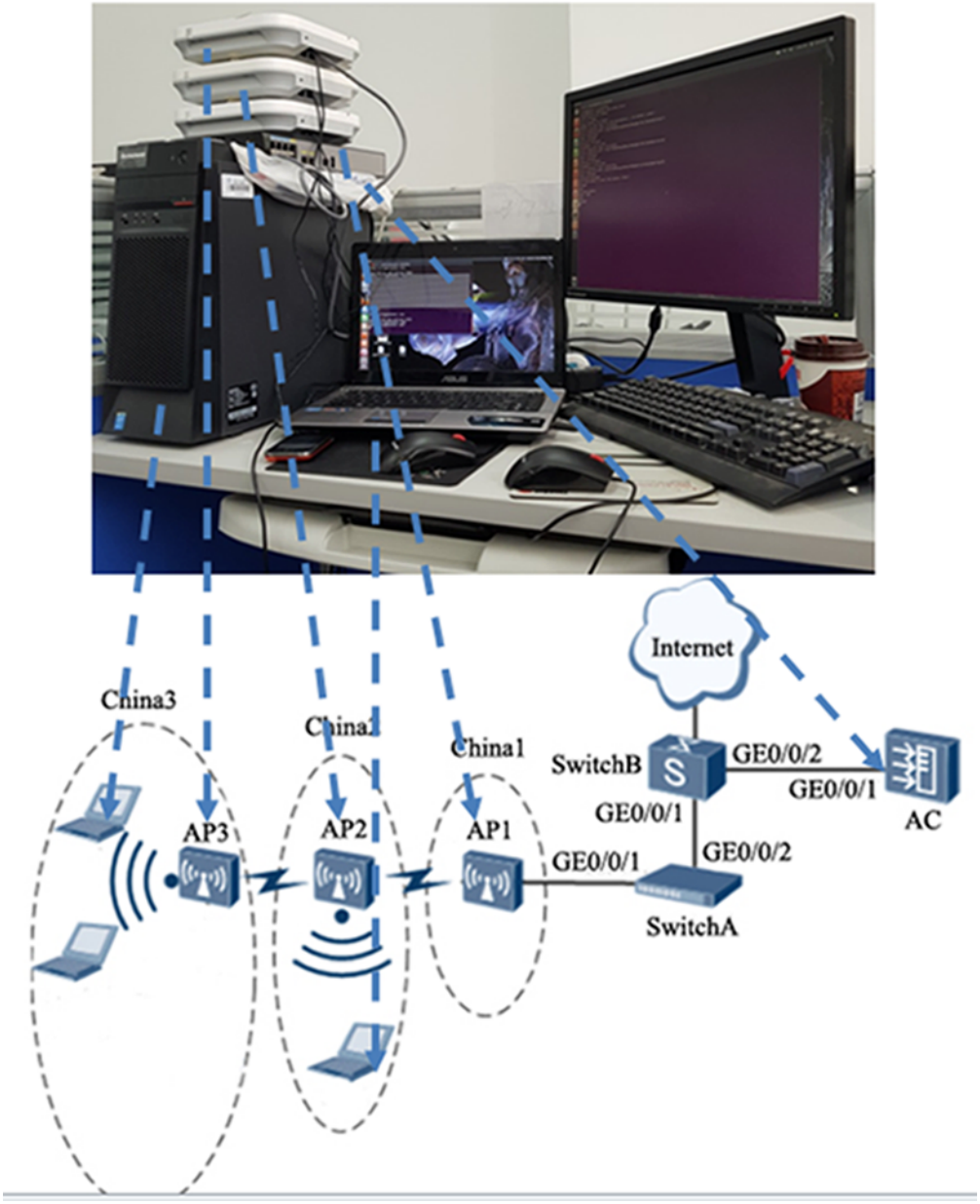

Figure 4: Components and configuration of the system.

```
Throughput1: 332.899 k/sec.                    calculate throughput for two networks
Throughput2: 1580.717 k/sec.
Best VLAN network to start the surgery: china 2 decide that china2 network is good to send
massage:
abcd        send message
following packet:
[<IP  flags=MF frag=0 |<Raw  load='a' |>>, <IP  flags=MF frag=3 |<Raw  load='b'
|>>, <IP  flags=MF frag=1 |<Raw  load='c' |>>, <IP  flags=MF frag=2 |<Raw  load=
```

Figure 5: Sending and receiving test packet to choose suitable network.

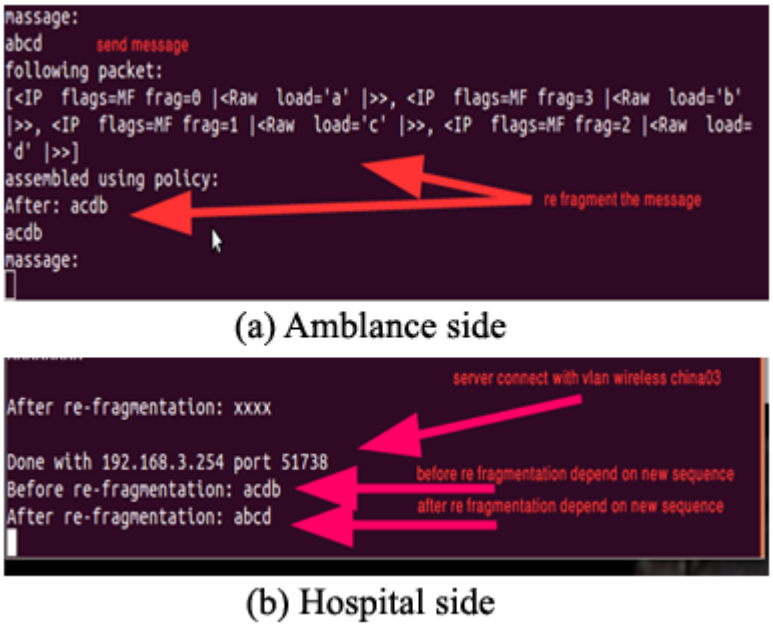

Figure 6: Re-Fragmentation results between hospital and ambulance.

5 Conclusion

Due to the need for a secure and efficient system for the ambulance VSN, this paper suggests that efficiency and security are important for patient. To achieve these requirements, SWARM and Re-Fragmentation approaches are introduced. SWARM allows exploring the fast packet forwarding while Re-Fragmentation secures the network session between ambulance and hospital. Simulations and performance analysis.

References

[1] I. Akyildiz and X. Wang. A survey on wireless mesh networks. *IEEE Communications magazine*, 43(9):S23–S30, September 2005.

[2] I. Akyildiz, X. Wang, and W. Wang. Wireless mesh networks: a survey. *Computer networks*, 47(4):445–487, March 2005.

[3] G. Berlin and J. Liebman. Mathematical analysis of emergency ambulance location. *Socio-Economic Planning Sciences*, 8(6):323–328, December 1974.

[4] M. Gendreau, G. Laporte, and F. Semet. Solving an ambulance location model by tabu search. *Location science*, 5(2):75–88, August 1997.

[5] M. Gunes, U. Sorges, and I. Bouazizi. Ara-the ant-colony based routing algorithm for manets, August 2002.

[6] D. Huang, X. Hong, and M. Gerla. Situation-aware trust architecture for vehicular networks. *IEEE Communications Magazine*, 48(11):128–135, November 2010.

[7] R. Hussain, W. Nawaz, J. Lee, J. Son, and J. Seo. A hybrid trust management framework for vehicular social networks. In *Proc. of the 2016 International Conference on Computational Social Networks (CSoNet'16), Ho Chi Minh City, Vietnam*, volume 9795 of *Lecture Notes in Computer Science*, pages 214–225. Springer, Cham, August 2016.

[8] A. Ingolfsson, S. Budge, and E. Erkut. Optimal ambulance location with random delays and travel times. *Health Care management science*, 11(3):262–274, September 2008.

[9] D. Karaboga and B. Akay. A survey: algorithms simulating bee swarm intelligence. *Artificial intelligence review*, 31(1):61, October 2009.

[10] J. Lee, S. Moon, and J. Park. A secure service framework for optimizing driver's health status. *Advanced Science Letters*, 22(9):2438–2443, September 2016.

[11] Z. Ning, F. Xia, N. Ullah, X. Kong, and X. Hu. Vehicular social networks: Enabling smart mobility. *IEEE Communications Magazine*, 55(5):16–55, May 2017.

[12] A. Shamir. Identity-based cryptosystems and signature schemes, November 1984.

[13] A. Vegni and V. Loscri. A survey on vehicular social networks. *IEEE Communications Surveys & Tutorials*, 17(4):2397–2419, July 2015.

[14] Y. Zhang, F. Tian, B. Song, and X. Du. Social vehicle swarms: A novel perspective on socially aware vehicular communication architecture. *IEEE Wireless Communications*, 23(4):82–89, August 2016.

Author Biography

Tianhan Gao received the BE in Computer Science & Technology, the ME and the PhD in Computer Application Technology, from Northeastern University, China, in 1999, 2001, 2006, respectively. He joined Northeastern University in April 2006 as a lecture of Software College. He obtained a promotion to a professor in June 2017. He has been a visiting scholar at department of Computer Science, Purdue, from February 2011 to February 2012. He obtained the doctoral tutor qualification in 2016. He is the author or co-author of more than 50 research publications. His primary research interests are next generation network security, wireless mesh network security, security and privacy in ubiquitous computing, as well as virtual reality.

Marwan Kadhim Mohammed Al-shammari was born in Iraq in 1977, PhD student, in Northeastern University. He received the B.S. in Computer Engineering from Baghdad University, Iraq in 2000, the M.S. in Computer Engineering from UTeM University, Malaysia, in 2014, CISCO American institute instructor from 2007. He joined Baghdad University in 2006 as a lecturer of Department of computer engineering. He was director for research & developing division and training & continues learning division respectively. He was Core member in advisory office of Baghdad University. He has been a team leader at South Korean and Canada with Coicka and ED companies respectively. He is team leader for many projects in the field of Java, Dot.net, visuals, IOS, OS, CG, Media, Networking, DB, Embedded Systems, Embedded Software, VR, EEG, Robotic surgery, Networking. 2 papers published.