Journal of Telematics and Informatics (JTI)
Vol.4, No.1, March 2016, pp. 1~11
ISSN: 2303-3703

A Mobility Aware Schema To Lower Packet Losses For Reactive Ad Hoc Routing Protocols

Bambrik Ilyas, Didi Fedoua
Laboratoire de Recherche Informatique de Tlemcen, Tlemcen, Algeria
e-mail: Ilyas9111@yahoo.fr

Abstract

In an increasingly wireless world, Ad hoc networks have progressively been developed to become a suitable replacement or, at least complement to the traditional wireless networks. In contrast to the conventional wireless network, the Ad hoc network does not necessarily need a preset infrastructure to be functional. The network members move freely and arrange themselves to perform the routing operations in a distributed fashion. The kernel technology enabling such flexibility is the routing protocol. Though the absence of the infrastructure lowers the installation, configuration and maintenance cost of the dynamic networks, the mobile nodes must deal with several complex issues. Thus, managing : a) security, b) power consumption and balance, c) Quality of Service, in a distributed manner is very challenging. However, above all else, maintaining a path formed by moving particles is the most problematic task. In this paper we analyse the effect of the nodes mobility on the routing protocol performance. Then, we propose a simple schema to counter this issue.

***Keywords**: Ad hoc networks, routing protocol, mobility management.*

1. Introduction

Because of their multiple advantages, dynamic networks progressively gained in popularity. This type of network is distinguished by its distributed nature and auto-healing / auto-governing features. At any moment, the network members are able to move freely which makes the network topology highly flexible. The main idea behind this category of network is to distribute the routing functions on the mobile components of the network rather than dedicating a preset infrastructure. Thus, limiting the deployment cost and enabling the extension of the network without the need of additional infrastructure. Several types of wireless networks, with various characteristics, apply the dynamic network concepts. Conventionally formed only by mobile devices, the Mobile Ad hoc Networks (MANETs) are the primitive incarnation of this category. Vehicular Ad hoc Networks (VANETs) are a derivation of the MANET that can also incorporate the Wireless Sensor Network (WSN) technology. Oriented towards navigation safety, this type of network was designed to disseminate critical messages and to enable communication in infrastructure-less areas. For instance, while the Wireless Mesh Networks (WMN) usually contain a preset infrastructure, the mobile clients organize themselves to extend the coverage of the network.

Regardless of the network specific characteristics, the lively nature of the topology is the root feature of all the aforementioned networks. Then again, performing routing in a completely distributed, randomly changing system, is much more complex than the tradition routing problem. The routing protocol designed to operate in Ad hoc networks must react fast to the topological changes and construct / maintain paths in a distributed fashion. Therefore, numerous routing protocols were specifically designed for this kind of network. Based on the way the Ad hoc protocols construct the paths, three types of protocols exist: a) proactive, b) reactive, c) hybrid.

Proactive protocols build and maintain a path to every possible destination in the network. This strategy requires a periodic broadcast of the topological information maintained by each node. Afterwards, the received routing messages are processed to update the routing table. As a result, this strategy provides a complete knowledge of the topology and reduces the transmissions delay. But over time, the constant broadcast / treatment of control messages can consume a considerable piece of the mobile hosts resources. On the other hand, reactive protocols waist less resources on routing operations by creating a path on request only. This strategy is based on a request / wait for reply cycle and doesn't require a periodic advertisement of the global topological information. Typically, during the construction of a path, the intermediate nodes forward the transmission request once only until the destination is found. After that, the destination generates a reply and sends it through the discovered path. Although this method reduces the overhead, the path construction process forces the source to wait until a path towards the destination is established which increases the transmission delay. Besides, with the absence of routing information exchange, the source is unable to find a better path unless the active one breaks.

Hybrid protocols combine the reactive and proactive methods. Usually, the proactive method is used to collect the routing information about the neighbourhood. Then, the reactive method is launched when a path to a remote destination is required. However, this type of protocol inherits partially the reactive protocols defects and doesn't necessarily produce the shortest path since the search for the destination is zone driven. Some protocols structure the topology in a form of multiple clusters / groups where each cluster, has one representative, in charge of routing, called Cluster Head (CH). Secondly, the nodes that belong to more than one cluster are used for communication between clusters and are called Gateways (GW). As a result, the hierarchical organization minimizes the routing operations performed by the cluster members since the routing functions are managed by the CHs and GWs only. Still, the downside is that the concentration of data flows on the CH / GW can lower the network performance. Eventually, this can also cause the depletion of the CH / GW energy.

In the last few years numerous routing algorithms have been developed to solve specific issues such as the network survivability / energy management [1-3], security related issues [4-6] and QoS insurance [7-9]. However, the most complex issue that all the protocols tailored for dynamic networks must be adapted to, is the random mobility of the nodes. Thus, improving the stability of the paths has attracted numerous contributions [10,11]. In this paper, we discuss how this problem is countered in the reactive protocols. We explain why the efficiency of the proposed strategies are situational. Then, we propose a method to lessen the negative effects of the nodes mobility on the reactive routing protocols performance. This paper is structured as follows: In Section II, the classical reactive protocols are discussed then, some of the most recent contributions addressing the mobility issue are explained. In Section III, we illustrate the effect of the mobility on three vastly extended reactive protocols. In Section IV, we explain the disadvantages of the previous proposed solutions that are based on mobility history during the path discovery process, before proposing an algorithm that can predict path failure to circumvent its negative effect. Finally, Section V concludes this paper.

2. Related Work

Recently, most of the proposed routing protocols for MANET and VANET are reactive protocols. In contrast to the exponential overhead / complexity of the proactive protocols, especially in large networks, the reactive protocols are much simpler to execute. Hence, leaving room for the designers to implement additional methods and upgrade the performance in a given aspect. Ad hoc On demand Distance Vector [12] (AODV) is one of the primal reactive protocols. Founded on the same principles of Destination Sequenced Distance Vector [13] (DSDV) to select the freshest path, which is the destination sequence number, this protocol applies a request / wait for reply cycle to build a path. When a path is required to a given destination, the search is initiated by the broadcast of a Route Request (RREQ). After receiving a RREQ, the intermediate node creates a reversed path to the source and the RREQ is forwarded only once (by each intermediate node) until the destination is reached or a node that has a recent path is attained. After that, a Route Replay (RREP) is forwarded towards the source to establish the transmission path.

The main disadvantage of AODV is its inadaptability to the frequent topological changes. When the nodes movement affects the transmission path, first, the source is informed about the path rupture, then the search for the destination is restarted from the beginning. As a result, the network members' movement can heavily influence the transmission delay and overhead. An extended version of this protocol proposed in [14] incorporate a local route repair method. This mechanism can reduce the transmission delay caused by disconnections especially when the nodes are moving slowly or at a medium speed. Most importantly, when the local route recovery is successful, the cost to repair the paths is usually lowered in terms of overhead.

Instead of memorizing the path in the intermediate nodes, Dynamic Source Routing [15] (DSR) includes all the routing directives in RREQ / RREP and data messages. When a path disconnection is detected, this protocol apply a packet salvaging method to reroute packets towards the destination. Though this protocol generate a large overhead, it mitigate the routing operations and eliminate the need to memorize the routing decisions. Plus, knowing the integrity of the path is a significant advantage especially for security insurance purposes. Which is why numerous security oriented routing algorithms are based on DSR [16-18].

To improve the resiliency against route failures, Ad hoc On demand Multi-path Distance Vector [19] (AOMDV) and Temporally Ordered Routing Algorithm [20] (TORA) build / uphold multiple paths towards the same destination. While applying AOMDV, during a path construction towards a single destination, a node accepts RREQs received from different links. Hence, resulting into the creation of disjoint reversed paths leading to the source. Afterwards, once the destination is located, the RREPs are forwarded to the source via the disjoint paths and all the unearthed paths are memorized although only one is used. Rather than restarting the search for the destination like AODV, AOMDV activates one of the alternative paths in case of a disconnection.

The first protocol to incorporate a mechanism to enhance the path stability is Associativity Based Routing [21] (ABR). To run this protocol, each node in the network attributes an associativity degree to its neighbours by counting the number of HELLO messages received. During the search for the destination, the associativity degree of the explored links are included in the request messages. Afterwards, when the destination is reached, the path with the highest associativity degree is selected. Also, this protocol includes a local path repair feature. Although the local path repair is rewarding when the nodes are moving at a medium / low pace, this method amplifies the transmission delay when it fails.

Location Aided Routing [22] (LAR) was specifically designed to diminish the effect of the nodes mobility on the network performance. While the location of the destination is forwarded regularly to the traffic source, this reactive protocol explores the existing geographical information about the destination (last known location, time elapsed since the last communication, speed and direction of movement) to near down the location where the destination might be found, in case of a path failure. First, the source calculates the relative distance that separates it from the destination and includes it in the request message. Subsequently, the intermediate node receiving the request message will rebroadcast it only if the current node is closer to the destination than the previous one. In order to enlarge the search area, the distance separating the destination from the source is augmented at the beginning of the process. This way, the probability of finding the destination is increased. Additionally, the frequency to broadcast routing packets depends on the node mobility. The faster a node moves, the more it announces its location. However, supposing that the next hop leading to the destination is the closest one to it (geographically), can be false. As a result, the path repair mechanism can falsely fail which leads to restarting the search for the destination and including all the network in the process. Additionally, building paths based on the geographical locations doesn't insure the creation of the shortest path.

Table 1. Comparison between the reactive protocols.

Protocol	Advantages	Inconveniences
AODV	• Avoids routing loops by the use of the destination sequence number. • Low complexity.	• When a path in current use is broken, the source is forced to restart the search for the destination from the beginning, which increases the transmission delay.
DSR	• Avoids routing loops by including the entire path in the data messages and route request / reply. • Requires less storage capacity / routing operations.	• Generates a high overhead.

AOMDV / TORA	• Creates multiple paths to the same destination for a better adaptability to the topology changes. • Lowering the overhead caused by path failures.	• Maintaining alternative paths requires extra processing.
ABR	• Creates paths through the nodes that have a low sate of mobility. • Applies a local repair mechanism to reduce the transmission delay.	• When the local repair process fails, the transmission delay is increased. • Local path repair does not necessarily produce the shortest path.
LAR	• Through the use of the geographical information, LAR minimizes the participants in the path recovery and accelerates the process.	• If the next hop towards the destination is not the closest one to it (geographically), the path recovery can fail falsely. This will force the source to restart the search in the entire network. • Path construction based on the geographical locations does not necessarily produce the shortest path.

Commonly, the recent protocols designed to promote path stability, are reactive or hierarchical protocols that estimate the relative mobility. During path discovery, the maximum mobility state of the intermediate nodes is forwarded to the source. This metric can be derived in various ways based on: a) Hello messages count, b) Geographical coordinates, c) signal strength, d) Link Expiration Time [23] (LET). Subsequently, the path offering the lowest mobility state, is used. Founded on this approach, Adaptive Mobility aware AODV [24] (AMAODV) is a multi constraint protocol that favours paths with high stability. This protocol simply forwards the collected metrics about the discovered paths and, the one with highest score, is chosen. For similar purposes, the protocol proposed in [25] relies on a fuzzy mobility value to promote long lived clusters in order to improve path stability. Furthermore, Speed Aware Routing Protocol [26] (SARP) reduces the probability of path failure by eliminating the nodes with a high speed of movement from the transmission path.

To estimate the durability of a link, several protocols are based on the LET metric. For a link between two nodes within range of each other, this metric is derived from: a) the speed and direction of movement of both nodes, b) distance. Power aware Multiple QoS constraints Routing Protocol with Mobility Prediction [27] (PMQRPMP) is one of the earliest protocols applying this concept. Similarly, BAT-AOMDV [28] is a multi objective protocol, inspired from the BAT meta heuristic [29], that estimate the link availability. Another aspect that can influence path stability is the power level of the intermediate nodes. Hence, the remaining energy of the nodes was combined with the relative mobility in several methods to reinforce path stability. For instance, Mobility Adjustment Routing [30] (MAR) is a hierarchical protocol that combines both previous metrics to select the CH / GW. Then, during the reactive path discovery session, the minimum remaining energy and maximum mobility of the intermediate nodes are transported to the source. Consequently, avoiding the participation of nodes with low battery power in the new transmission. Likewise, based on Fuzzy Logic, the protocol designed in [31] combines the residual energy and relative mobility to compute a trust value for the intermediate nodes during path discovery. Afterwards, the path offering the highest trust value, is selected.

3. Results and Analysis

Table 2. Simulation parameters.

Network Size	30
Transmission Range	250m
Connections	10
Connections Type	CBR
Max. Speed	**2m/s - 25m/s**
Packet Rate	6
Packet Size	512byte
Simulation Space	1000m x 1000m
Simulation Type	200s

To compare how different routing protocols react to the nodes mobility, we ran a series of simulations with Network Simulator 2 [32] (NS2) where the nodes speed of movement is augmented progressively (Table 2). The three tested protocols implement different methods to adapt to the nodes mobility and path failures. First, when a path is broken, AODV restarts the search from the beginning. Secondly, AOMDV relies on alternative paths to avoid reinitiating path construction. And third, LAR [33] employs the latest known geographical information about the destination to avoid searching for it in the entire network. These three protocols were chosen because they are widely used to develop mobility aware algorithms.

Typically, the increase of the nodes movement speed leads to the elevation of the Packet Loss Ratio (PLR). As the nodes move rapidly, path failures are much more frequent. Consequently, the PLR of all the tested protocols is raised as shown in Figure 1. Nonetheless, the performances of the protocols are not affected equally. Though AOMDV activates one of the alternative paths in case of path failure, the increase of the nodes mobility eventually breaks the alternative paths as well. Thus, the failure of the alternative path amplifies the PLR while using AOMDV. On the other hand, once a path rupture is sensed, AODV launches the search for the destination immediately. As a result, this protocol re-establishes the connection and diminish packet losses. Like AODV, LAR restarts the search for the destination when a path breakdown is sensed. However, only the nodes closer to the destination participate in the path recovery process. Though this strategy is efficient at low / medium speed, the possibility of recovery failure augment with the increase of the nodes movement speed. Hence, forcing the source to restart the search for the destination while including all the network in the second attempt. As a result, expanding the PLR as well.

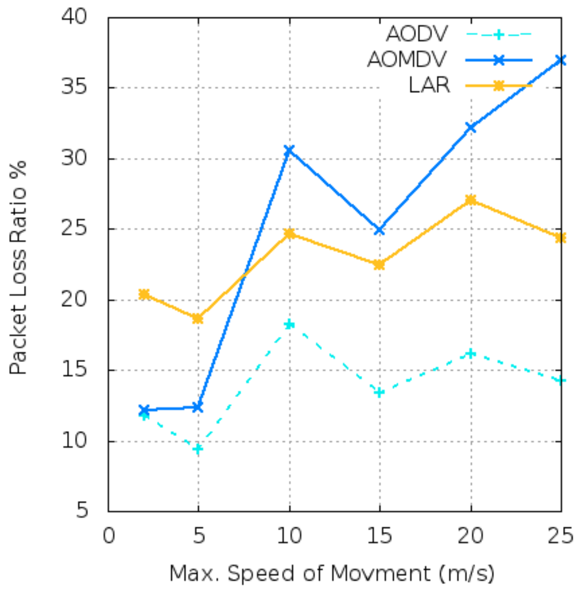

Figure 1. Movement speed VS PLR.

Same, as disconnections are more recurring due to the increase of the nodes mobility, all reactive protocols must revive the connection between the source and destination. Accordingly, the normalized overhead of all the tested protocols is increased as shown in Figure 2. While running AODV, a path failure generates a RREQ storm to relocate the destination.

Though LAR searches for the destination in a restricted area, the location of the destination is forwarded frequently towards the source in order to update the location table. Consequently, increasing the overhead of this protocol as well. By using alternative paths instead, AOMDV is the least affected protocol. Respectively with the resulting overhead, AODV processes the highest number of routing packets as shown in Figure 3. On the other hand, LAR treats less routing packets than AOMDV. While running AOMDV, maintaining alternative paths introduces additional processing by the intermediate nodes forming the alternative paths. Conversely, LAR processes less routing packets. Though this protocol announces the location of the destination frequently, only the nodes forming the transmission path process the corresponding packets. Afterwards, during path recovery, LAR avoids generating a RREQ storm by nearing down the area where the destination can be located.

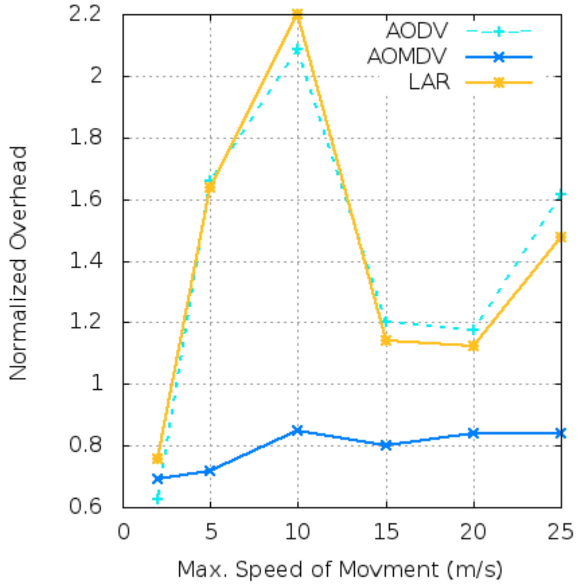

Figure 2. Movement speed VS Normalized overhead.

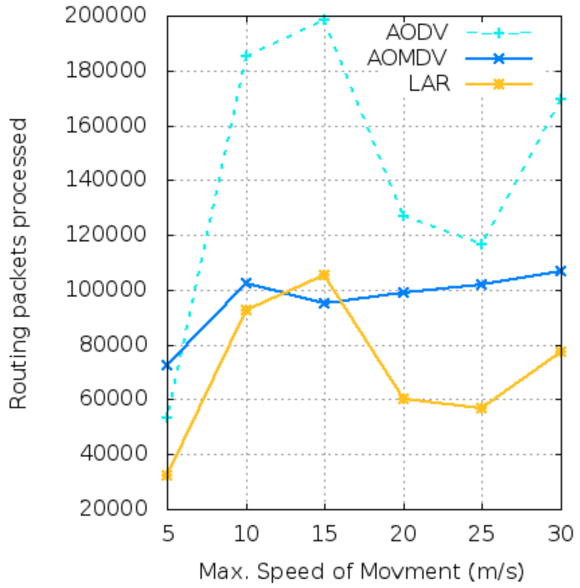

Figure 3. Movement speed VS Routing packets processed.

Particularly, the increase of the nodes mobility augment the end to end delay of AODV as illustrated in Figure 4. In case of path failure, AOMDV instantly activates an alternative path to reach the destination and LAR accelerates the search for the destination through the use of the geographical information. Thus, when the methods applied by these two protocols are successful, the connection is resurrected quickly by comparison with the traditional method applied by AODV. Table 3 summarizes the effects of the nodes mobility on the tested protocols.

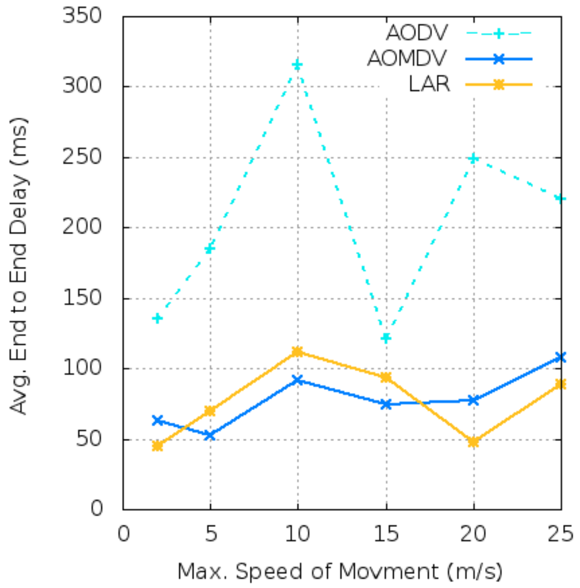

Figure 4. Movement speed VS Average end to end delay.

Table 3. The negative mobility effect on the tested protocols.

Protocol	PLR	Overhead	Delay
AODV	Low	High	High
AOMDV	High	Low	Low
LAR	Medium	Medium	Low

4. Proposition

Though many protocols have been proposed to react better to path failures, most of the proposed algorithms are based on the nodes mobility history. This approach improve somewhat the probability of creating a stable path but in a realistic scenario where the nodes can randomly change their direction / speed of movement, this method does not offer much guarantee especially in teams of Packet Delivery Ratio (PDR). The approach that we propose in this paper is meant to anticipate a possible path failure to alarm the source node beforehand. As a result the source either rebuild a path, attempt a local repair or selects an alternative path.

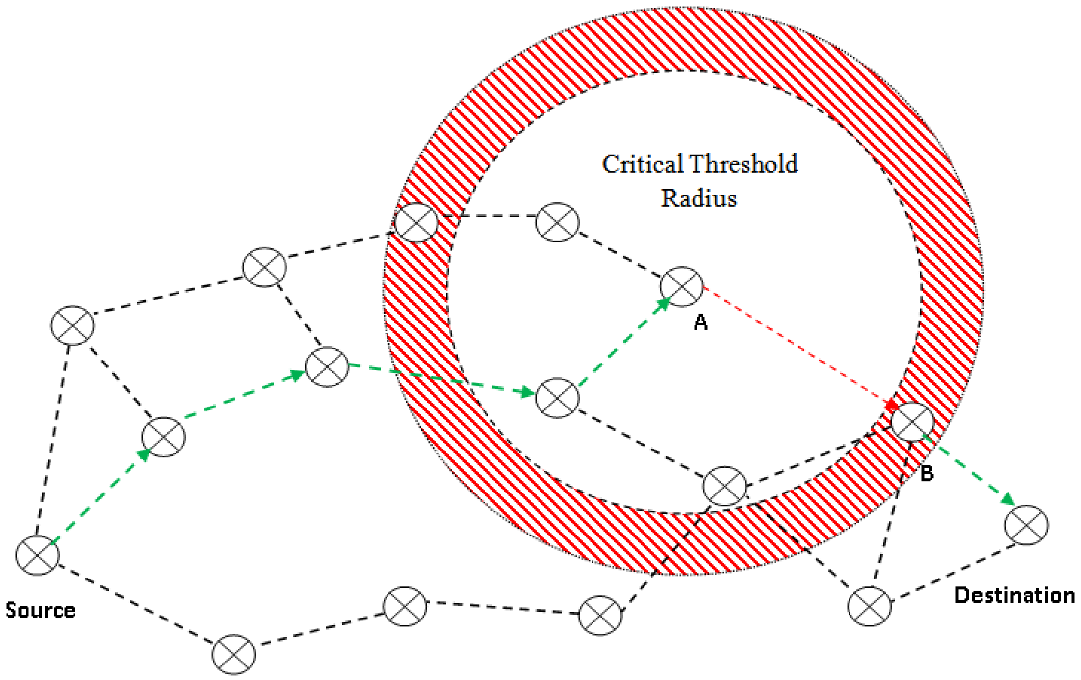

Figure 5. Path failure prediction through signal strength measurement.

The approach that we propose can be implemented as an extension of AODV or AOMDV. First, after that the primal routing approach is applied to search for the destination (AODV / AOMDV), regardless of the path quality metric, the Minimum Signal Strength (MSS) of each discovered path is collected and registered at the source. Afterwards, through the periodic HELLO messages broadcast, the intermediate nodes of the active and alternative paths alike, measure the signal strength of the downstream nodes to detect the decline of signal strength (i.e. Figure 5). Eventually, an intermediate node that detects that a downstream node has moved beyond the Critical Threshold (CT) warns the source about the possibility of a link failure. As a result, the source can choose to launch a path recovery or select a substitute path with a solid remaining MSS. Reasonably, this method introduces additional processing / control overhead. However, the slight raise of the overhead comes with a possibly significant profit in PDR. Particularly, in the case of AOMDV, the alternative paths are better managed and the probability of using a deteriorating backup route, is narrowed .

```
void Processing_Received_Routing_Message(Routing_Message Received_RM){
 NodeID GeneratorIP=Received_RM.GeneratorIP();
 Neighbour_Info Gen_Neighbour=NeighbourhoodTable.getNeighbourInfo(GeneratorIP);
 boolean Direction;
 Signal_Strength=Received_RM.ReceivingSignalStrength();
 if(Gen_Neighbour==null){
     Gen_Neighbour=new Neighbour_Info(GeneratorIP, Signal_Strength, true);
     NeighbourhoodTable.addNewNeighbour(Gen_Neighbour);
     return ; // If it's a new neighbour, the process is halted
 }
 else {
     Direction= (Signal_Strength-Gen_Neighbour.PreviousSignalStrength())>=0;
     /* Direction = true <=> the two nodes are moving towards each other
      *  Direction = false <=> the two nodes are moving away*/
     NeighbourhoodTable.updateInfo(GeneratorIP, Signal_Strength, Direction);
     }
 if((Critical_Threshold > Signal_Strength) && (!Direction)){
     /* If the link signal strength with the neighbour deteriorate past the
      * Critical_Threshold, a warning message is sent to the corresponding
      * sources*/
     Vector Destination_List=new Vector();
     Destination_List
         .addAll(RoutingTable.isNextHopInActivePath(GeneratorIP));
     Destination_List
         .addAll(RoutingTable.isNextHopInAlternativePath(GeneratorIP));
     /* Destination_List is the list of transmissions that the corresponding
      * neighbour is involved in.*/
     if(Destination_List.isEmpty()) return;
     /* If the neighbour is not involved in any tramissions, the process is
      * halted*/
     NodeID Destination;
     for(int i=0;i<Destination_List.size(); i++){
         Destination=(NodeID)Destination_List.elementAt(i);
         SendWarning(Destination,Signal_Strength);
     }
 }
}
```

Figure 6. Mobility aware algorithm to predict imminent path failures.

The algorithm presented in Figure 6 shows how the received Hello messages are processed to apply the proposed method. Based on the variation of the signal strength, the algorithm detects when two nodes are moving away from each other. Subsequently, when the signal quality deteriorates past the defined CT, the sources are warned about the possible imminent link breakage. For simplicity sake, the algorithm that we propose here deals only with the possibility of link failure. It's possible to extend this method to administer the path discovery process. For instance, while applying AOMDV, instead of forwarding all the RREQs received from different links, packets received from links that are on the verge of failing are dropped accordingly. As a result, limiting the overhead / maintenance cost.

5. Conclusion

In this paper, we propose a simple extension for a reactive protocol to alarm the source of the path failure possibility. Unlike other protocols that relies solely on the mobility history of the nodes during the discovery session, the proposed method can react when the mobility state of the nodes changes suddenly. Though this approach certainly introduces additional treatment and possibly increases marginally the overhead, its gain from a PDR perspective can be significant. This extension could be beneficial especially for AOMDV to avoid the usage of a failing backup path. In a future work, we aim to implement this method in a reactive protocol and analyze its effect on the resulting performance.

References

[1] Savitha KK, Chandrasekar C. An energy aware enhanced AODV routing protocol in MANET. *International Journal of Communication Networks and Distributed Systems*. 2013; 10(3): 233-242.
[2] Sofiane Z, Soufiene D, John M. A fast, reliable and lightweight distributed dissemination protocol for safety messages in Urban Vehicular Networks. *Ad Hoc Networks*. 2014; 27: 26-43.
[3] Ramanna H, Attimarad GV, Prasad MNG. EASR: Graph based Framework for Energy Efficient Smart Routing in MANET using Availability Zones. *International Journal of Electrical and Computer Engineering*. 2015; 5(6): 1381-1395.
[4] Djenouri D, Bouamama M, Mahmoud O. Blackhole resistant ENADAIR-based routing protocol for Mobile Ad hoc Networks. *International Journal of Security and Networks*. 2009; 4(4): 246-262.
[5] Wang, X, Jing Y, Zetao L, Handong L. The energy efficient group key management protocol for strategic mobile scenario of MANETs. *EURASIP Journal on Wireless Communications and Networking*. 2014; 2014:161, doi:10.1186/1687-1499-2014-161.
[6] Sumathi A, Sundaram BV. Evaluating An Authenticated Trust Based Adhoc On Demand Distance Vector For Malicious Nodes Isolation In MANET. *Journal of Computer Science*. 2014; 10(9): 1859-1864.
[7] Sondi P, Gantsou D, Lecomte S. A multiple-metric QoS aware implementation of the optimised link state routing protocol. *International Journal of Communication Networks and Distributed Systems*. 2014; 12(4): 381-400.
[8] Palaniappan S, Chellan K. Energy efficient stable routing using QoS monitoring agents in MANET. *EURASIP Journal on Wireless Communications and Networking*. 2015; 2015:13, doi: 10.1186/s13638-014-0234-9.
[9] Alharbi, A., Al Dhalaan A., Al Rodhaan M.: A Q-Routing Protocol Using Self Aware Approach for Mobile Ad hoc Networks. *American Journal of Applied Sciences*. 2015; 12 (12): 1014-1022.
[10] Akunuri, K, Guardiola I, Phillips A. Mobility and fast fading impact study on wireless ad hoc networks. *International Journal of Mobile Network Design and Innovation*. 2010; 3(3): 160-168.
[11] Ali M, Abdallah B. A survey of routing protocols based on link stability in mobile ad hoc networks. *Journal of Network and Computer Applications*. 2015; 47: 1-10.
[12] Perkins CE, Belding RE, Das S. Ad hoc On Demand Distance Vector Routing. *RFC IETF Internet Draft*. 2003. https://www.rfc-editor.org/rfc/rfc3561.txt.
[13] Perkins CE, Bhagwat P. *Highly dynamic destination sequenced distance vector routing for mobile computers*. Conference on Communications architectures, protocols and applications (SIGCOMM). London. 1994, 234–244.
[14] Alshanyour M, Baroudi U. *Bypass AODV: Improving Performance of Ad Hoc On Demand Distance Vector (AODV) Routing protocol in wireless ad hoc networks*. 1st International conference on Ambient media and systems (AMBI-SYS). Quebec. 2008; doi : 10.4108/ICST.AMBISYS2008.2895.
[15] Johnson D, Hu Y, Maltz D. The Dynamic Source Routing Protocol for Mobile Ad Hoc Networks for IPv4. *RFC IETF Internet Draft*. 2007. https://www.ietf.org/mail-archive/web/ietf-announce/current/msg03407.html.
[16] Subathra P, Sivagurunathan S. Secure Route Discovery in DSR against Black Hole Attacks in Mobile Ad Hoc Networks. In: Debashis S, Varadharajan S. Next Generation Data Communication Technologies: Emerging Trends. 2012: 125-143.
[17] Mohanapriya M, Krishnamurthi I. Modified DSR protocol for detection and removal of selective black hole attack in MANET. *Computers & Electrical Engineering*. 2014; 40(2): 530-538.
[18] Jebadurai IJR, Rajsingh EB, Paulraj GJL. Enhanced dynamic source routing protocol for detection and prevention of sinkhole attack in mobile ad hoc networks. International Journal of Network Science. 2016: 1(1): 63-79.
[19] Marina MK, Das RS. Ad hoc On demand Multipath Distance Vector routing. *Wireless Communications And Mobile Computing*. 2006; 6(7): 969-988.
[20] Park VD, Corson MS. *A highly adaptive distributed routing algorithm for mobile wireless networks*. Sixteenth Annual Joint Conference of the IEEE Computer and Communications Societies; Driving the Information Revolution (INFCOM). Kobe. 1997; 3: 1405-1413.

[21] Toh CK. Associativity based routing for ad hoc mobile networks. *Wireless Personal Communications*. 1997; 4(2): 103-139.

[22] Ko YB, Vaidya NH. Location Aided Routing in mobile Ad hoc networks. *Wireless Networks Journal*. 2000; 6(4): 307-321.

[23] Su W, Lee SJ, Gerla M. *Mobility Prediction in Wireless Networks*. 21st Century Military Communications Conference Proceedings (MILCOM). Los Angeles. 2000; 1: 491-495.

[24] Bisengar A, Rziza M, Ouadou M. Queue Length and Mobility aware Routing Protocol for Mobile Ad hoc Network. *International Journal of Communication Networks and Information Security*. 2012; 4(3), pp.207-211.

[25] Venkateswaran P, Orea K, Mousumi K, Nandi R, Shaw S. Fuzzy Logic Based Mobility Metric Clustering Algorithm for MANETs. Varadharajan S, Debashis S. Web Based Multimedia Advancements in Data Communications and Networking Technologies. 2013: 207-219.

[26] Akunuri K, Arora R, Guardiola I. A Study of Speed Aware Routing for Mobile Ad Hoc Networks. In: Michael RB, Steven RP. Advancements and Innovations in Wireless Communications and Network Technologies. 2013; pp. 190-212.

[27] Senthilkumar M, Somasundaram S, Amuthakkannan R. Power aware multiple QoS constraints routing protocol with mobility prediction for MANET. International *Journal of Information Systems and Change Management*. 2009; 4(2): 156-170.

[28] Prabha R, Ramaraj N. An improved multipath MANET routing using link estimation and swarm intelligence. *EURASIP Journal on Wireless Communications and Networking*. 2015; 2015:173, doi:10.1186/s13638-015-0385-3.

[29] Maghrebi MF, Aghaebrahimi MR, Taherian H, Attari M: Determining the Amount and Location of Leakage in Water Supply Networks Using a Neural Network Improved by the Bat Optimization Algorithm. *Journal of Civil Engineering and Urbanism*. 2014: 4(3): 322-327.

[30] Alagiri I, Madhuviswanatham V, Krishna PV. Efficient Data Transfer by Mobility Adjustment Algorithm for Clustered Mobile Ad Hoc Networks. *Cybernetics and Information Technologies* . 2014; 14(2): 50-64.

[31] Nihad IA, Mustafa I. Fuzzy approach to improving route stability of the AODV routing protocol. *EURASIP Journal on Wireless Communications and Networking*. 2015; 2015:235, doi:10.1186/s13638-015-0464-5.

[32] The Network Simulator ns-2. http://www.isi.edu/nsnam/ns/index.html. 1995.

[33] Jeff B, Wilcox L. DREAM and LAR patch for NS 2.33. https://doc-0g-3o-docs.googleusercontent.com/docs/securesc/ha0ro937gcuc7l7deffksulhg5h7mbp1/9jr6me6ajnd4mgnscmbpjiscohr3qgbn/1436248800000/04198340273633395013/*/0B7S255p3kFXNM2JwbktMSGxoUkE?e=download. 2002.