Available Online at www.ijcsmc.com

International Journal of Computer Science and Mobile Computing

A Monthly Journal of Computer Science and Information Technology

ISSN 2320–088X

IJCSMC, Vol. 3, Issue. 5, May 2014, pg.1288 – 1294

RESEARCH ARTICLE

A RELIABLE APPLICATION LEVEL BROADCASTING PROTOCOL FOR VANET

S. Vijayakumar[1], A. Noble Mary Juliet[2], Dr. M.L.Valarmathi[3]

[1]PG Student, Department of CSE, NPRCET, Natham, Tamilnadu

[2]Assistant Professor, Department of CSE, NPRCET, Natham, Tamilnadu

[3]Associate Professor, Department of CSE, GCT, Coimbatore, Tamilnadu

Abstract: Many applications are built on broadcast communications, so efficient routing methods are critical for their success. Here, we develop the Distribution-Adaptive Distance with Channel Quality (DADCQ) protocol to address this need and show that it performs well compared to several existing multihop broadcast proposals. The high cost aggravates the inherent resource constraint problem in MANETs particularly in multimedia wireless applications. To proposal high anonymity protection, we suggest an Anonymous Location-based Efficient Routing protocol (ALERT). It s also called Reliable Application Level Broadcasting (RALB) protocol. RALB dynamically dividers the network field into zones and randomly chooses nodes in zones as intermediate relay nodes, which form a no traceable anonymous route. RALB proposals anonymity protection to sources, destinations, and routes. RALB has policies to successfully counter intersection and timing attacks. We theoretically analyze RALB for anonymity and efficiency. RALB achieves similar routing effectiveness to the GPSR geographical routing protocol. The DADCQ protocol utilizes the distance method to select advancing nodes.The performance of this method be contingent heavily on the value of the result threshold, but it is difficult to choose a value that results in good performance crossways all scenarios. an anonymous communication protocol that can provide intractability is needed to strictly ensure the anonymity of the sender when the sender communicates with the other side of the field Node density, spatial distribution pattern, and wireless channel quality all touch the optimum value. The node recognizes its neighbor as a node that inside the node's radio range. Once the source need to send a packet, it usually stores the position of the destination in the packet header which will help in promoting the packet to the destination without needs to route discovery, route maintenance, or even alertness of the network topology.

Keywords: VANET, Wireless broadcast, statistical broadcast, broadcast storm, anonymity, routing protocol, geographical routing

I. INTRODUCTION

The Distribution Adaptive Distance with channel quality protocol utilizes the distance method to select forwarding nodes.The performance of this method be contingent heavily on the value of the result threshold, but it is difficult to choose a value that results in good performance crossways all scenarios. Node density, spatial distribution pattern, and wireless channel quality all touch the optimum value. The node recognizes its neighbor as a node that inside the node's radio range. Rapid development of Vehicular Ad Hoc Networks (VANETs) has stimulated numerous wireless applications that can be used in a wide number of areas such as commerce, emergency services, military, education, and entertainment. Most of the current approaches are limited by focusing on enforcing anonymity at a heavy cost to precious resources because public-key-based encryption and high traffic generate significantly high costVehicular Ad Hoc Networks (VANETs) and Mobile Ad Hoc Networks (MANETs) use anonymous routing protocols that hide node identities and/or routes from outside observers in order to provide anonymity protection. However, existing anonymous routing protocols relying on either hop-by-hop encryption or redundant traffic either generate high cost or cannot provide full anonymity protection to data sources, destinations, and routes [7].

RALB has approaches to successfully counter intersection and timing attacks. We theoretically analyze ALERT for anonymity and efficiency. ALERT also achieves similar routing efficiency to the GPSR geographical routing protocol. "Identity and location anonymity of sources and destinations" means it is hard if possible for other nodes to obtain the real identities and exact locations of the sources and destinations. For route anonymity, adversaries, either en route or out of the route, cannot trace a packet flow back to its source or destination, and no node has information about the real identities and locations of intermediate nodes en route.

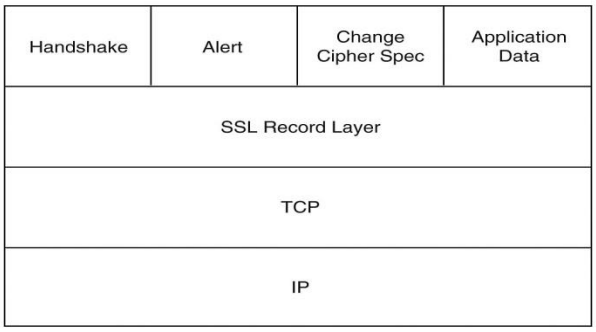


Fig.1.Protocol Layer for ALERT

II. DISTRIBUTION ADAPTIVE DISTANCE WITH CHANNEL QUALITY PROTOCOL

Wireless communications generally and VANET in particular isloss of packets as they traverse the medium. Multipath fadingcauses a signal to interfere with itself as it splits into

multiplepaths due to being reflected off objects in the environment.Packets can also be lost when different transmitted signalsinterfere with each other, a phenomenon called a collision.These effects vary in intensity across space and time and canwork against the design of multihop broadcast protocols. If abroadcast protocol is designed and tested in an environment thatassumes perfectly reliable communications, it could break downwhen fading and collisions are introduced.Often, broadcast protocols must accommodate packetcommunication failures by increasing the number of nodes thatare rebroadcasting source messages.

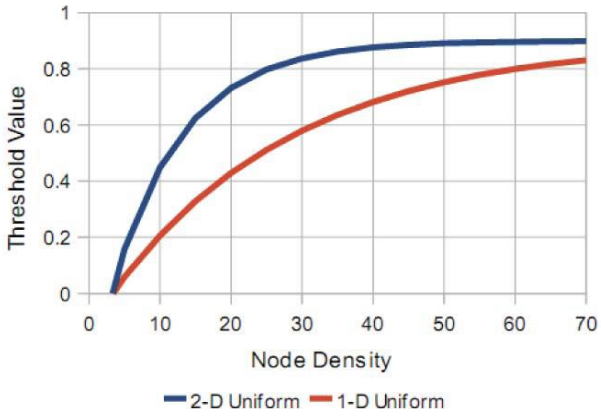
The contributions of this work are summarized as follows:

DADCQ protocol: The primary contribution of this work is the proposed multihop broadcast protocol DADCQ. DADCQ combines local spatial distribution information and other factors with the distance method heuristic to select rebroadcasting nodes. Previous broadcast protocols proposed for ad hoc that make use of the distance method use less comprehensive supplemental information. A key insight proposed here is a methodology for incorporating more information into the protocol. This extra information is used to make the protocols adaptive to more networking scenarios than many previous proposals.

Adaptive threshold function design: This paper gives a novel design strategy for a decision threshold function. Threshold functions are a critical component of many multihop broadcasting methods, such as stochastic broadcast (gossiping), the counter method, the distance method, and the location method [4]. The proposed design scheme builds a threshold function using three independent input variables chosen to allow the threshold to be adaptive to the environmental conditions of primary interest. These variables measure local node density, the distribution pattern of nearby nodes, and the wireless channel quality. Thus, the resulting threshold function of these three inputs causes the protocol to operate efficiently across a broad range of conditions.

Quadrate method for spatial distribution characterization: One of the factors used to compute the rebroadcasting decision threshold in DADCQ is local node distribution pattern. This work is the first to propose that the quadrate method of spatial statistics be used to characterize the spatial distribution of nodes for use in a multihop broadcast protocol. Because distribution pattern may affect the behavior of many multihop broadcast methods, this contribution may be applicable in a wider context as well.

Analysis of behavior with respect to threshold value: This paper presents original results addressing the nature of the threshold value used in the distance method. We show that system performance exhibits a phase transition with respect to the threshold value and suggest that an optimal threshold value should cause the system to operate in the supercritical region of performance as close to the transition region as possible.



Advantage of RALB and Distance based protocol

Statistical broadcast protocols typically do not use this rapidlychanging neighborhood information. Statistical protocolsmeasure the value of one or more locally available variablesand make a decision to rebroadcast based on the measuredvalue and a cutoff threshold. For example, the statistical methodused in this work, the distance method, measures the distance tothe nearest neighbor from which a node has received thebroadcast message. If that distance is greater than a thresholdvalue, then the node rebroadcasts the message.

The threshold value is calculated as a function of more slowly changingtopological factors such as node density and spatial distributionpattern [4].The advantage of the ALERT offers anonymity protection to sources, destinations, and routes. It also has strategies to effectively counter intersection and timing attacks. To offer high anonymity protection at a low cost

The contribution of this work includes:
1. *Anonymous routing*. RALB provides route anonymity, identity, and location anonymity of source and destination.
2. *Low cost*. Rather than relying on hop-by-hop encryption and redundant traffic, RALB mainly uses randomized routing of one message copy to provide anonymity protection.
3. *Resilience to intersection attacks and timing attacks*. RALB has a strategy to effectively counter intersection attacks, which have proved to be a tough open issue [16]. RALB can also avoid timing attacks because of its no fixed routing paths for a source destination pair.
4. *Extensive simulations*. We conducted comprehensive experiments to evaluate RALB's performance in comparison with other anonymous protocols.

III. AN ANONYMOUS LOCATION-BASED EFFICIENT ROUTING PROTOCOL

PACKET FORMAT OF ALERT:

For successful communication between S and D, S and each packet forwarder embeds the following information into the transmitted packet.
1. The zone position of ZD, i.e., the Hth partitioned zone.

2. The encrypted zone position of the Hth partitioned zone of S using D's public key, which is the destination for data response.
3. The current randomly selected TD for routing.
4. A bit (i.e., 0/1), which is flipped by each RF, indicating the partition direction (horizontal or vertical) of the next RF. With the encrypted Hth partitioned zone in the information of (2)

1. Capabilities. By eavesdropping, the adversary nodescan analyze any routing protocol and obtain informationabout the communication packets in theirvicinity and positions of other nodes in the network.They can also monitor data transmission on the flywhen a node is communicating with other nodesand record the historical communication of nodes.They can intrude on some specific vulnerable nodesto control their behavior, e.g., with denial-of-service(DoS) attacks, which may cut the routing in existinganonymous geographic routing methods [6].

2. In capabilities. The attackers do not issue strong activeattacks such as black hole. They can only performintrusion to a proportion of all nodes. Theircomputing resources are not unlimited; thus, bothsymmetric and public/private key cannot be brutallydecrypted within a reasonable time period. Therefore, encrypted data are secure to a certaindegree when the key is not known to the attackers [7].

IV. PARAMETERS

We use the following metrics to evaluation the routingperformance in terms of effectiveness on anonymityprotection and efficiency [10]:

1. *The number of actual participating nodes*. These nodesinclude RFs and relay nodes that actually participatein routing. This metric demonstrates the ability ofALERT's randomized routing to avoid routingpattern detection [11].
2. *The number of random forwarders*. This is the numberof actual RFs in an S-D routing path. It shows routinganonymity and efficiency [10].
3. *The number of remaining nodes in a destination zone*.This is the number of original nodes remaining in adestination zone after a time period. A largernumber provides higher anonymity protection to adestination and to counter the intersection attack.We measure this metric over time to show effectivenesson the destination anonymity protection [12].
4. *The number of hops per packet*. This is measured as theaccumulated routing hop counts divided by thenumber of packets sent, which shows the efficiencyof routing algorithms.
5. *Latency per packet*. This is the average time elapsedafter a packet is sent and before it is received. Itincludes the time cost for routing and cryptography.This metric reflects the latency and efficiency ofrouting algorithms.
6. *Delivery rate*. This is measured by the fraction ofpackets that are successfully delivered to a destination.It shows the robustness of routing algorithms toadapt to mobile network environment.

V. THEORETICAL ANALYSIS OF ALERT

In this section, we theoretically analyze the anonymity androuting efficiency properties of ALERT. We analyze thenumber of nodes that can participate in routing thatfunction as camouflages for routing nodes. We estimatethe number of RFs in a routing path, which shows the routeanonymity degree and routing efficiency of ALERT. Wecalculate the anonymity protection degree of a destinationzone as time passes to demonstrate ALERT's ability tocounter intersection attacks [9] [10].

VI. CONCLUSION

We present Distribution based protocol for multihop Broadcast thewarning messages in VANETs [2]. It provides highreachability and efficient use of bandwidth in both urban andhighway scenarios with varying node density and fadingintensity. The simulation results show that our system outperforms than previously used methods. This protocol hasproved that extremely effective when the density of vehicles ishigh, especially in maps with low density of streets andjunctions [3]. Our proposed method also performs well in all thescenarios like urban, sub-urban and highway updated. A packet in ALERTincludes the source and destination zones rather than theirpositions to provide anonymity protection to the source andthe destination. ALERT further strengthens the anonymityprotection of source and destination by hiding the datainitiator/receiver among a number of data initiators/receivers. It has the "notify and go" mechanism for sourceanonymity, and uses local broadcasting for destinationanonymity. In addition, ALERT has an efficient solution tocounter intersection attacks. ALERT's ability to fight againsttiming attacks is also analyzed. Experiment results showthat ALERT can offer high anonymity protection at a lowcost when compared to other anonymity algorithms. It canalso achieve comparable routing efficiency to the base-lineGPSR algorithm.

REFERENCES

1) F. Ye, R. Yim, J. Guo, J. Zhang, and S. Roy,"Prioritized Broadcast Contention Control inVANET," Proc. IEEE Int'l Conf. Comm. (ICC), pp. 1-5, May 2010.

2) J. Cartigny, D. Simplot, and J. Carle, "StochasticFlooding Broadcast Protocols in Mobile WirelessNetworks," technical report, Universite´ des Scienceset Technologies de Lille 1, http://citeseer.ist.psu.edu/525199.html, May 2002

3) S. Biswas, R. Tatchikou, and F. Dion, "Vehicle-to-Vehicle Wireless Communication Protocols forEnhancing Highway Traffic Safety," IEEE Comm.Magazine, vol. 44, no. 1, pp. 74-82, Jan. 2006.

4) Y. Bi, L. Cai, X. Shen, and H. Zhao, "A Cross LayerBroadcast Protocol for Multihop Emergency MessageDissemination in Inter-Vehicle Communication,"Proc. IEEE Int'l Conf. Comm. (ICC), pp. 1-5, May2010

5) Y. Li, K. Moaveninejad, and O. Frieder, "RegionalGossip Routing for Wireless Ad Hoc Networks,"Mobile Network Applications, vol. 10, nos. 1/2, pp.61-77, 2005

[6] K.E. Defrawy and G. Tsudik, "PRISM: Privacy-Friendly Routingin Suspicious MANETs (and VANETs)," Proc. IEEE Int'l Conf.Network Protocols (ICNP), 2008.
[7] Y.-C. Hu, A. Perrig, and D.B. Johnson, "Ariadne: A Secure On-Demand Routing Protocol for Ad Hoc Networks," WirelessNetworks, vol. 11, pp. 21-38, 2005.
[8] I. Aad, C. Castelluccia, and J. Hubaux, "Packet Coding for StrongAnonymity in Ad Hoc Networks," Proc. Securecomm and Workshops,2006.
[9] C.-C. Chou, D.S.L. Wei, C.-C. Jay Kuo, and K. Naik, "An EfficientAnonymous Communication Protocol for Peer-to-Peer Applicationsover Mobile Ad-Hoc Networks," IEEE J. Selected Areas inComm., vol. 25, no. 1, pp. 192-203, Jan. 2007.
[10] X. Wu, "AO2P: Ad Hoc On-Demand Position-Based PrivateRouting Protocol," IEEE Trans. Mobile Computing, vol. 4, no. 4,pp. 335-348, July/Aug. 2005.
[11] B. Zhu, Z. Wan, M.S. Kankanhalli, F. Bao, and R.H. Deng,"Anonymous Secure Routing in Mobile Ad-Hoc Networks," Proc.IEEE 29th Ann. Int'l Conf. Local Computer Networks (LCN), 2004.

