Available online at http://www.journalcra.com

International Journal of Current Research
Vol. 5, Issue, 08, pp.2218-2221, August, 2013

INTERNATIONAL JOURNAL OF CURRENT RESEARCH

ISSN: 0975-833X

RESEARCH ARTICLE

THE NEW NOVEL FOR REDUCING OVER HEAD IN AOMDV PROTOCOL USING KERNAL ADATRON ALGORITHM

***Revathi, J., Kokila, N. and Suganthi, S.**

Department of Computer Science, Vivekanandha College of Arts and Sciences for Women (Autonomous),
Elayampalaya Tiruchengode – 637 205

ARTICLE INFO

Article History:
Received 15th May, 2013
Received in revised form
20th June, 2013
Accepted 22nd July, 2013
Published online 23rd August, 2013

Key words:

Overhead, KA algorithm,
AOMDV-DPU, Robust Route, MANET.

ABSTRACT

Wireless networks, and mobile ad-hoc networks (MANETs) in particular, are characterized by time- varying link characteristics and network topology. In such an environment, the network must accommodate the changes, providing end-end packet delivery while at the same time incurring low control overhead. This paper proposes a routing algorithm for MANETs with the primary goal of maximizing connectivity while limiting overhead. The KA algorithms of AOMDV-DPU strengthen the primary route and secondary routes, respectively. As a result, the frequencies of Received Route Requests RREQ, RREP (route replies), and RERR (route error) messages are reduced considerably. As a result, the route breakage probability increases. Node mobility in mobile ad hoc networks (MANETs) causes frequent route breakages and intermittent link stability. In this paper, we introduce a robust routing scheme, known as ad hoc on-demand multipath distance vector with dynamic path update (AOMDV-DPU), for delay-sensitive data transmission over MANET.

INTRODUCTION

Wireless mobile ad-hoc networks (MANETs) are usually bandwidth restricted and characterized by time-varying error-prone channels due to node mobility, consequential in the link loss,[1] route breakage, and short route lifetime. These personalities pose a serious challenge in manipulative efficient routing schemes, especially for supporting the delay-sensitive traffic such as video streaming. They achieve lower average end-to-end packet delay and higher throughput than AODV [2] by using the alternate routes between source and destination when the primary route fails. However, high node mobility may cause the routes to break frequently forcing the source to switch between routes or rediscover new routes, which increases both packet losses and latency. To counter it, the use of better routing metrics has been proposed in the literature, including the received signal strength indicator (RSSI) along with hop count. Various route maintenance mechanisms have also been investigated in the literature, which avoid the need to use costly route discovery. The logical solution to reduce this overhead would be to use a hierarchical structure like the used in Internet, in which the nodes are aggregated into subnets to be handled as a single entity for routing purposes. However, this structure is difficult to apply in MANETs due to their dynamic and distributed nature. The main problems to solve in such hierarchical structure are the address acquisition under mobility scenarios, the dynamic creation and removal of subnets and the intendances of already established sessions when a node moves from one subnet to other and changes its [3] IP address. We are proposing a scheme, which takes advantage of the fact that currently the nodes in MANETs can be grouped following physical or environmental constraints to apply this hierarchical structure. These formed clusters can be considered subnets of a MANET, giving the chance of representing multiple routes of a large number of nodes by a single route. Since the routing information is cutting down, a reduction in the overhead may be obtained. We investigate braided routing from more than a few different viewpoints in order to fully explore and understand its properties. We analytically characterize the reliability (the likelihood that the source and destination nodes have a at the same time path) of a class of braids, their optimality properties, encounter-examples to conjectured optimality properties in a well-structured network. We also compare the steadfastness of braided, disjoint-path, and full-network routing in simulations in both torus and random networks.

Related work

To reduce the number of route detection appropriate to route failures in AOMDV, a scheme is obtainable in to continue all the paths by means of episodic update packets. These update packets assess the RSSI [4] in each hop along the alternate paths and only the path with the strongest received signal strength is used for data transmission. The scheme discussed in builds two paths between source and destination and creates backup paths during route answer back, route preservation, and local recovery process to improve the data transfer and fault tolerance. In AOMDV-APLP multiple paths are generated by ease of understanding forecast,[5] from which the route with the strongest signal strength is selected depending on the link life value predicted by a link breakage prediction technique. Enhanced AOMDV reduces the route failure by preemptively predicting link failures based on the signal strength at a receiver. In MANETs, packet transmission is impaired by radio link fluctuations. The channel-aware AOMDV (CA-AOMDV) uses a received signal strength entrance of the channel to select stable links for path discovery and apply a anticipatory handoff strategy to maintain reliable connections by exploiting the channel state information. Several other on-demand multipath protocols were also reviewed. In this set of experiments, the packet generation rate varies from 0.25 to 2 packets/s for each

Corresponding author: Revathi, J.,
Department of Computer Science, Vivekanandha College of Arts and Sciences for Women (Autonomous), Elayampalaya Tiruchengode – 637 205

connection, the average node speed is 5m/s, and 50 source destination pairs are activated in order to compare the results. The minimum offered load is 50kb/s and the maximum load is 400kb/s. As the AOMDV-DPU scheme achieves significantly lower (place loss routing) PLR than the AOMDV scheme for all the packet generation rates with maximum difference of 15% and 12% at 2 packets/s for the delay-agnostic and delay-sensitive [6] traffic, respectively. For the proposed scheme, the PLR is relatively high at low packet generation rates because the packets are also generated at a low rate and therefore tracking SR (Source Routing) nodes becomes difficult. As a result, the route breakage probability increases. As the packet rate increases, the LPU process becomes more effective and PLR decreases.

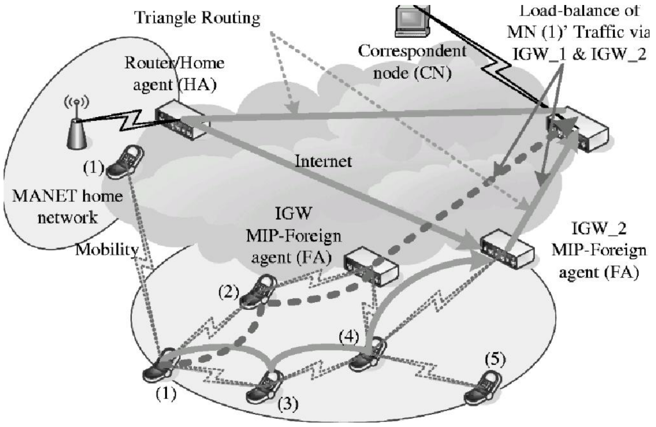

Fig.1. MANET Routing Protocol

That the property of pre-determining an end-to-end route and unicast are two key sources of vulnerability in conventional MANET routing protocols. Owing to the unstable wireless channel, constantly changing network topology, [7] and even malicious nodes' misbehavior, it is very difficult to maintain a deterministic route and discovery and recovery processes are too long. In fact, because of the broadcast nature of a wireless channel, when the next hop node on a route fails to receive the packet or is malicious and drops the packet, its neighbors might have eavesdropped the signal.

Potential Multipath

In case the suboptimal forwarder is out of the range of a better forwarder as illustrated in Fig. 2 (B cannot hear A), it will relay the packet after a certain period of time. Then, the packet will be transmitted through a second path which can be seen as a backup. If the packet reaches a node (C) that has already received the same packet, it will be discarded and the two paths are merged. Otherwise, it may be delivered to the destination (D) independently. Though more resource might be consumed in such potential multipath scenarios, resilience is actually being improved.

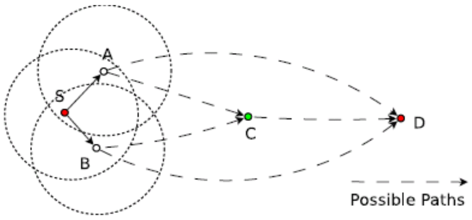

Fig. 2. Multipath in POR

Resilience to Dead-end

In GPSR like geographic routing, a node's negated will lead to gluttonous forwarding's breakdown and such a problem is called a "dead-end" [8]. As illustrated Node A that has no neighbors nearer than itself to the destination D will be selected by Node S as the next hop and thus the greedy forwarding stops. In fact, the packet might be routed through Node B. The spotted area together with the shaded area is called Node A's void area. This 'void' area looks very large for unicast geographic routing. However in POR (Place of Record), due to its multicast mechanism, the spotted area is now covered and is no longer a void zone, leaving only the shaded area where nodes such as Node B can reside. This remaining void zone is therefore much smaller than that of other unicast protocols. In fact, if there are other sub-optimal forwarders, such as Node C nearby, even this small void zone can be partially covered.

Resilience to Selective Forwarding

We only believe discriminating forwarding attack. Spiteful nodes behave like normal nodes most of the time but selectively drop packets. There are two parameters: one is the spiteful nodes' proportion (*pm*) and the other is the probability that a malicious node drops forwarding packets (*pd*). Then there is a probability of *x* = *pmpd* that a data packet will be dropped at every hop. For GPSR and AODV like unicast routing protocols, suppose the percentage of *i* hops transmission is *mi* and the corresponding packet delivery ratio is *Pi*, then the whole packet delivery ratio in normal situations will be

$$P = \sum_{i=1}^{N} m_i P_i \tag{1}$$

Here, we take for granted the least amount number of hops is N. In critical atmosphere with selective forwarding, the ratio will become

$$P_{unicast} = \sum_{i=1} m_i P_i (1-x)^{i-1} \tag{2}$$

Assume $P_i = 1$ $(i = 1, \ldots, N)$ for simplicity, we get

$$P_{unicast} = \sum_{i=1}^{N} m_i (1-x)^{i-1} \tag{3}$$

$$Pr_k = x^{(k-1)}(1-x) \tag{4}$$

Assume on average the *k*-th forwarder relays the packet for successful transmission, then

$$\overline{k} = \frac{\sum_{k=1}^{n} kPr_k}{\sum_{k=1}^{n} Pr_k} \tag{5}$$

Neglecting the collisions and transmission errors, the probability that a packet can be successfully delivered to the destination is:

$$P_{multicast} = m_1 + (1-m_1)[1-x^n]^{(\overline{N}-1)} \tag{6}$$

Here, t0 denotes the packet transmission delay in corresponding normal situations in which both pm and pd are 0. ΔT is the time slot. On the contrary, the transmission delay of unicast routing protocols will be decreased. The reason is the high packet dropping probability will lead to the reduction of the number of hops that the data packet can go any further.

Routing Security, Fairness, and Robustness

In mobile ad hoc networks work as network nodes and relay packets originated by other nodes. Mobile ad hoc networks can work properly only if the participating nodes cooperate in routing and forwarding. For individual nodes it might be advantageous not to cooperate, though. The new routing protocol extensions presented in this paper make it possible to detect and isolate misbehaving nodes, thus making it unattractive to deny cooperation. In the presented scheme, trust relationships and routing decisions are made based on experienced, observed, or reported routing and forwarding behavior of other nodes. A hybrid scheme of selective altruism and utilitarianism is presented to strengthen mobile ad hoc network protocols in their resistance to security attacks, while aiming at keeping network throughput, or good put, high.

The Kernal Adatron Algorithm

We will now outline an efficient algorithm which is straightforward to implement and trains an AOMDV-DPU rapidly. This algorithm the kernel adatron is based on the packets are a also generated at a low rate and therefore tracking SR nodes becomes difficult. As a result, the route breakage probability increases. Node mobility in mobile ad hoc networks (MANETs) causes frequent route breakages and intermittent link stability. In this paper, we introduce a robust routing scheme, known as ad hoc on-demand multipath distance vector with dynamic path update (AOMDV-DPU), for delay-sensitive data transmission over MANET.

1.Initialize x_i=1 y_i=0.
2.Starting from pattern j=1 for labeled points(x_i,y_j) calculate:

$$z_i = \sum_{j=1}^{p} \alpha_j y_j K(x_i, x_j) - \theta$$

3.For all pattern i=1 calculated x_i=$y_i z_j$ and execute step 4 and step 5 belows
4.Let bai =(1-r) be the proposed change to the multipliers ai.
5.If (x_i+y_j)< 0 then x_i=0.
6.If (x_i+y_j)>0 then X←---$_{xii}$.
7.Calculate:

$$\theta = \frac{1}{2}\left(\min\left(z_i^{+}\right) + \max\left(z_i^{-}\right)\right)$$

Where x_i are those pattern j with class label +1 and zi those with class label-1.
8.If a maximum number of presentation of the pattern set has been exceeded or the margin

$$m = \tfrac{1}{2}(\min(z_i^{\bar{+}}) - \max(z_i^{-}))$$

Has been approach 1 than stop.
9.Other Wise return to step 2.

Protocol overhead Performance

Protocol overhead refers to metadata and network routing information sent by an application, which uses a portion of the available bandwidth of a communications protocol. This extra data, making up the protocol headers and application-specific information is referred to as overhead, since it does not contribute to the content of the message. Network overhead is an important concept to understand. Understanding overhead is basic to understanding the methodology employed by various technologies to get information from one place to another, and the costs involved.

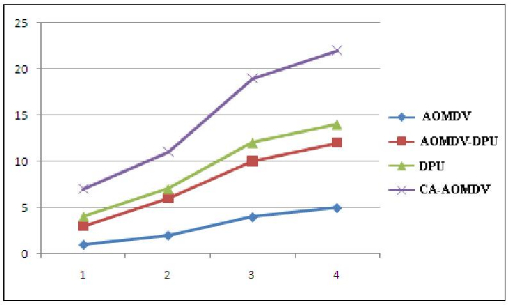

Fig. 3. Packet delivery ratio in normal situations

To evaluate the performance of POR, we simulate the algorithm in a variety of mobile network topologies in together with the famous geographic routing protocol [4] GPSR and on demand routing protocol AODV. Two network environments: the normal one without malicious nodes and the critical one with selective forwarding attack are simulated. Performance metrics include packet delivery ratio, the 90th percentile and average of packet transmission delay. These results then provide valuable insight into more general network topologies, which are analytically intractable. As discussed above, these leading terms correspond to the minimum cuts in the network; as the source-destination distance increases by 1, there is a single additional minimum cut of length k+1.

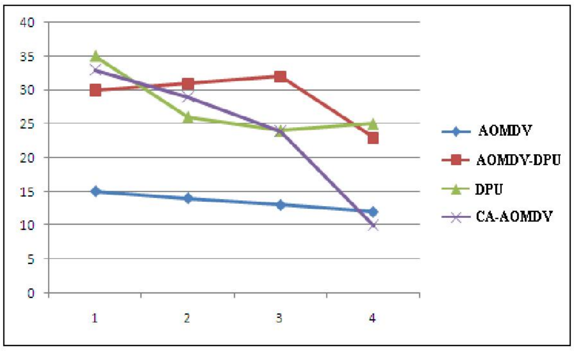

Fig. 4. The 90th percentile of transmission delay in normal situations

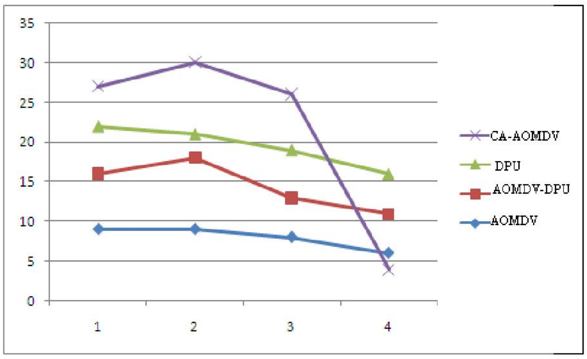

Fig. 5. Packet delivery ratio in critical situations

Conclusion

This paper proposes a general, parameterized model for analyzing protocol control overhead in mobile ad-hoc networks. A probabilistic model for the network topology and the data traffic is proposed in order to estimate overhead due to control packets of routing protocols. Our analytical model is validated by comparisons with simulations, both taken from literature and made specifically for this paper. For example, our model predicts linearity of control overhead with regard to mobility as observed in existing simulations results Notice that using the same route from time to time may be considered as route creations since entries of a routing table have a timeout. If the period between two emissions on the same route is greater than this timeout, the second emission will produce a route request. In a networking environment, the node most likely to detect non-compliant ‘criminal’ behavior are the nodes in the vicinity of the criminal and in some cases the source and the destination, if they detect unusual behavior or do not get proper responses. Mobile ad hoc networks exhibit new vulnerabilities to security attacks. As opposed to traditional networks, mobile ad hoc networks do not rely on any infrastructure and central authorities; they can be highly dynamic and mobile and operate over unreliable wireless media. Simulations results indicate that CA-AOMDV Protocol is better suited as soon as a significant number of links can be reused for several routes.

REFERENCES

[1] J. Burgess, G. D. Bissias, M. D. Corner, and B. N. Levine, “Surviving attacks on disruption-tolerant networks without authentication,” in MobiHoc ’07. New York, NY, USA: ACM, 2007, pp. 61–70.

[2] L. Buttyn and J.-P. Hubaux, Security and Cooperation in Wireless Networks. Cambridge University Press, November 2007.

[3] C. J. Colbourn. The Combinatorics of Network Reliabiilty. Oxford University Press, New York, 1987.

[4] S. Jain, K. Fall, and R. Patra, “Routing in a delay tolerant network,” SIGCOMM Comput. Commun. Rev., vol. 34, no. 4, pp. 145–158, 2004.

[5] J. Ghosh, H. Ngo, S. Yoon, and C. Qiao. On a routing problem within probabilistic graphs and its application to intermittently connected networks. In Infocom, 2007.

[6] A. Vahdat and D. Becker, “Epidemic routing for partially connected ad hoc networks,” Duke University,Tech.Rep., 2000.

[7] K.-W. Chin, J. Judge, A. Williams, and R. Kermode. Implementation experience with MANET routing protocols. Computer Communication Review, 32(5):49–59, 2002.

[8] B. Kannhavong, H. Nakayama, Y. Nemoto, N. Kato, and A. Jamalipour, “A survey of routing attacks in mobile ad hoc networks,” Wireless Communications, IEEE, vol. 14, no. 5, pp. 85–91, October 2007.

[9] R. Anderson and F. Stajano. The resurrecting duckling. Lecture Notes in Computer Science, Springer-Verlag, 1999.

[10] M. Blaze, J. Feigenbaum, and J. Lacy. Decentralized trust management. In Proceedings of IEEE Conference on Security and Privacy, Oakland, CA, 1996.

[11] S. Buchegger and J.-Y. L. Boudec. IBM Research Report: The Selfish Node: Increasing Routing Security in Mobile Ad Hoc Networks. RR 3354, 2001.

[12] L. Buttyan and J.-P. Hubaux. Enforcing service availability in mobile ad-hoc wans. MobiHOC, 2000.

[13] K. Fall, “A delay-tolerant network architecture for challenged internets,” in SIGCOMM ’03. New York, NY, USA: ACM, 2003, pp. 27–34.

[14] D. Ganesan, R. Govindan, S. Shenker, and D. Estrin. Highly-resilient, energy-efficient multipath routing in wireless sensor networks. Mobile Computing and Communications Review, 4(5), 2001.

[15] R. Groenevelt, P. Nain, and G. Koole. The message delay in mobile ad hoc networks. Technical Report RR-5372, INRIA Sophia Antipolis, Nov. 2004.

****