ISSN 2394-3777 (Print)
ISSN 2394-3785 (Online)
Available online at www.ijartet.com
International Journal of Advanced Research Trends in Engineering and Technology (IJARTET)
Vol. 3, Special Issue 24, April 2016

Improving for Internet access for moving Vehicles communication using NLOS in VANET

Punitha.D[1] Rajeswari.V[2] Saradha.S[3] Arun kumar.S[4]
Student, ECE, Jairupaa College Of Engineering,Tirupur,India[1,2,3]
Assistant Professor, ECE, Jairupaa College Of Engineering,Tirupur,India[4]

ABSTRACT

Network services and applications (e.g., safety messages) require an exchange of vehicle and event location information. The data are exchanged among vehicles within each vehicle's respective radio communication range through direct communication. In reality, direct communication is susceptible to interference and blocked by physical obstacles, which prevent the proper exchange of information about localization information. Demand for Internet access from moving vehicles has been rapidly growing. Meanwhile, the overloading issue of cellular networks is escalating due to mobile data explosion. Thus, WiFi networks are considered as a promising technology to offload cellular networks. However, there pose many challenging problems in highly dynamic vehicular environments for WiFi networks. For example, connections can be easily disrupted by frequent handoffs between access points (APs). A scheme, called SWIMMING, is proposed to support seamless and efficient WiFi-based Internet access for moving vehicles. In uplink, SWIMMING operates in a "group unicast" manner. All APs are configured with the same MAC and IP addresses, so that packets sent from a client can be received by multiple APs within its transmission range. Unlike broadcast or monitor mode, group unicast exploits the diversity of multiple APs, while keeping all the advantages of unicast. To avoid possible collisions of ACKs from different APs, the conventional ACK decoding mechanism is enhanced with an ACK detection function. In downlink, a packet destined for a client is first pushed to a group of APs through multicast. Obstacles can create a state of nonline of sight (NLOS) between two vehicles, which restricts direct communication even when corresponding vehicles exist within each other's physical communication range, thus preventing them from exchanging proper data and affecting the localization services' integrity and reliability. This AP group is maintained dynamically to follow the moving client. The packet is then fetched by the client. With the above innovative design, SWIMMING achieves seamless roaming with reliable link, high throughput, and low packet loss. Test bed implementation and experiments are conducted to validate the effectiveness of the ACK detection function. Extensive

ISSN 2394-3777 (Print)
ISSN 2394-3785 (Online)
Available online at www.ijartet.com
International Journal of Advanced Research Trends in Engineering and Technology (IJARTET)
Vol. 3, Special Issue 24, April 2016

simulations are carried out to evaluate the performance of SWIMMING. Experimental results show that SWIMMING outperforms existing schemes remarkably.

1.INTRODUCTION

WITH the penetration of portable smart devices, thedemand for Internet access from moving vehicles has grown sharply in recent years. An increasing number of commuters and passengers prefer accessing the Internet using their smart phones or tablet computers while traveling, such as browsing the web, dealing with E-mails, making VoIP calls, watching video programs, playing online games, etc. At present, cellular networks (e.g., GPRS, 3 G, or LTE) provide ubiquitous Internet connection, but with relatively expensive cost. Furthermore, the cellular networks have been proven to be insufficient for the surging amount of data from Internet-enabled mobile devices [1]. Due to the explosive growth of the subscriber number and the mobiledata, cellular networks are suffering overload, and the users are experiencing service quality degradation. WiFi, based on IEEE 802.11, is another technology to provide wireless connectivity. It has undergone rapid development and has entered a new period of prosperity. To date, WiFi hotspots are deployed widely and densely in many cities, and the trend continues [2]. Compared with cellular networks, WiFi has obvious advantages: lower cost and higher peak throughput. Thus, WiFi is considered as a suitable solution for cellular traffic offloading [2], [3]. However, it is still challenging to provide Wi Fi-based Internet access for users in moving vehicles. The reasons are elaborated as follows. First, channel condition in a vehicular environment is usually harsh owing to severe multi-path fading, interference, and noise, which results in high packet loss rate. Second, since a client moves at a vehicular speed, it is extremely difficult for it to be always associated with the most appropriate AP. Third, due to the limited coverage of each single AP, a client suffers from frequent connection disruptions caused by handoffs and re-associations. In this paper, we propose a solution, referred to as SWIMMING, to support seamless and efficient Wi Fi-based Internet access from moving vehicles. In SWIMMING, a group of APs are employed to communicate with a client (called “AP diversity”), and the transmission succeeds if any AP in the group accomplishes the delivery with the client (called “opportunistic transmission”). Such AP diversity and opportunistic transmission are exploited to overcome the high packet loss rate, which is achieved by configuring allthe APs with the same MAC and IP addresses. With such aconfiguration, a client gets a graceful illusion that only one(“virtual”) AP exists, and will always be associated withthis “virtual” AP. For uplink communications, when the client transmits a packet to the virtual AP, actually multiple APs within its transmission range are able to receive it. The transmission is successful as long asat least one AP receives the packet

ISSN 2394-3777 (Print)
ISSN 2394-3785 (Online)
Available online at www.ijartet.com
International Journal of Advanced Research Trends in Engineering and Technology (IJARTET)
Vol. 3, Special Issue 24, April 2016

correctly. Since each AP that receives the packet returns an acknowledgement (ACK) frame, SWIMMING operates in a "group unicast" mode. Unlike broadcast or promiscuous mode, ACK-based rate control mechanisms can be seamlessly applied to this group unicast mode, which increases the efficiency and reliability of the channel utilization. In order to avoid possible collisions of ACKs P.

Lv, X. Xue, and M. Xu are with the College of Computer, National University of Defence Technology, Changsha 410073, China. E-mail: {lvpin08, xuexiuhui, xuming}@nudt.edu.cn. X. Wang is with the University of Michigan-Shanghai Jiao Tong UniversityJoint Institute, Shanghai Jiao Tong University, Shanghai 200240, China. E-mail: wxudong@ieee.org. Manuscript received 16 Aug. 2013; revised 25 June 2014; accepted 3 July 2014. Date of publication 21 July 2014; date of current version 30 Mar. 2015.For information on obtaining reprints of this article, please send e-mail to: reprints@ieee.org, and reference the Digital Object Identifier below. Digital Object Identifier no. 10.1109/TMC.2014.2341652 IEEE TRANSACTIONS ON MOBILE COMPUTING, VOL. 14, NO. 5, MAY 2015 1085 1536-1233 2014 IEEE. Personal use is permitted, but republication/redistribution requires IEEE permission.

See http://www.ieee.org

from different APs, an additional ACK detection function is developed to enhance the conventional ACK decoding. Furthermore, as all APs are configured with the same MAC address and IP address, both layer-2 and layer-3 handoffs of the mobile client are totally eliminated. For downlink communications, a packet destined for a client is delivered in two stages. In the first stage, the packet is pushed to a group of APs through multicast rather than being pushed to the client directly through unicast. This AP multicast group is maintained dynamically to follow the moving client. In the second stage, the client then sends periodical requests to APs to fetch its packet buffered in the AP group. This twostage strategy maintains stable end-to-end downlink communications for the client in a moving vehicle. The advantages of SWIMMING are summarized below: 1) By exploiting the AP diversity and opportunistic transmission, the link reliability is enhanced, and packet loss is significantly reduced. 2) An ACK detection function is designed to eliminate the adverse effect of multiple ACKs. This function ensures that ACK-based rate control mechanisms can be adopted in SWIMMING to improve the efficiency of the channel utilization. 3) By configuring all APs with the same setting, both layer-2 and layer-3 handoffs of the mobile client are eliminated, and seamless roaming within the coverage of the entire network is achieved. 4) The two-stage packet delivery in downlink communications dramatically increases the probability of successful transmissions. Thanks to these advantages, SWIMMING outperforms other schemes remarkably. For

ISSN 2394-3777 (Print)
ISSN 2394-3785 (Online)
Available online at www.ijartet.com
International Journal of Advanced Research Trends in Engineering and Technology (IJARTET)
Vol. 3, Special Issue 24, April 2016

example, the throughput improvement achieves up to 100 to 200 percent. The remainder of the paper is organized as follows. Related work is summarized in Section 2. The architecture of SWIMMING is described in Section 3. Details of uplink and downlink communication protocols are presented in Sections 4 and 5, respectively. Experimental results from both real testbed and simulator are reported in Section 6. The paper is concluded in Section 7

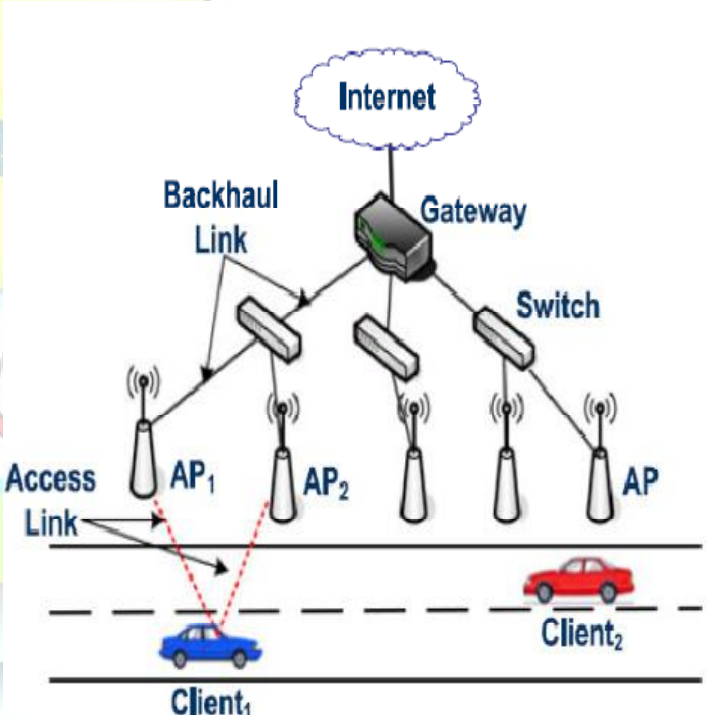
2 RELATED WORK

The related work can be classified into three categories. The differences between our solution and the representative schemes in each category are explained below. Internet access from moving vehicles. With a rapid growth of demand for Internet access from moving vehicles, researchers come up with a number of solutions based on the cellular networks or the WiFi networks. MAR [4] is a cellularbasedsolution, while MobTorrent[5] and Wiffler [3] jointly consider cellular networks and WiFi networks by utilizing their complementary functions. Measurement studies of WiFi connectivity in the vehicular environments can be found in [6], [7] and [8]. Drive-thru Internet [9] and Cabernet [10] are designed to maximize the transmission opportunity and link utilization in a network with sparse AP deployment and intermittent connectivity. Several literatures propose particular methods for file uploading [11] or downloading [12] of vehicular clients respectively. IEEE 802.11p standard [13] has been released to support wireless access in vehicular networks, and many studies are based on this standard, e.g., [14]. The major difference between the above references and our work is that SWIMMING takes advantage of AP diversity to overcome the issue of unreliable links and unstable connections.AP diversity. The association scheme in the WiFi context is inflexible, i.e., a client is associated with a certain AP at any time. The consequence of this limitation is that, if the associated AP of the client receives a packet with errors, the transmission fails even if a neigh boring AP overhearsthe packet successfully. In order to benefit from the broadcast nature of the wireless links, a number of works (such as [15], [16], [17], [18]) exploit AP diversity to improve system performance. MRD [15] recovers a frame from multiple erroneous copies of the frame without retransmission in enterprise WLAN deployment. Our previous work [16] represents a network-leading association scheme for Wi-Fi-based wireless mesh networks (WMNs). In [16], the access interfaces of all the mesh APs are set to the identical MAC address, IP address, ESSID and channel, thus multiple APs can receive packets from a client. To reduce transmission redundancy and avoid ACK collisions, the most appropriate AP is selected adaptively to forward the packets to the gateway, and return ACKs to the client. The ACK functions of other APs are disabled for the client. Similar to[16], APs in OmniVoice [17] also broadcast the same ESSID and MAC address in their beacons,

ISSN 2394-3777 (Print)
ISSN 2394-3785 (Online)
Available online at www.ijartet.com
International Journal of Advanced Research Trends in Engineering and Technology (IJARTET)
Vol. 3, Special Issue 24, April 2016

but the ACK collision issue is not considered in this scheme. In [18], a protocol called ViFi opportunistically exploits AP diversity to minimize disruptions of mobile services. In this protocol, a vehicle designates one of the nearby APs as the anchor, which is responsible for the vehicle's connection to theInternet. Other nearby APs are selected as auxiliaries. The transmitter uses MAC-layer broadcast so that packets canbe received by multiple APs. Hence, it has to send packetsat the lowest bit-rate in broadcast, which leads to longerchannel holding time. If an auxiliary overhears a packet,but has not heard a customized ACK within a small window, it probabilistically relays the packet to the anchor. The transmission from the auxiliary to the anchor incurs extra delay and overhead. In our proposed SWIMMING, the AP diversity is achieved in the same way as [16]. To avoid performance degradation caused by possible collision of ACKs from different APs, the ACK decoding at the client side is enhanced with an ACK detection function. Therefore, ACK-based rate control mechanisms can be easily applied to improve wireless channel utilization. The transmission succeeds if at least one AP receives the packet correctly, which also increases the efficiency. Fast handoff in WiFi networks. The mobility of clients makefast handoff become a critical issue in WiFi networks. A number of papers aim at minimizing the handoff delay in WLANs [17], [19], [20] and WMNs [16], [21]. Several approaches (e.g., SyncScan [19] and Proactive Scan [20]) reduce handoff delay by decoupling the time-consuming channel scan from the actual handoff. As previously mentioned, client handoff delay is eliminated in [16] and [17] in that APs have exactly the same configuration. Nonetheless

LV ET AL.: SWIMMING: SEAMLESS AND EFFICIENT WIFI-BASED INTERNET ACCESS FROM MOVING VEHICLES 1087



an interference map needs to be generated in [17], while an appropriate AP needs to be selected to serve a client in [16]. Both of them are unfit for highly dynamic vehicular environments. In SMesh [21], the mesh node, which believes ithas the best

ISSN 2394-3777 (Print)
ISSN 2394-3785 (Online)
Available online at www.ijartet.com
International Journal of Advanced Research Trends in Engineering and Technology (IJARTET)
Vol. 3, Special Issue 24, April 2016

connectivity with the client, sends a gratuitous ARP message to the client. The client then updates its ARP cache, and the handoff is accomplished. Moreover, IEEE 802.11r standard [22] has been promulgated to reduce handoff delay to support real-time applications, such as VoIP. All the above-mentioned approaches are not designed for the scenario that clients move at a vehicular speed. In SWIMMING, a client is not associated with a certain AP, and no handoff is triggered when the client roams within coverage of the entire network. Therefore, SWIMMING is the most appropriate for the WiFi-based communications in vehicular environments.

3.THE ARCHITECTURE OF SWIMMING

In this work, we consider a scenario (as demonstrated in Fig. 1) that a road is completely covered by open WiFiaccess points (APs), and coverage of each AP may overlap with others. Each AP is equipped with two interfaces; one is for client access based on WiFi, while the other uses wired or wireless medium to form a backhaul. Hence, the backhaul can be either a local area network (LAN) or a wireless mesh network. The backhaul connects to the Internet through a gateway. It is assumed that both bandwidth and reliability of backhaul links are higher than that of access links, and packet loss in backhaul is negligible. Moreover, only the traffic between clients and the Internet is taken into account in this paper. When APs have established routing paths to the gateway, the backhaul is organized into a tree topology with the gateway as the root and APs as leaves. In [8], the researchers conduct a large number of measurements in real vehicular environments, and the following experimental observations are revealed:

1) Gray-zone behaviour (i.e., intermediate packet loss rate) is a dominating phenomenon;

2) Temporal correlation is weak;

3) Spatial correlation is weak;

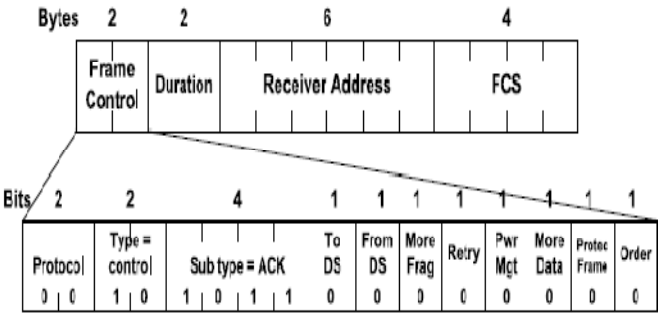
4) Incoming and outgoing links exhibit a strong symmetric correlation. These issues are properly addressed by SWIMMING.

Since packet loss is severe in vehicular environments, AP diversity and opportunistic transmission are designed to enhance transmission reliability. More specifically, the backhaul network works as a conventional method does, while the interface for client access of each AP is configured with the same parameters as those of others, including the MAC address, the IP address, the wireless channel, and the ESSID. With such settings, a client gets a graceful illusion that there exists only one AP (i.e., the “virtual” AP) in the environment. When the client intends to join the network, it is associated with this virtual AP, and requests an IP address through DHCP. The DHCP server running at each AP uses the same hash function to compute a unique IP address for the client based on the its MAC address. The hash function maps a MAC address to a class A private IP

ISSN 2394-3777 (Print)
ISSN 2394-3785 (Online)
Available online at www.ijartet.com
International Journal of Advanced Research Trends in Engineering and Technology (IJARTET)
Vol. 3, Special Issue 24, April 2016

address in the form of 10.A.B.C. The default gateway on the client is set to the IP address of the virtual AP. When the client transmits a packet to the virtual AP, actually multiple APs within its transmission range are able to receive the packet. Owing to weak temporal and spatial correlation, the receptions of different APs can be viewed to be independent.When an AP misses a packet,its neighbour AP mayreceive it. As long as the packet is received by one AP, it can be forwarded to the Internet, and thus the successful transmission probability increases. For instance, both AP1 and AP2 in Fig. 1 are located within the transmission range of Client1. Assume the success probabilities that these two APs receive the packets of Client1 are P1 and P2, respectively. When Client1 sends a packet to them, the probability that the transmission succeeds is $P=1-(1-P_1)(1-P_2)=P_1+P_2-P_1P_2$

The identical configuration of all the APs has another important advantage: both IP-layer and MAC-layer handoff are eliminated. Hence, connection disruptions caused by the handoffs and re-associations are avoided, and the network connection will not be disrupted even if an AP crashes. A potential requirement of AP diversity is that all APs operate on the same wireless channel. In fact, SWIMMING can be easily extended to multi-channel deployment as follows. An AP is able to be equipped with multiple WiFi radios, and these radios are configured to different non-overlapping channels. The radios, which belong to different APs but operate on the same channel, are organized into a virtualAP as described above. Under this circumstance, there are multiple virtual APs in the network, and the system capacity is multiplied. As prices of WiFi radios are rather low nowadays, this kind of multi-radio extension of the APwould not cause significant cost increment. If client broadcasts its packets or APs are set to promiscuous mode, there also have multiple APs receiving the client's packets. However, in these two ways, no acknowledgement frame (ACK) is replied, and the client cannot know whetherthe transmission is successful. Thus, in order to maximize the delivery ratio, the client has to transmit packets at the lowest bit-rate, which leads to inefficient bandwidth utilization. Furthermore, without MAC-layer acknowledgement, the confirmation and the retransmission have to rely on upper layer protocols (e.g., TCP). When packet loss happens, the performance deteriorates quickly due to the congestion control mechanism of TCP. As APs are configured into the



ISSN 2394-3777 (Print)
ISSN 2394-3785 (Online)
Available online at www.ijartet.com
International Journal of Advanced Research Trends in Engineering and Technology (IJARTET)
Vol. 3, Special Issue 24, April 2016

unicast mode, they send ACKs back upon receiving a packetcorrectly. Therefore, the ACK-based rate control mechanisms (e.g., ARF [23], and RRAA [24]) can be readily applied to our SWIMMING scheme. With rate control, the transmission rate can adapt to channel conditions. As a result, wireless resources are utilized in a more efficient manner, and the performance is much improved. If multiple APs receive a packet, each of them will transmit an ACK after a period of short inter-frame space (SIFS). These multiple copies of ACKs may collide at the client. Hence, a new scheme is designed to handle such collisions. In the new scheme, the ACK decoding is enhanced with ACK detection, which is described in Section 4.1. Successful receptions of multiple APs may also incur redundant transmission in the backhaul. A strategy of dropping duplicate packets as early as possible is taken to reduce such redundancy as described in Section 4.2. The overhead caused by AP diversity is analysed in Section 4.2. The downlink communication in SWIMMING is divided into two stages. In the first stage, packets destined for a client are delivered to a group of APs through multicast. This AP multicast group is maintained dynamically to follow the moving client. In the second stage, the client periodically sends downlink packet requests (DPRs) to fetch its packets buffered in the AP group. The introduction of DPR brings two benefits. First, it helps APs to locate the moving client, even if the client has no uplink packets to transmit. Second, it probes the channel quality. Due to the strong symmetric correlation of wireless links, if an AP receives a DPR from a client and transmits a packet to the client immediately, it is with high probability that the packet can be received by the client. This two-stage strategy significantly reduces unnecessary transmissions when channel condition is poor, and dramatically improves the downlink transmission efficiency. How to establish and maintain the multicast group is discussed in Section 5.1. The protocol of downlink packet request is presented in Section 5.2. How to determine the key parameters in the protocol is discussed in Section 5.3.

4 UPLINK COMMUNICATION

4.1 ACK Detection Scheme

The format of the acknowledgement (ACK) frame specified in IEEE 802.11 standard is revealed in Fig. 2. For a certain data packet of a client, the 14-byte ACKs generated by different APs are exactly the same. When multiple identical ACKs are emitted by different APs almost simultaneously, whether or not these ACKs will collide at the client raises a question. Consider a scenario as shown in Fig. 3.

ISSN 2394-3777 (Print)
ISSN 2394-3785 (Online)
Available online at www.ijartet.com
International Journal of Advanced Research Trends in Engineering and Technology (IJARTET)
Vol. 3, Special Issue 24, April 2016

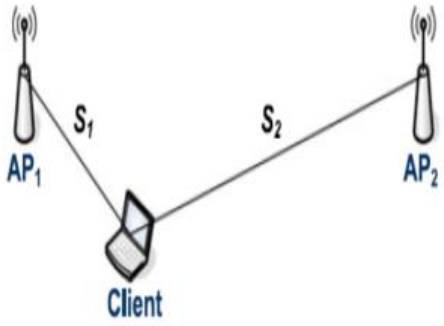


Fig. 3. An example scenario of two APs within the transmission range of the client.

The distance between the client and AP1 is denoted as S1, while the distance between the client and AP2 is S2. Without loss ofgenerality, it is assumed that S1 < S2. Hence, when both AP1 and AP2 reply ACKs to the client, the two ACKs partially overlaps as sketched in Fig. 4. The duration from the arrival of the first ACK to the arrival of the last ACK, referred to as arrival time difference is 2(T2-T1), where T1 and T2 are the signal propagation time from the client to AP1 and AP2, respectively.The overlapping signals can be decoded under two conditions:

(1) the strength of one signal is considerably higher than the strength of the other one; (2) the arrival time difference is less than the OFDM guard interval TGI (which isdesigned to eliminate multipath effect). Under the first condition,the weak signal is dropped by the filter of thereceiver, and only the strong signal is retained to be decoded.

Under the second condition, in order to decode the signal transmitted from AP1 and AP2, the difference of

T1 and T2 should satisfy

$$\Delta T = |T2 - T1| < 1/2\ T_{GI} \quad (2)$$

Let the constant C be the electromagnetic wave propagation

speed in the air, so Si = CTi , i = 1,2.

Thus, it can be obtained that

$$\Delta S\ |S2 - S1| < 1/2\ CT_{GI} \quad (3)$$

The OFDM guard interval (TGI) for 20 MHz channel spacing defined in IEEE 802.11 standard is 0.8 ms, and the constant C is 3×10^8m/s. If only considering the direct path, the signal can be received without collision when the difference of S1 and S2 satisfies

$$\Delta S = |S2 - S1| < 120 \text{ m.} \quad (4)$$

When the difference of S1 and S2 is greater than 120 meters, there usually exists significant difference between the strengths of the signals from AP1 and AP2. Therefore, ACK can be correctly

Fig. 2. Format of ACK frame specified in IEEE 802.11 standard. Fig. 3.An example scenario of two APs within the transmission range of the client.

Fig. 4.Illustration of ACK overlap.

ISSN 2394-3777 (Print)
ISSN 2394-3785 (Online)
Available online at www.ijartet.com
International Journal of Advanced Research Trends in Engineering and Technology (IJARTET)
Vol. 3, Special Issue 24, April 2016

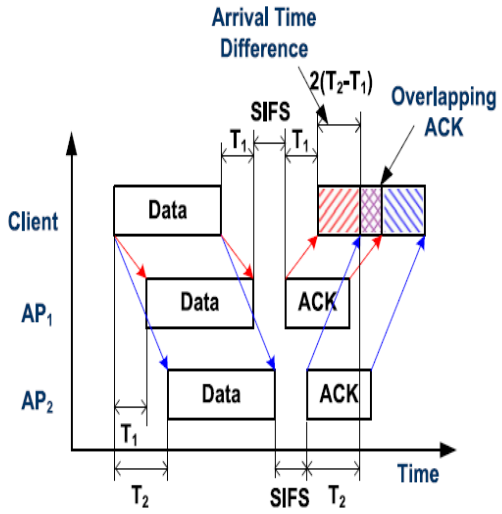


Fig. 4. Illustration of ACK overlap.

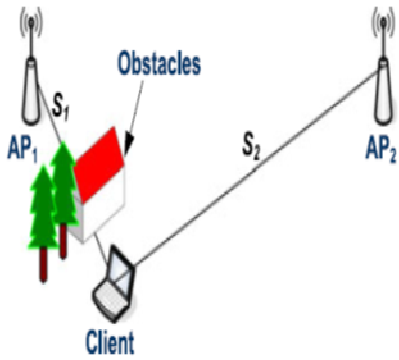


Fig. 5. An example scenario of two APs with different distances but similar signal strengths.

decoded as explained in the first condition. However, if the direct path from AP1 to the client is blocked by some obstacles as shown in Fig. 5, the signal strength of AP1 may be similar to that of AP2 at the client. In this case, the overlapping ACKs cannot be decoded correctly. In order to avoid retransmissions caused by ACK collisions, an additional ACK detection function is proposed. Once a WiFi node has received a data frame correctly, it responds the transmitter with an ACK after a short inter frame space as specified in IEEE 802.11 standard. The medium after SIFS is reserved for a period of ACK transmission. For this reason, even though the simultaneously transmitted ACKs collide at the client, no other signals exist during the ACK transmission period. Based on this principle, we can still detect ACK even if ACK collision happens. The solution is explained as follows. We know that, total duration of the ACK (T_{Total}) includes three parts: the preamble duration ($T_{Preamble}$), the physical layer convergence procedure (PLCP) header duration (TPLCP), and the ACK frame transmission duration (TACK):

$$T_{Total} = T_{Preamble} + T_{PLCP} + T_{ACK} \quad (4)$$

The ACK transmission duration can be calculated by

$$T_{ACK} = (L_{ACK}/R_{ACK}) \quad (5)$$

where LACK is the length of the ACK frame, while RACK is the bit-rate of the ACK transmission. As specified in IEEE 802.11 standard, $T_{Preamble}$ of OFDM is 20 ms, and TPLCP of OFDM is 4 ms.It is revealed in Fig. 2 that the length of the ACK frame is 112 bits (14 bytes), which is obviously shorter than frames of other types. The bit-rate of the ACK transmission is determined by the bit-rate of the data frame transmission. The ACK bit-rate is equal to

ISSN 2394-3777 (Print)
ISSN 2394-3785 (Online)
Available online at www.ijartet.com
International Journal of Advanced Research Trends in Engineering and Technology (IJARTET)
Vol. 3, Special Issue 24, April 2016

the data bit-rateif the data is transmitted at the level no higher than24 Mbps; if the data bit-rate is elevated to a higher level, the ACK bit-rate remains at 24 Mbps. For example, when the ACK is transmitted at 24 Mbps, the theoretical total duration of ACK is about 28.7 ms. Owing to partial overlapping, the actual duration of the collided ACKs should be a little longer than the theoretical duration. Based on this obvious pattern, the ACK can be distinguished from random noise or other types of frames. Therefore, after the transmission of a data frame, if the length of an undecodable signal is detected to be within a certain range of the theoretical ACK transmission duration, it can be recognized as the collided ACKs. The detection range is measured in Section 6.1. If an interference signal happens to appear after a data packet transmission and a period of SIFS, possible cases are analyzed in Fig. 6.

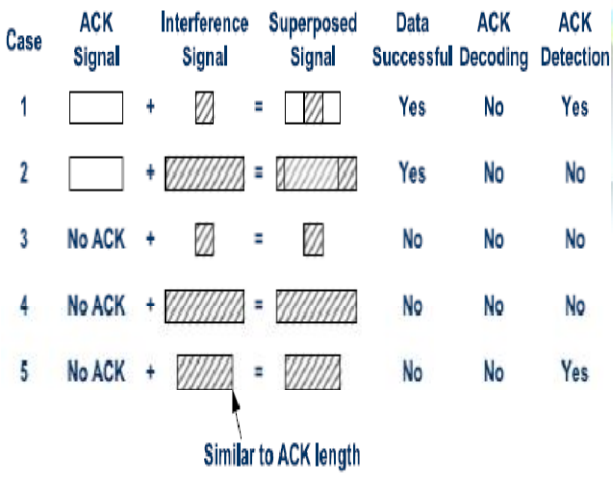


Fig. 6. Possible cases of interference signal.

In Case 1, the data transmission is successful and an ACK is returned. If a sudden interference signal comes, which is shorter than the ACK, the traditional ACK decoding scheme cannot decode the ACK frame, thus a retransmission of data packet is needed. With ACK detection scheme, the disturbed ACK frame can still be detected, which avoids unnecessary retransmissions. In Case 2, the ACK frame is totally covered by a continuous interference signal which is much longer than the ACK. In this case, the ACK detection scheme cannot find the ACK frame, which has the same effect with the traditional ACK decoding. In Cases 3 and 4, the data transmission is unsuccessful, and no ACK frame is transmitted. In these cases, the ACK detection mechanism will not recognize the interference signal as the ACK if the length of the interference signal is too short or too long. The only case that the ACK detection method reports a false positive result is indicated in Case 5. Since the length of the interference signal is similar to the ACK frame, it is mistaken for the ACK by the ACK detection scheme. Hence, a packet loss takes place in this case, and the packet has to be recovered by upper-layer protocols. Fortunately, the probability of this case is rather low in practice since both the length and the arrival time of the interference signal have to follow the ACK frame pattern.The ACK detection scheme is entirely implemented at the client. Our implementation is based on a wireless network interface card with Atheros AR5414 chipset and MadWiFi. The duration of ACK reception is measured by a 32-bit

ISSN 2394-3777 (Print)
ISSN 2394-3785 (Online)
Available online at www.ijartet.com
International Journal of Advanced Research Trends in Engineering and Technology (IJARTET)
Vol. 3, Special Issue 24, April 2016

counter register RFCNT, which counts the time at the 40 MHz (for 802.11a mode) or 44 MHz (for802.11g mode) built-in quartz resolution. The counter of RFCNT accumulates the time in clock units during which the card receives signals. To record the receiving time of a single ACK, a few interrupts are exploited to reset the counter at a proper time. As demonstrated in Fig. 7, when a data frame is delivered to the hardware and the queue is empty, an interrupt of TXEOL is triggered; at the time that an ACK is decoded successfully, an interrupt of TXOK happens; if the client is not able to decode the ACK and the timer expires, an interrupt of TXERR is invoked. Consequently, in our implementation, only one packet is pushed into the queue each time, and the counter of RFCNT is reset at every TXEOL interrupt. When the TXERR interrupt occurs, the count of RFCNT is checked. If the counted time falls within a certain range, it is considered that an ACK is replied and the data frame has been transmitted correctly. To avoid retransmissions conducted by hardware, the original retransmission function should be switched off, and the retransmission is implemented in the MAC driver.

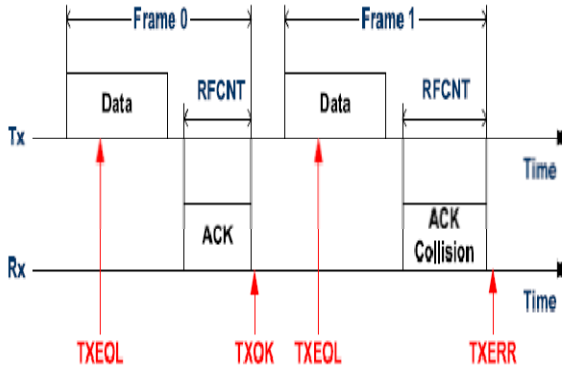


Fig. 7.Illustration of ACK detection.

4.2 Transmission Redundancy

Since the diversity of multiple APs is exploited, a packet can be received by multiple APs. If all copies of the same packet are forwarded to the gateway, extra overhead is introduced to the backhaul. A metric of transmission redundancy ratio (TRR) is defined to measure the overhead:

$$TRR = R/E \quad (6)$$

where R is the redundant transmissions, and E is the effective transmission times. For instance, if a packet is transferred from an AP to the gateway through three hops, the value of E is 3. In order to minimize TRR, a redundancy removal mechanism is proposed as follows. If an intermediate node in thebackhaul network (as shown in Fig. 1) receives a packet thathas been forwarded, it simply drops the duplicated packet. To determine whether a packet has been delivered before, a few fields of the packet are checked to identify the packet. For a TCP packet, it can be identified by a 5-tuple

ISSN 2394-3777 (Print)
ISSN 2394-3785 (Online)
Available online at www.ijartet.com
International Journal of Advanced Research Trends in Engineering and Technology (IJARTET)
Vol. 3, Special Issue 24, April 2016

of<*source*_IP, *source*_port, *destination*_IP, *destination*_port,TCP_*sequence*_number>. For a UDP packet, TCP_*sequence*_- number in the 5-tuple is replaced by checksum.

In a LAN backhaul, the APs are interconnected by cables, hubs and switches. When a node transmits a packet to its upper-layer node, other nodes in the same subnet can overhear the packet as well. Thus, these node are able to directly avoid redundant transmissions. In a WMN backhaul, one AP may not overhear the backhaul transmission of a packet from another AP. In this case, two APs may forward the same packet to an upper-layer node. Such redundancy has to be eliminated at the upper-layer node. Suppose the hierarchical backhaul is organized into a complete k-tree topology with m layers, the gateway is at the first layer, while all the APs are located at the mth layer. The APs are deployed uniformly along a straight road as

shown in Fig. 8, and the distance between two adjacent Aps is d, and the length of the AP-formed line within the transmission range of the client is denoted as s. Since the road is entirely covered by the APs, s is definitely greater than d.The number of APs within the transmission range of the client (called communicating APs) is denoted as a. The value of a can be |s/d| (Fig. 8a) or |s/d|(Fig. 8b). Consider the case that all these communicating Aps receive the packet sent by the client without packet loss. In this case, the TRR achieves the upper bound. Limited by the transmission power, it is assumed that a<= k, i.e., all communicating APs belong to only one or two bottom subtrees. The redundancy is determined by the layer on which the closest common parent (CCP) node is located. If the CCP node is at the (m-1) 1Þth layer,

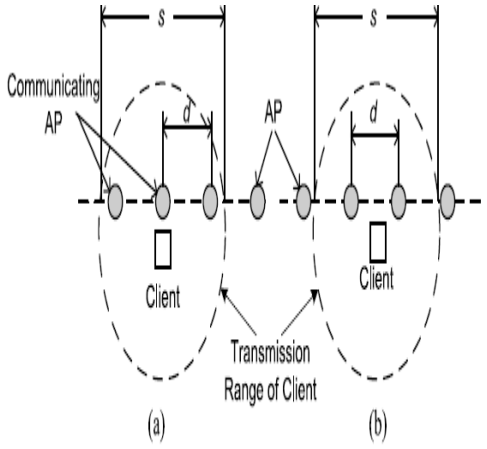


Fig. 8. Two cases of APs within the transmission range of the client.

i.e., all communicating APs belong to the same bottom subtree, the redundant transmissions is zero for LAN, and is (a - 1) for WMN in the worst case. If the CCP node is at the ith layer

where 1 <= i<= m-2, the communicating APs are distributed in two bottom subtrees. Without loss of generality, suppose the numbers of the communicating APs in the two bottom subtreesare p and q respectively, where 1 ≤ p ,q≤ a -1 and p + q =a. For LAN backhaul, two copies of the same packet are delivered to upper-layer nodes from the mth layer. The duplicated packet is dropped at the (i +1)th layer. Hence, the number of the redundant transmission.

ISSN 2394-3777 (Print)
ISSN 2394-3785 (Online)
Available online at www.ijartet.com
International Journal of Advanced Research Trends in Engineering and Technology (IJARTET)
Vol. 3, Special Issue 24, April 2016

(p-1)+(q-1)+(m-i)=m+a-i-2.(7)

Since there are k^{m-1} APs, the total number of communicating AP groups is k^{m-1}-a+1.. The number of cases that the a APs in the same group belong to the same subtree is k^{m-2}(k-a+1). The number of communicating AP groups with the CCP node located at the ith($1 \leq i \leq m-2$) layer is k^{m-2}(k-a+1).Therefore, the TRR upper bound for LAN is k^{i-1}(k-1)(a-1)

$$TRR_{LAN}= \sum_{i=1}^{m-1(} ki-1(k-1)(a-1)./km-1-a+1).(m-i-1/m-1)$$

where (m-1) in the denominator is the effective transmissions. Suppose the percentage of communicating APs that can-not overhear each other is b.

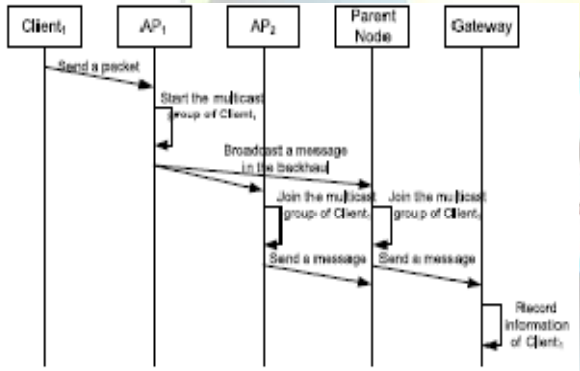


Fig. 9. Multicast group establishment.

5.DOWNLINK COMMUNICATION

When packets from the Internet need to be delivered to a client, AP diversity and opportunistic transmission are also leveraged to improve transmission reliability. In other words, there are still a group of APs being employed to serve the client. Inorder to reduce transmission overhead, the packets are sent to this AP group using multicast. Consequently, for downlinkcommunicationsinSWIMMING,a multicastgroup isestablishedforeachclient.

5.1 Multicast Group Management

For a client with the IP address of 10.A.B.C, its corresponding multicast group is assigned a class D private multicast IP address of 239.A.B.C. Once an AP receives a client's packet, the AP starts the multicast group of the client automatically. As the client is moving, geographically neighbouring nodes of the AP are likely to communicate with the clientlater.Usually,geographicallyneighbouri ngnodes probably locate within the same backhaul broadcast domain. Hence, the AP broadcasts a message from its backhaul inter- face toinformthenodeswithinits broadcast domain(including its parent node) to join the multicast group of the client. Upon receiving the message, each AP sets itself as a member of the multicast group, and then informs its parent node. The parent node also sends a notification to its parent iteratively until a multicast tree rooted at the gateway has been established. Since the bandwidth of the backhaul is much higher than access links, the cost to maintain and manage the multi- cast group is negligible. The process of multicast group establishmentisillustratedinFig.9. How an AP leaves a multicast group will be discussed in Section 5.2. When quitting from the multicast group, the AP also issues a notification to its parent node. As a parent node, when all its child nodes have left the

ISSN 2394-3777 (Print)
ISSN 2394-3785 (Online)
Available online at www.ijartet.com
International Journal of Advanced Research Trends in Engineering and Technology (IJARTET)
Vol. 3, Special Issue 24, April 2016

multicast group, it also withdraws from the multicast group and then sends a notification to its parent node.

5.2 Downlink Packet Delivery

Since each client is assigned a class A private IP address, the gateway needs to run a network address translation (NAT) service to enable the communication with the Internet. Additionally, the gateway also maintains a sequence number for each client to count the downlink packet number of the client. The sequence number is initialized as zero. When a packet from the Internet arrives at the gateway, the

Gateway firstly looks up the mapping table to find out the IP address of the destination, e.g., 10.A.B.C. Next, the gate- way encapsulates the packet with a new IP header with the destination IP address of 239.A.B.C. The gateway also puts the corresponding sequence number in the option field of the new IP header, and increases the sequence number by 1 for the next packet. The newly-encapsulated packet is transferred through multicast, and is buffered by the multicast group members. Sinceit isunknownwhichAP istheoptimalchoicetodeliver the packet, the client needs to requests its downlink packet from the APs in sequence. The client sends a MAC-layer frame, referred to as downlink packet request, with a specified sequence number. For convenience in writing, denote theDPRwithasequencenumber n as DðnÞinthefollowing. Upon receiving DðnÞ, the AP checks its buffer to deter- mine whether it has the packet with the sequence number n. If such a packet exists in its buffer, the AP removes the IP header for multicast and delivers the actual IP packet to the client immediately. Owing to the strong symmetric correlation of wireless links, it is with high probability that the packet can be received by the client. When multiple APs receive the DPR, these APs contend the channel based on CSMA/CA to deliver the packet. If an APs cannot get a chance to transmit the packet, it continues to hold the packet. However, the DPR will become invalid, and the AP will not attempt to transmit the packet again after a certain period for two reasons. First, probably another AP has sent the packet to the client already. Second, the channel condition may have changed due to the weak temporal correlation, so the delivery cannot be guaranteed. The period equals to the duration of the packet transmission, which is deter- mined by the packet length and the bit-rate. Due to the link symmetry, the bit-rate equals to the bit-rate at which client sends DðnÞ. If the client is not responded with its packet after sending DðnÞ, it sends DðnÞ repeatedly. If the client successfully receives its packet, it sends Ððnþ1Þ next. The AP counts the number of packets with sequence number larger than n, and the number is attached in the data packet. Thus, the client knows how many unreceived packets still remain in the buffer of the AP. If such packets exist, the client will send another DPR immediately; otherwise, there are two opportunities to send a new DPR. First, if the client has an uplink packet to

ISSN 2394-3777 (Print)
ISSN 2394-3785 (Online)
Available online at www.ijartet.com
International Journal of Advanced Research Trends in Engineering and Technology (IJARTET)
Vol. 3, Special Issue 24, April 2016

transmit, it will piggyback the DPR with the uplink packet to reduce overhead. Second, if there is no uplink packet to be transmitted within a given interval, the client will send a DPR directly. How to set the interval will be discussed in Section 5.3. The downlink communication process is demonstrated in Fig. 10. If the AP delivers the packet successfully, it removes the packet from the buffer as well as the packets with lower sequence numbers, as the client has already obtained these packets. The AP also sends a notification to every multicast group member to delete the corresponding packets. There- fore, all the APs in the multicast group are synchronized, and they do not store obsolete packets for the client. On receiving an uplink packet or a DPR, the AP sends a keep-alive message to the multicast group. If an AP has not received any uplink packet, DPR, or keep-alive message of

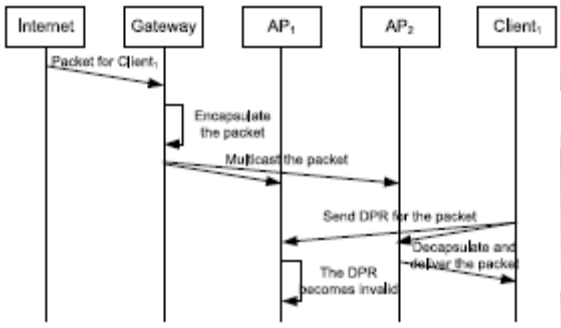


Fig. 10. Downlink communication process.

the client for a certain period, it will leave the multicast group. The length of the period is determined in Section 5.3. When the AP leaves the multicast group of the client, it deletes all the packets buffered for the client.

5.3 Parameter Determination

Since a DPR is needed when a client has no uplink packets for a period that is long enough to cause latency issue in the downlink transmission. To support real-time applications like voice, we require one-way delay at the downlink to be less than a certain value. According to ITU G.114 [25], a net- work one-way delay of 0-150 ms is acceptable for voice applications. Considering other factors that may also cause network delay, the delay budget for the downlink transmission in our protocol is set to be 30 ms. Thus, a client has to send a DPR whenever it lacks uplink packets for 30 ms. The overhead from this frequency of DPR transmission is analyzed below. Considering that a 64-byte DPR is sent using the lowest bit-rate of 802.11a (6 Mbps) and 15 clients need to send a DPR every 30 ms, then the total time for DPR will be 64158=6;000=1:28 ms. Thus, the total overhead will be 1:28=30 ¼ 4:3%. In reality, the overhead is much smaller for two reasons: 1) a DPR can be sent with a higher bit-rate; 2) the number of clients that need to send a DPR every 30 ms is much smaller than 15, since many clients have uplink packets to piggyback DPR. In our design, the client sends a DPR every 30 ms even if it has no uplink packets to transmit, and APs in the same multicast group gets a keep-alive message upon receiving a DPR by one AP. Thus, the APs in the multicast group know a client is still alive if a DPR is delivered properly. In view of high packet loss rate in vehicular environment, the DPR may be lost. Considering an extreme case

ISSN 2394-3777 (Print)
ISSN 2394-3785 (Online)
Available online at www.ijartet.com
International Journal of Advanced Research Trends in Engineering and Technology (IJARTET)
Vol. 3, Special Issue 24, April 2016

where the delivery ratio is only 5 percent, the probability that 100 continuous DPRs (from a specific client) are all lost (i.e., no DPR is received within 3 seconds from the client) is less than 0.6 percent, which is a rare event. Hence, if the AP in the multicast group has not received any uplink packet, DPR or keep-alive message for 3 seconds, it can consider the client has been unreachable (maybe out of the network coverage or power off), and packets in buffer are no longer needed for the client. On this occasion, the AP leaves the multicast group and deletes the buffered packets of the client. Since an AP has to buffer packets for all clients, in the extreme case that no DPR of any client is received within 3 seconds, the AP has to buffer all packets from the Internet

for 3 seconds. However, the packet arrival rate cannot exceed the highest downlink transmission rate, otherwise the buffer overflows even though downlink packets can be delivered to clients. If the 802.11a highest bit-rate is considered, 3 seconds of downlink packets is equivalent to 543=8 ¼ 20:3 Mbytes.1 Hence, 25 MB is large enough to buffer packets for all clients. Because an AP usually has a memory of several hundred megabytes, it is reasonable to utilize 25 MB memory space to buffer packets. The above-mentioned parameter values are given to illustrate the feasibility of our proposed solution. All these parameters can be reconfigured to adapt to particular application requirements or practical environments.

6PERFORMANCE EVALUATION

6.1 Verification of ACK Detection

ACK detection, as the foundation of SWIMMING, has never been proposed or implemented by previous studies. In order to verify the effectiveness of ACK detection, this scheme is implemented on a real testbed. The wireless network interface card used in the experiments is based on Antiheros AR5414 chipset. The Made WiFi driver is modified to read the RFCNT register at every TXERR interrupt and to reset the register at every TXEOL interrupt. Three WiFi nodes are deployed in the experiments. One of them works as the client, while the other two serve as the APs. The configurations of the two APs are totally identical. All the nodes are configured into 802.11a mode, and operate on Channel 40 (5.20 GHz). In the experiments, the client transmits UDP packets to the APs, and the APs return ACKs. To prevent retransmissions when ACKs collide, the retransmission function of the client is modified such that retransmission is initiated by our driver codes instead of hardware. This driver level retransmission function also ensures only one packet is pushed to the hardware queue at a time, which guarantees a TXEOL interrupt after a transmission. Two experiments are conducted in different scenarios as described below. Experiment I: Outdoor environment with different signal strengths. In this experiment, the three nodes are deployed in an outdoor environment, and they are placed statically like the example

ISSN 2394-3777 (Print)
ISSN 2394-3785 (Online)
Available online at www.ijartet.com
International Journal of Advanced Research Trends in Engineering and Technology (IJARTET)
Vol. 3, Special Issue 24, April 2016

shown in Fig. 3. A direct line-of-sight exists between the client and each AP. The length of S1 is 5 m, while S2 is about 100 m. Under this circumstances, the arrival time difference of the two returned ACKs can be larger than the OFDM guard interval. The signal strength of AP1 at the client varies from -47 to -45 dBm, which is much higher than the signal strength of AP2 (between -80 and -76 dBm). To ensure packets sent by the client be received by both APs, the client is fixed to transmit at the lowest bit-rate, i.e., 6 Mbps. Otherwise, if a higher bit-rate is adopted, AP2 is unable to decode the packet, thus it does not send back the ACK frame. Since an obvious gap exists between the signal strengths of the two APs, the weaker ACK signal has negligible impact to the ACK with stronger signal. Hence, the two

Fig. 10. Downlink communication process.

1. The physical layer rate (54 Mbps) instead of MAC layer rate is considered here for a more aggressive evaluation.

TABLE 1
Measurements in Outdoor Environment with Different Signal Strengths

	Data&ACK OK	Data Error	ACK Collisior
AP_1 & AP_2	99.96%	0.04%	0
AP_1 Only	99.88%	0.12%	0
AP_2 Only	99.76%	0.24%	0

returned ACKs do not collide at the client. As revealed in Table 1, 99.96 percent packets are delivered successfully when both APs receive the packets. The probabilities are 99.88 and 99.76 percent respectively if only AP1 or AP2 receives the packets. The high packet delivery ratio in the case of two APs indicates that AP diversity exists even in static environment. Experiment II: Outdoor environment with similar signal strengths. In Experiment II, AP1 is relocated to a room, and its line-of-sight to the client is blocked by a wall, like the scenario depicted in Fig. 5. The length of S1 is still 5 meters. However, because of the obstruction, the signal strength of AP1 at the client declines to-77 dBm, which is similar to the signal strength of AP2. The client is still fixed to transmit at the bit-rate of 6 Mbps. According to measurements, the lengths of the overlapping ACKs range from 46 to 48 ms. Thus, if the length of the detected signal falls in the range between 46 and 48 ms, it is recognized as an ACK frame. With such settings, ACK collisions occur frequently. As indicated in Fig. 11, with standard ACK decoding, only about a quarter of packets are delivered successfully. Most transmission failures are due to ACK collisions. However, when the ACK detection is applied, the delivery ratio is improved up to 99.93 percent, as shown in Fig. 11. The above two experiments are carried out under static conditions. The scenario that the client is moving is also tested. Under dynamic conditions, most overlapping ACKs can be easily decoded. This is because the arrival time difference of the two ACKs is smaller than the OFDM guard interval, or the signal strength of one ACK significantly exceeds the other one. Only in some special cases (like the scenario

ISSN 2394-3777 (Print)
ISSN 2394-3785 (Online)
Available online at www.ijartet.com
International Journal of Advanced Research Trends in Engineering and Technology (IJARTET)
Vol. 3, Special Issue 24, April 2016

in Experiment II), ACK collisions can be observed, and it is verified that the ACK detection scheme is effective. Based on the test, it can be concluded that the ACK

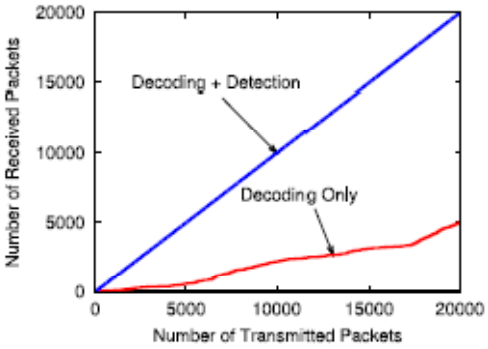


Fig. 11. Measurements in outdoor environment with similar signal strengths.

TABLE 2
Bit-Rate with Respect to Transmission Range

Bit-rate (Mbps)	54	48	36	24	18	12	9	6
Min Sensitivity (dBm)	−65	−66	−70	−74	−77	−79	−81	−82
Tx Range (m)	40	45	70	110	160	200	250	280

detection is insensitive to client mobility, and configuring all APs to the same MAC address is feasible.

7. Position Verification Computation

The position computation for the proposed protocol is based on triangulation calculations. In Fig. 3, node A wants to verify node C's location; however, direct communication is not possible due to the existence of an obstacle. While node B can communicate directly with both A and C, each node knows its GPS position (x,y) in a two-dimensional plane. Node A sends a request to node B to verify location C with its announced position (xc,yc) and mobility vector. B can verify C's location by determining its distance using radio measurements, such as RSSI, and comparing the announced and measured values. If both values are a match, B will send a response back to A containing the distance d_{bc} and verifying the location of C. Once received, A verifies dab (using the radio measurement) and calculates the angle θ between$\overrightarrow{BA}$ and$\overrightarrow{BC}$, where

$$\theta = \arccos(\overrightarrow{BA} \cdot \overrightarrow{BC}).$$

A will then calculate its distance d_{ac} from C using the calculated values d_{bc}, dab, and θ as follows:

Node A now has the distance to C using RSS computation $d_{ac}$and the information from the last record update D_{ac}.

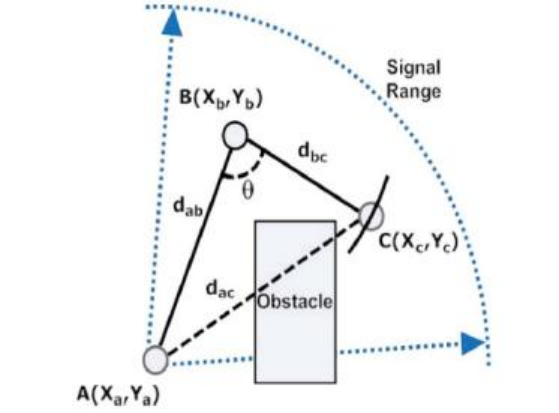


Fig. 3. Estimating the distance between two nodes using a third common neighbor node.

ISSN 2394-3777 (Print)
ISSN 2394-3785 (Online)
Available online at www.ijartet.com
International Journal of Advanced Research Trends in Engineering and Technology (IJARTET)
Vol. 3, Special Issue 24, April 2016

Fig. 3.Estimating the distance between two nodes using a third common neighbour node.

However, due to mobility, the actual position has changed since the information was received. To make a fair comparison of both values, both distances dac and Dac must be adjusted to reflect the change using the acquired mobility information from both the verification and the last record update, respectively. The new estimated location of C is calculated such that´

$$xc = xc + \Delta x \acute{}$$

$$yc = yc + \Delta y$$

TABLE II
NOTATIONS USED IN THE ALGORITHM

Variable	Description
V	*Verifier vehicle*
C	*Claimer (questioned) vehicle*
N_i	*Vehicle* N_i
Loc_i	*Location of node i*
Req_{id}	*Verification request info*
Rep_{id}	*Verification reply info*
G_{id}	*Group ID*
ID_i	*Vehicel i ID*
d_c	*Relative distance to C*
M_i	*Mobility vector for node i*
Hop_{vc}	*Hop counter between V and C*

where Δx and Δy are the changes in C's location caused by mobility, and ´ xc and ´ yc are the estimated new coordinates of C's location. The distance to C's new location with respect to both sources of data is then computed as follows:

$$\acute{}d\,ac = \acute{}((x - \acute{}\,xc)2 + (y - \acute{}\,yc)2)^{1/2}$$

$$\acute{}Dac = ((x - \acute{}\,xc)2 + (y - \acute{}\,yc)2)^{1/2}$$

With two sources of information for the distance to C, both values (´Dac and ´ dac) are compared, and C is verified when both values match or fall within an error range $\Delta v\,\Delta t$, where Δv is the change in C's speed, and Δt is the time difference between the last record update and the time the reply message was received through the verification process; the records will be updated accordingly.

8. Position Verification Algorithm

Based on the aforementioned computation method, we built our protocol algorithm using the notation in Table II. The steps are as follows:

1) Each vehicle maintains a database of its neighbour's information, which is initially gathered and updated by the received beacons or group messages. Location and mobility information are monitored to detect inconsistencies, such as unpredicted changes in a node location, mismatches in received information, or expired records. In any such event, the system will trigger the verification process.

2) When an inconsistency is detected, node V is triggered to verify a questioned neighbour C from its list. If V cannot verify C using direct communication or interference is causing calculation errors, then the node will send a verification request Req to its direct neighbours. The Req

ISSN 2394-3777 (Print)
ISSN 2394-3785 (Online)
Available online at www.ijartet.com
International Journal of Advanced Research Trends in Engineering and Technology (IJARTET)
Vol. 3, Special Issue 24, April 2016

message contains {Reqid,Gid,IDc,Locc,Mc,IDv, Locv,Mv}

Algorithm 1 Request for verification

1:if data inconsistency detected then

2: Verification is triggered

3: if NLOS(C) is True then No direct LOS with C

4: msg ← Reqc

5: Send(msg)

6: To one-hop neighbors

7: StartWaitTimer

8: end if

9:end if

3) If a node Ni receives the request, it will first verify the sender by checking its existence in its neighbourhood list. It will then check to determine whether it has a direct communication with C. If it also does not have a direct communication with C, it will mark C in its table as a node to be verified and forwards the message to C. Before forwarding the message, node Ni listens to its neighbours and checks to determine whether any of them has forwarded the same message. If it has been forwarded, the node will ignore the forwarding process and wait for a reply. If it was not forwarded and a maximum number of hops were not reached, it will forward the message. The forwarded message contains the original request, adds (piggybacks) its information as a sender, and updates the hop count. If a reply is not received after a certain time, the message will be discarded, and the record for C will be deleted .Algorithm 2 Received a request message

1:receive(Reqmsg) 2:if verify msg sender then 3: if Group = Gid then 4: if NLOS(C) is True then

280 IEEE TRANSACTIONS ON VEHICULAR TECHNOLOGY, VOL. 61, NO. 1, JANUARY 2012

5: No direct LOS with C

6: Mark C for update

7: Update processed requests

8: Update(Reqc)

9: msg ← Reqc

10: Forward(msg)

11: To one-hop neighbors

12: else Direct comm. is available

13: if V erify(C) then Algorithm 3

14: msg ← (Repc,Cid,Locc,Mc,dc,Hopvc)

15: Reply msg

16: Send reply msg

17: end if 18: end if

19: end if

20: end if

ISSN 2394-3777 (Print)
ISSN 2394-3785 (Online)
Available online at www.ijartet.com
International Journal of Advanced Research Trends in Engineering and Technology (IJARTET)
Vol. 3, Special Issue 24, April 2016

4) If the request reaches a node Ni with direct communication, it will measure its distance dc from C by measuring the RSS. Once measured, Ni com- pares the measured distance with the distance calculated from the announced position information. If both distances are equal, Ni sends a reply Rep to V with a message containing {Reqid,Gid,Nid,Locn,Mn, dnc,Cid,Locc,Mc,Hopvc}.

Algorithm 3 Verify claimed position

1:if NLOS is False then

2: Measure RSSc

3: Compute dc From RSS

4: Compute dnc From announced data

5: if dc = dnc then

6: return(True,dc)

7: end if

8:else

9: if Hopnc> 1 then

10: Compute θ

11: Compute distance to sender

12: Compute dc From RSS

13: Compute dnc From announced data

14: if dc = dnc then

15: return(True,dc)

16: end if

17: end if

18:end if

5) When a node Ni receives a reply message, it will verify the sender and determine whether it processed the related request. If the request was processed, it will compute and verify the distance to the sender from the received signal and then compute its distance from C. If the distance matches the information in the table, it will mark the record as updated and adds a flag that the node has an NLOS. If the node Ni is not the request originator V , it will forward the reply to V and update the value of dc with its own. A node may receive replies from different 6: Mark C for update 7: Update processed requests 8: Update(Reqc) 9: msg ← Reqc 10: Forward(msg) 11: To one-hop neighbors 12: else Direct comm. is available 13: if V erify(C) then Algorithm 3 14: msg ← (Repc,Cid,Locc,Mc,dc,Hopvc) 15: Reply msg 16: Send reply msg 17: end if 18: end if 19: end if 20: end if

4) If the request reaches a node Ni with direct communication, it will measure its distance dc from C by measuring the RSS. Once measured, Ni com- pares the measured distance with the distance calculated from the announced position information. If both distances are equal, Ni sends a reply Rep to V with a message containing {Reqid,Gid,Nid,Locn,Mn, dnc,Cid,Locc,Mc,Hopvc}.

ISSN 2394-3777 (Print)
ISSN 2394-3785 (Online)
Available online at www.ijartet.com
International Journal of Advanced Research Trends in Engineering and Technology (IJARTET)
Vol. 3, Special Issue 24, April 2016

5) When a node Ni receives a reply message, it will verify the sender and determine whether it processed the related request. If the request was processed, it will compute and verify the distance to the sender from the received signal and then compute its distance from C. If the distance matches the information in the table, it will mark the record as updated and adds a flag that the node has an NLOS. If the node Ni is not the request originator V , it will forward the reply to V and update the value of dc with its own. A node may receive replies from different

neighbours, which increases the distance computation confidence. If the distance does not match or is not within the acceptable range criteria (within physical communication range and road limits), it will ignore the message and delete the record for C To evaluate the proposed protocol, we used Network Simulator-2 (NS-2) ver. 2.34 [25], which is an open-source network communication simulator that has been used and accepted by many researchers. In this section, we will discuss our simulation environment setup and parameters and highlight our experiment's methodology.

Algorithm 4 Received a verification reply

1:receive(Rep msg)

2:if verify msg sender then

3: if Group = Gid then

4: if V erify(C) then Algorithm 3

5: Update local tables

6: if I'm not the originator then

7: Update(Repv,dc)

8: msg ← Repv

9: Send(msg) Forward msg

10: end if

11: end if

12: end if

13:end if

A. Obstacle and Mobility Model

One of the main challenges in VANET simulation is realistic mobility and propagation with obstacle effects. In NS-2, there are three types of propagation models: 1) free space; 2) two-ray ground reflection; and 3) shadowing propagation. These propagation models do not fulfill our requirements to simulate our protocol because they are used for line-of-sight communication between wireless nodes. For our work, we need to simulate obstacles that present road vehicles with their own mobility and object dimensions. To overcome this limitation, we have developed our own obstacle model. To determine whether a line of sight is obstructed by an object or not, we need to determine whether the obstacle lies between the sender and the receiver. To do so, as shown in Fig. 4, we present the object as a line segment from its

ISSN 2394-3777 (Print)
ISSN 2394-3785 (Online)
Available online at www.ijartet.com
International Journal of Advanced Research Trends in Engineering and Technology (IJARTET)
Vol. 3, Special Issue 24, April 2016

front end (x3,y3) to its back end (x4,y4). We also present the line of sight between the sender (x1,y1) and receiver (x2,y2) as another line segment. A NLOS condition occurs where the two line segments intersect. To maintain obstacle mobility, the obstacle's front end (x3,y3) is attached to a vehicle node that is marked as an obstacle, such as a truck. The back end of the obstacle is calculated based on the vehicle location, moving direction, and length of the obstacle. In our simulation, we used an obstacle length of 10–15 m. In our experiments, we consider an NLOS condition to be a total signal block that results in a message drop.

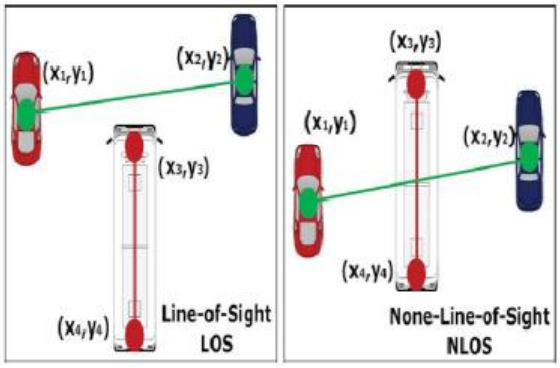


Fig. 4. Obstacle (bus) blocking the line of sight of two cars.

TABLE III
SIMULATION AND EXPERIMENT PARAMETERS

Parameter	Value Setting (s)
Radio Propagation	*Two-ray ground, Nakagami*
Antenna Type	*Omni antenna*
MAC Layer	802.11p
Radio Range	300*m*
Beacon Freq	1 *Hz*
Max Hop	4
Data Rate	6 *Mbps*
Packet Payload	152 *byte*
Number of Vehicles	100–1000
Speed Limits (Highway)	0–100*km/h*
Road length (Highway)	20*km*
Simulation Time	15–30*Min*

As for mobility, we used the traffic and network simulation environment (TraNs) [26] to generate realistic mobility traces for NS-2. TraNsparses traffic simulation movement from the simulation of urban mobility (SUMO) and generates a trace file that can be easily imported to NS-2. The generated traffic supports realistic VANET characteristics, including collision- free movement, lane changes, maintaining distance between vehicles, and the right of way rule, which includes traffic lights. Using the TraNs map importing features, we used maps of highway 417 in Ottawa, ON, Canada, to simulate a representative highway environment. Table III summarizes the parameters used in these simulations

9. System Performance Simulation

9.1 Simulation Setup

In order to measure performance of large-scale systems, we develop a simulator based on MATLAB as well as its communication toolbox, and carry out extensive simulations to evaluate the performance of the entire system. In the simulations, APs are deployed

ISSN 2394-3777 (Print)
ISSN 2394-3785 (Online)
Available online at www.ijartet.com
International Journal of Advanced Research Trends in Engineering and Technology (IJARTET)
Vol. 3, Special Issue 24, April 2016

uniformly along a road. The backhaul is organized into a four-layer tree structure, in which each parent node has five child nodes. Each node only generates UDP traffic. A variant of ARF is adopted as the rate control mechanism in SWIMMING. If the number of consecutive successful transmissions reaches the threshold, the bit-rate is raised to the next upper level. On the contrary, if the number of consecutive failures reaches the threshold, the bit-rate drops to the next lower level. All wireless nodes operate in IEEE 802.11a mode, and the transmission power is set to 100 mW (20 dBm). The corresponding transmission range of each bit-rate level is shown in Table 2. Default values of other parameters are listed in Table 3. The packet loss rate is computed as follows. At first, a randomly-generated bit stream is modulated using a certain modulation scheme. The modulation scheme is selected according to IEEE 802.11a standard. For instance, if the bit- rate is 6 Mbps, the modulation is BPSK; while if the bit-rate is 54 Mbps, the modulation is 64-QAM. The following path- loss model [26] is adopted in the simulations:

$$PL_{model}|_{dB}=-20\log10(c_0/4\pi f)+n_{att.}10.\log_{10}(d) \quad (10)$$

where c0 is the speed of electromagnetic waves, f is the carrier frequency, d is the distance between the transmitter

TABLE 3
Default Values of Parameters in Simulations

Physical Meaning	Value
Vehicle speed	20 m/s
AP interval	100 m
Road length	5000 m
Data frame length	1500 bytes
ACK frame length	14 bytes
DPR frame length	64 bytes
Slot time	9 μs
SIFS time	16 μs
DIFS time	34 μs
Average backoff time	62.7 μs
Preamble duration	20 μs
PLCP header duration	4 μs
Rate control threshold	5
Tx power	100 mW

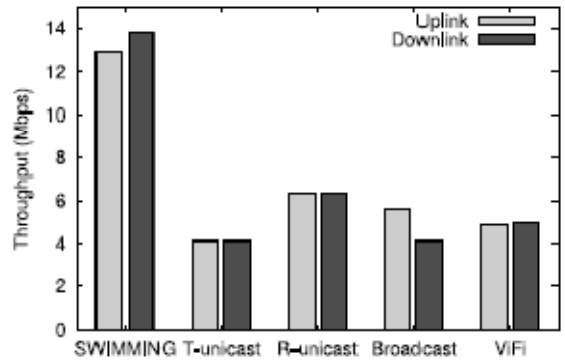


Fig. 12. Throughput comparison.

and the receiver, and natt is the attenuation coefficient. The value of natt is set to 1:8 according to the measurements in [26]. After the modulated bit stream is transmitted through a Rayleigh channel, noise is added into it. After demodulating the bit stream with noise, a new bit stream is obtained. By comparing the new bit stream with the original one, the uncoded bit error rate (BER) is computed. Next, a bit stream is generated randomly, and is encoded using convolutional code as the channel coding technology. Consider bit errors occur in transmission, a number of randomly-chosen bits in the encoded bit stream are inverted.

ISSN 2394-3777 (Print)
ISSN 2394-3785 (Online)
Available online at www.ijartet.com
International Journal of Advanced Research Trends in Engineering and Technology (IJARTET)
Vol. 3, Special Issue 24, April 2016

The proportion of the inverted bits is equal to the uncoded BER. A Viterbi decoder is used to decode the bit stream with errors, and the encoded BER is obtained by contrasting the new and the original bit streams. Based on the encoded BER, the packet loss rate is deduced. If the speed of a vehicle is 30 m/s (108 km/h) and the centre frequency of its radio is 5.20 GHz, the Doppler spread incurred by mobility is only 520 Hz, which is much less than the subcarrier spacing (312.5 kHz in IEEE 802.11a). It is inferred that the vehicle-level mobility does not significantly impact packet loss rate, which is in accordance with the observation in [8]. Hence, the Doppler effect is ignored in our simulations. Based on this model, the packet loss rate is only related to transmission distance and bit-rate adaptation. Performance of SWIMMING is compared with four other schemes including the traditional unicast method (T-unicast), the 802.11r-based unicast method (R-unicast), the broadcast method, and ViFi. The client in the T-unicast and R-unicast schemes is associated with one AP at a time. When the client travels out of the transmission range of an AP, it takes several seconds (set to 5 s in the simulations) to scan the channels and re-associate with a newly-selected AP in T-unicast, while such delay is not considered in R-unicast. The two unicast schemes adopt the same rate control mechanism as SWIMMING. In the broadcast method, the client broadcasts its packets at the lowest bit-rate. In this method, the down- link is the same as that of the T-unicast method. WiFi is a scheme proposed in [18], and packets are sent using MAC-layer broadcast.

9.2. Simulation Results

Since channel contention among multiple clients is orthogonal to our solution andfocus on scenarios which include one client under saturation condition. Namely, the client always has packets to transmit or receive. The MAC-layer throughputs of both uplink and down- link communications are measured. As depicted in Fig. 12, both uplink and downlink throughputs of SWIMMING are remarkably higher than other schemes. Although DPRs incur extra overhead (about 4 percent) for downlink communications

comparative methods, we firstly

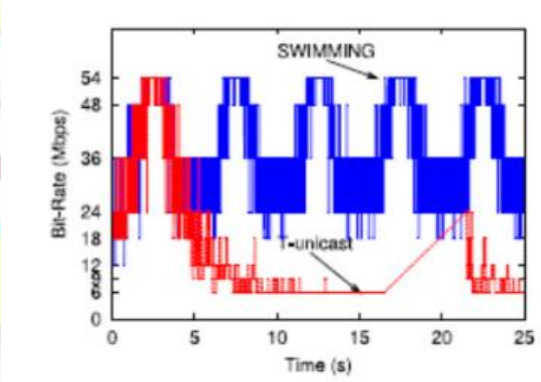


Fig. 13. Bit-rate variation during the transmission.

, the downlink throughput of SWIMMING is even a little higher than its uplink throughput. This is because the DPRs can probe channels between the client and the APs, and unsuccessful transmissions are greatly reduced. Since the length of DPR is much shorter than a normaldatapacket,the incurredoverheadisoffsetbyitsbenefit.

ISSN 2394-3777 (Print)
ISSN 2394-3785 (Online)
Available online at www.ijartet.com
International Journal of Advanced Research Trends in Engineering and Technology (IJARTET)
Vol. 3, Special Issue 24, April 2016

Compared with the broadcast and ViFi methods, SWIMMING can easily incorporate rate control mechanism, which dramatically increases the channel utilization efficiency. The throughput gapbetween SWIMMING andR-unicastrootsin AP diversity and opportunistic transmissions. The throughputof T-unicastismuchlowerthanthatof R-unicast because ofthelonghandoffdelay. Since results of uplink and downlink are similar, only the results of uplink are shown in the remainder of the paper. The probability of successful transmissions is higher in SWIMMING,thusthelinkbit-ratetendstostayathigher levels. The bit-rate comparison of a 25-second period between SWIMMING and T-unicast is shown in Fig. 13. In Fig. 13, the communication of T-unicast suffers from an outage (from aboutthe16thsecondtothe21thsecond),whileSWIMMING always keeps continuous communication with relatively highbit-rate. The transmission redundancy ratios of these schemes are shown in Table 4, where the redundancy removal mechanism is considered for SWIMMING and the broadcast scheme. The unicast schemes do not incur transmission redundancy, while the broadcast scheme results in a large overheadtothebackhaultransmissions.TheTRRinWiFioriginatesonlyfromtheredundantrelays,soitisusuallylow.The overheadcausedbySWIMMINGisonly0.26percentforLAN backhaul and 1.62 percent for WMN backhaul. It is much lowerthantheupper-boundcomputedinSection4.2,because the number of APs that receive a packet is much smaller than the theoretical value a due to packet loss. This reflects the advantage of AP diversity in SWIMMING. Such overhead do

TABLE 4
Transmission Redundancy Ratio

	SWIMMING	Unicast	Broadcast	ViFi
TRR_{LAN}	0.26%	0	13.75%	1.35%
TRR_{WMN}	1.62%	0	72.47%	1.35%

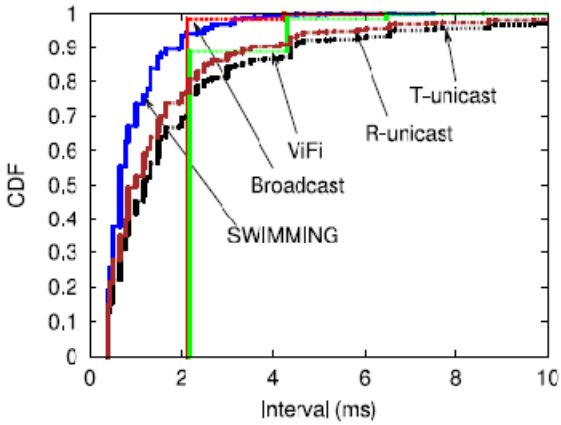


Fig. 14. CDF of intervals between successive successful transmissions.

ISSN 2394-3777 (Print)
ISSN 2394-3785 (Online)
Available online at www.ijartet.com
International Journal of Advanced Research Trends in Engineering and Technology (IJARTET)
Vol. 3, Special Issue 24, April 2016

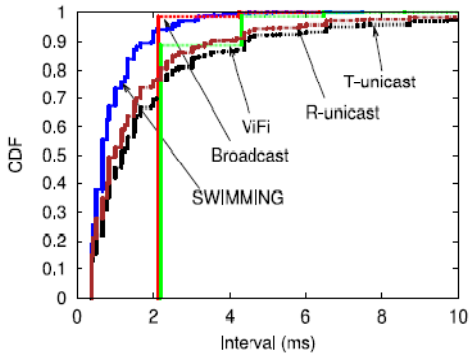


Fig. 14. CDF of intervals between successive successful transmissions.

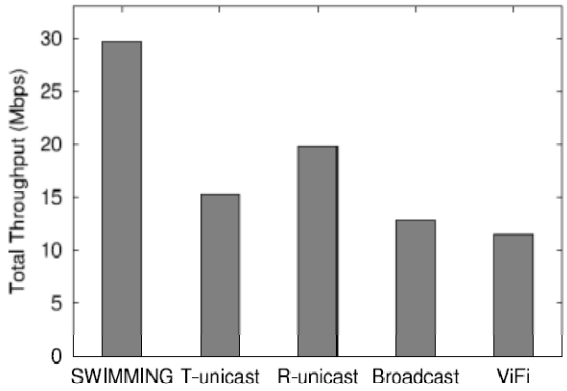


Fig. 17. Total throughput of multiple moving clients.

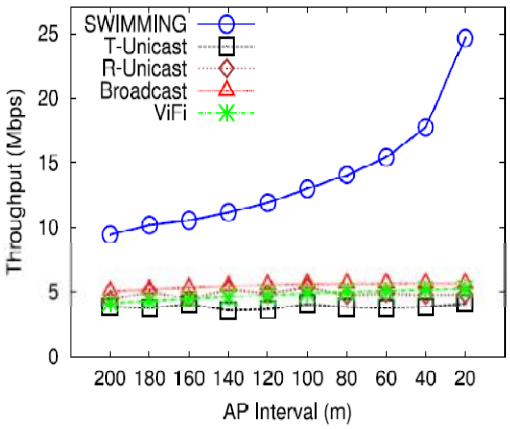


Fig. 15. Throughput with different AP deployment densities.

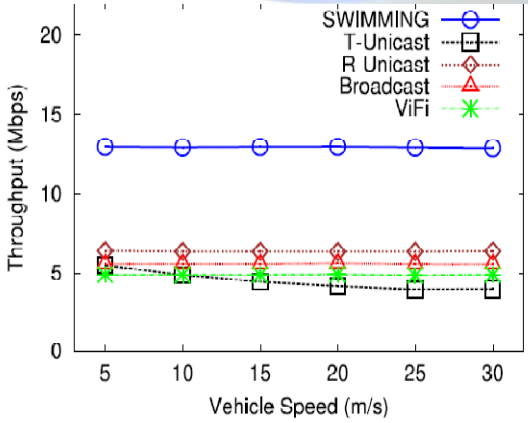


Fig. 16. Throughput with different vehicle speeds.

not impact performance of backhaul, since the bandwidth of backhaullinksaremuchhigherthanaccesslinks . Cumulative distribution function of intervals between two successive successful transmissions is shown in Fig. 14. Most intervals of SWIMMING are shorter than those of other schemes. The result implies that SWIMMING can pro- vide much better quality of service, especially for real-time or interactive applications. With variation of the AP deployment density, the throughputs of the five schemes are shown in Fig. 15. Except for SWIMMING, the other four schemes are not sensitive to the AP density. This result indicates that adding APs to increase diversity is beneficial for SWIMMING, but not for the other schemes. The throughputs with respect to vehicle speed are revealed in Fig. 16. The performance of the T-unicast scheme becomes lower if the vehicle speed increases, due to frequent handoffs and re-associations. No such phenomenon exists in the other four schemes, since handoff delay is minimized in all of them.Finally, a

ISSN 2394-3777 (Print)
ISSN 2394-3785 (Online)
Available online at www.ijartet.com
International Journal of Advanced Research Trends in Engineering and Technology (IJARTET)
Vol. 3, Special Issue 24, April 2016

scenario with multiple moving clients is simulated. In this scenario, five vehicles travel in the same direction along the road, and their speeds vary from 10 to 30 m/s. Their starting points are selected randomly. The interference range of each client is set to 400 meters. A client has to con- tend a channel with other clients located within its interference range, if they operate on the same channel. With T-unicast and R-unicast schemes, adjacent APs are assumed to be set to non-overlapping channels. Total throughputs of these moving clients with various approaches are shown in Fig. 17. The throughputs of T-unicast and R-unicast have significant improvement due toconcurrenttransmissions on different channels. However, these two schemes are still inferior to SWIMMING, because of the high packet loss rate. More- over, if multi-radio multi-channel deployment is applied, the total throughput of SWIMMING will achieve a further enhancement.

CONCLUSION:

Obstacles can have a negative effect on drivers' real-time traffic hazard awareness, which will affect some critical safety transactions such as merging with traffic, responding to sudden traffic pattern changes, and blind spot awareness. Wi-Fi-based Internet access for moving vehicles it consists of innovative protocols in both uplink and downlink. A state of NLOS between two vehicles may result in ignoring each other's existence while they are just a few meters apart.We believe that neighbour hood awareness is essential to supporting reliability and integrity in VANET applications. Current VANET location verification solutions assume that direct communication among vehicles is available. In this paper, we presented a collaborative protocol to verify an announced position when direct communication between the questioned node and the verifier is not possible. In addition to verifying a node location in a multihop cooperative approach, several security measures were included to improve themessage integrity. Seamless roaming of clients was gracefully achieved, while channel utilization efficiency was dramatically improved. Experimental results from both real testbed and simulations revealed feasibility and effectiveness.

ACKNOWLEDGMENTS The work of Pin Lv, XiuhuiXue and Ming Xu was sup- ported in part by the National Natural Science Foundation of China (NSFC) under Grant 61070211 and in part by the PhD Programs Foundation of the Ministry of Education (MOE) of China under Grant 20104307110004. The research work of Xudong Wang was supported by NSFC under Grant 61172066 and Oriental Scholar Program of Shanghai Municipal Education Commission. The authors would like to thank these sponsors for their generous support. The work of Pin Lv and XiuhuiXue was done while they were visiting the Wireless and Networking Lab at UM-SJTU Joint Institute, Shanghai Jiao Tong University. X. Wang is the corresponding author.

ISSN 2394-3777 (Print)
ISSN 2394-3785 (Online)
Available online at www.ijartet.com
International Journal of Advanced Research Trends in Engineering and Technology (IJARTET)
Vol. 3, Special Issue 24, April 2016

REFERENCES

[1] Cisco visual networking index: Global mobile data traffic forecast update. (2011–2016) [Online]. Available: http://www.cisco.com/ en/US/solutions/collateral/ns341/ns525/ns537/ns705/ns827/ white_paper_c11–520862.html [2] A. Aijaz, H. Aghvami, and M. Amani, "A survey on mobile data offloading: Technical and business perspectives," IEEE Wireless Commun., vol. 20, no. 2, pp. 104–112, Apr. 2013. [3] A. Balasubramanian, R. Mahajan, and A. Venkataramani, "Augmenting mobile 3g using wifi," in Proc. ACM 8th Int. Conf. Mobile Syst, Appl. Services, 2010, pp. 209–222. [4] P. Rodriguez, R. Chakravorty, J. Chesterfield, I. Pratt, and S. Banerjee, "Mar: A commuter router infrastructure for the mobile internet," in Proc.ACM2ndInt.Conf.MobileSyst.,Appl.Services,2004,pp.217–230. [5] B. Chen and M. Chan, "Mobtorrent: A framework for mobile internet access from vehicles," in Proc. IEEE INFOCOM, 2009, pp. 1404–1412. [6] V. Bychkovsky, B. Hull, A. Miu, H. Balakrishnan, and S. Madden, "A measurement study of vehicular internet access using in situ wi-fi networks," in Proc. ACM 12th Annu. Int. Conf. Mobile ComputNetw., 2006, pp. 50–61. [7] R. Mahajan, J. Zahorjan, and B. Zill, "Understanding wifi-based connectivity from moving vehicles," in Proc. 7th ACM SIGCOMM Conf. Internet Meas., 2007, pp. 321–326. [8] F. Bai, D. Stancil, and H. Krishnan, "Toward understanding characteristics of dedicated short range communications (DSRC) from a perspective of vehicular network engineers," in Proc. 16th Annu.Int. Conf. Mobile ComputNetw., 2010, pp. 329–340. [9] J. Ott and D. Kutscher, "Drive-thru internet: IEEE 802.11b for 'automobile' users," in Proc. IEEE INFOCOM, 2004, pp. 362–373. [10] J. Eriksson, H. Balakrishnan, and S. Madden, "Cabernet: Vehicular content delivery using wifi," in Proc. ACM 14th ACM Int. Conf. Mobile Comput. Netw., 2008, pp. 199–210. [11] M. Cheung, F. Hou, V. Wong, and J. Huang, "Dora: Dynamic optimal random access for vehicle-to-roadside communications," IEEE J. Sel. Areas Commun., vol. 30, no. 4, pp. 792–803, May 2012. [12] A. Balasubramanian, Y. Zhou, W. Croft, B. Levine, and A. Venkataramani, "Web search from a bus," in Proc. ACM 2nd ACM Workshop Challenged Netw., 2007, pp. 59–66. [13] Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specification Amendment 6: Wireless Access in Vehicular Environments, IEEE Std., 2010. [14] J. Gozalvez, M. Sepulcre, and R. Bauza, "IEEE 802.11p vehicle to infrastructure communications in urban environments," IEEE Commun. Mag., vol. 50, no. 5, pp. 176–183, May 2012. [15] A. Miu, H. Balakrishnan, and C. Koksal, "Improving loss resilience with multi-radio diversity in wireless networks," in Proc. ACM 11th Annu.Int. Conf. Mobile ComputNetw., 2005, pp. 16–30. [16] P. Lv, X. Wang, M. Xu, and Y. Chen, "Network-leading association scheme in IEEE 802.11

ISSN 2394-3777 (Print)
ISSN 2394-3785 (Online)
Available online at www.ijartet.com
International Journal of Advanced Research Trends in Engineering and Technology (IJARTET)
Vol. 3, Special Issue 24, April 2016

wireless mesh networks," in Proc. IEEE Int. Cnf. Commun., 2011, pp. 1–5. [17] N. Ahmed, S. Keshav, and K. Papagiannaki, "Omnivoice: A mobile voice solution for small-scale enterprises," in Proc. 12th ACM Int. Symp. Mobile Ad Hoc Netw.Comput., 2011, pp. 1–11. [18] A. Balasubramanian, R. Mahajan, A. Venkataramani, B. Levine, and J. Zahorjan, "Interactive wifi connectivity for moving vehicles," in Proc. ACM SIGCOMM, 2008, pp. 427–438.

[19] I. Ramani and S. Savage, "Syncscan: Practical fast handoff for 802.11 infrastructure networks," in Proc. IEEE INFOCOM, vol. 1, 2005, pp. 675–684. [20] H. Wu, K. Tan, Y. Zhang, and Q. Zhang, "Proactive scan: Fast handoff with smart triggers for 802.11 wireless lan," in Proc. IEEE INFOCOM, 2007, pp. 749–757. [21] Y. Amir, C. Danilov, M. Hilsdale, R. Musloiu-Elefteri, and N. Rivera, "Fast handoff for seamless wireless mesh networks," in Proc. ACM 4th Int. Conf. Mobile Syst., Appl. Services, 2006, pp. 83–95. [22] Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specification Amendment 2: Fast Basic Service Set (BSS) Transition, IEEE Std., 2008. [23] A. Kamerman and L. Monteban, "WaveLan-II: A highperformance wireless LAN for the unlicensed band," Bell Labs Tech. J., vol. 2, no. 3, pp. 118–133, 1997. [24] S. Wong, H. Yang, S. Lu, and V. Bharghavan, "Robust rate adaptation for 802.11 wireless networks," in Proc. ACM MobiCom, 2006, pp. 146–157. [25] ITU-T Recommendation G. 114, One Way Transmission Time, ITU-T Std., 1996. [26] A. Paier, J. Karedal, N. Czink, C. Dumard, T. Zemen, F. Tufvesson, A. F. Molisch, and C. F. Mecklenbr€auker, "Characterization of vehicle-to-vehicle radio channels from measurements at 5.2 Ghz," Wireless Personal Commun., vol. 50, no. 1, pp. 19–32, 2009.

Pin LvreceivedtheBScdegreefromNortheastern University, China, in 2006, and the PhD degree in computer science from NUDT in 2012. From 2010 till 2012, he was a visiting PhD student with the Wireless and Networking Lab under supervision of ProfXudongWang.HeiscurrentlywiththeCollege of Computer, National University of Defense Tech-nology (NUDT), China. His research interests include wireless networks, network virtualization, cloud computing, etc. He isamemberofthe IEEE.

Xudong Wang received the PhD degree in elec- trical and computer engineering from Georgia Institute of Technology in August 2003, he has been a senior research engineer, senior network architect, and R&D manager in several compa- nies. He is currently with the UM-SJTU Joint Institute, Shanghai Jiao Tong University. He is a distinguished professor (Shanghai Oriental Scholar) and is the director of the Wireless and NetworkinG (WANG) Lab. He is also an affiliate faculty member with the Electrical Engineering Department at the University of Washington. He has been actively involved in R&D, technology transfer, and commercialization of various wireless networking technologies. His research

ISSN 2394-3777 (Print)
ISSN 2394-3785 (Online)
Available online at www.ijartet.com
International Journal of Advanced Research Trends in Engineering and Technology (IJARTET)
Vol. 3, Special Issue 24, April 2016

interests include wire- less communication networks, smart grid, and cyber physical systems. He holds several patents on wireless networking technologies and most of his inventions have been successfully transferred to products. He is an editor for the IEEE Transactions on Mobile Computing, IEEE Trans- actions on Vehicular Technology, Elsevier Ad Hoc Networks, and ACM/ Kluwer Wireless Networks. He was also a guest editor for several jour- nals. He was the demo co-chair of the ACM International Symposium on Mobile Ad Hoc Networking and Computing (ACM MOBIHOC 2006), a technical program co-chair of Wireless Internet Conference (WICON) 2007, and a general co-chair of WICON 2008. He has been a technical committee member of many international conferences and a technical reviewer for numerous international journals and conferences. He is a senior member of the IEEE and was a voting member of IEEE 802.11 and 802.15 Standard Committees.

1096 IEEE TRANSACTIONS ON MOBILE COMPUTING, VOL. 14, NO. 5, MAY 2015

XiuhuiXue received the BSc and MSc degrees from National University of Defense Technology, China, in 2010 and 2012, respectively. His research interests include wireless networks, embedded systems,etc.

Ming Xu received the BSc and MSc degrees from WuhanUniversity,China,in1984and1987,res pec- tively, and the PhD degree from National University of Defense Technology (NUDT), China, in 1995. He isaprofessorandtheheadattheNetworkEngine er- ing Department, College of Computer, NUDT. His recent research interests include wireless mesh net- works, mobile security, wireless sensor networks, and mobile data management. He has published morethan130academicpapersinjournalsandc on- ferences, co-authored of three books. Among them, Mobile Computing Technology is the first book in China mainland containing extensive research results around wireless networks and mobile computing. He isaneditorofIASTEDInternational Journal of Computers& Applications, also an editor of Journal of Communication. He has co-chaired four interna- tional conferences, and been program committee members for over 30 inter- national conferences or workshops. He is a senior member of China ComputerFederation(CCF),andamemberoft heACM,andtheIEEE.

" For more information on this or any other computing topic, please visit our Digital Library at www.computer.org/publications/dlib.