https://doi.org/10.26682/sjuod.2023.26.1.35
Journal of University of Duhok., Vol. 26, No.1 (Pure and Engineering Sciences),Pp 365-371, 2023

ROUTING MISBEHAVIOR IN MOBILE AD HOC NETWORKS

DELAN **S**HERZAD **A**LSOUFI and **I**SMAIL **A**MIN **A**LI
Dept. of Computer Electrical and Computer Engineering, College of Engineering,
University of Duhok, Kurdistan Region-Iraq

(Received: August 20, 2022; Accepted for Publication: May 15, 2023)

ABSTRACT

An ad hoc network is a temporary network that consists of wireless mobile hosts. Due to the absence of a centralized or structured infrastructure, a host may need assistance in forwarding a packet to a desired location. This is applicable in the cases whereby a limited range of transmissions is visible in mobile hosts. Dynamic Source Routing (DSR) is a simple but effective protocol intended specifically for those networks that lack a predetermined infrastructure. However, DSR becomes less reliable and may show misbehavior when network topology changes rapidly. One such misbehavior occurs when some 'selfish' nodes contributing in route discovery and safeguarding of the network refuse to send data packets. To address this problem and improve the throughput of MANETs, this paper proposes a modified DSR protocol based on two techniques: a 2ACK scheme and a pathrater extension. This paper has outlined the newly proposed and improved method in the attempt of enhancing the DSR protocol.

Keywords: Mobile Ad Hoc Network (MANET), DSR protocol, routing misbehavior, selfish nodes, 2ACK, pathrater

1. INTRODUCTION

The strategic policy of routing protocols for mobile ad hoc networks (MANETs) is based around the hypothesis that all of the partaking nodes are fully accommodating. However, due to the absence of a centralized infrastructure (an access point), there will be topological changes thus eventually resulting in routing challenges .

In ad hoc networks, all available nodes are used for routing and forwarding packets (), thus maximizing total network throughput. Nonetheless, a node is considered selfish when it misbehaves by agreeing to forward a data packet but in fact does not. This act of selfishness or misconduct may result in severe system degradation in terms of performance. Thus, for this paper we are driven to detect possible misbehavior potentialities and identify how we can enhance the detection process. Contemporary versions of ad hoc routing algorithms include the dynamic source routing (DSR) (Rajeshkumar & Sivakumar, 2013). DSR is a meek, effectual protocol built and intended specifically for those networks that are unequipped of a predetermined infrastructure, allowing a networks ability to be self-configured (Najafi & Gudakahriz, 2018), whereby nodes can play the role of a router or host (Najafi & Gudakahriz, 2018), with no prearranged periodic routing messages. In previous studies the DSR protocol has been represented to show outstanding performances with regards to throughput and end to end delay (Zhang, Anpalagan, & Guo, 2014). This accommodates further to the benefits of this protocol as it avoids bandwidth overhead which in turn preserves battery power (Khabir, Siraj, Habib, Hossain, & Ahad, 2018).

However, the main drawback of this protocol is that it uses the shortest path assuming it to be the most successful path. It only identifies if the receiver's network interface has acknowledged data packets assuming that the routing nodes do not misbehave.

In this study, we investigate an alternative strategy to identify and mitigate the chances of routing misbehavior. the routing misbehavior is presented in the context of the DSR protocol, which will be utilized as the fundamental routing protocol to exemplify our recommended add-on schemes: the 2ACK and Pathrater schemes. The 2ACK scheme involves the process of sending back a particular two-hop acknowledgment to the node that sends out a packet, in order to indicate the success of a received data packet at the next (destination) node. The main idea behind the pathrater module is that it syndicates the knowledge of misbehaving nodes with the link

delan.alsofi@uod.ac

reliability data in the attempt to select the most likely reliable route (Rajeshkumar & Sivakumar, 2013). With these two schemes used as extensions to the DSR protocol we can alleviate and lessen the hostile effects of misbehaving nodes.

1.1 Problem Statement

Due to the open structure of an ad hoc network, whereby a node takes on the role of a router and is free to move as it wishes, it introduces the concept of routing misbehavior. In MANETs, routing misbehavior can brutally impair network performance and in turn efficiency . Routing misbehavior includes the act of misbehaved nodes whereby they partake and contribute in the routing discovery but fail to send packets to an intended destination.

There are several reasons as to why a node may act up, whether it be overloaded, selfish, malicious or even broken. A node that is congested has insufficient network bandwidth so it cannot forward packets. A malicious node denies service by dropping packets. A selfish node is reluctant to expend battery life and finally a broken node is one with software fault preventing it from forwarding any packets. Throughout this paper we will be emphasizing on certain schemes that will alleviate or to some extent even eliminate the effects of node misbehavior.

The structure of this essay is as follows: Section two concentrates on the associated research involving credit-based and reputation-based methods which are often used to reduce or better yet prevent node misbehaviour in MANETs. Section three explains the proposed solution to potentially boost the performance of the DSR protocol using the methodologies of pathrator and 2ACK schemes. Section four demonstrates the mathematical model for the representation of probability of the misbehaving routes that are common in MANETs. Section five, presents the discussions and intentions for future work and finally a conclusion is added in order to complete this research study.

2. RELATED WORK

Previously, the misbehavior problems faced in wireless networks including MANETs have been researched by a number of researchers . A variety of approaches and methods have been considered in the attempt to prevent the ‘selfish’ nodes from degrading the performance of MANETs. These methods can be categorized as: credit-based schemes and reputation-based schemes.

2.1 Credit-Based schemes

The main idea behind the credit-based schemes is to present encouragement for the nodes to correctly carry out the networking functions. To do this, a virtual (electronic) currency of some sort is arranged. In such a case, nodes are compensated for their contribution in offering services to other nodes. However, having said that, the node in which requests the help of other nodes in forwarding packets, will utilize the same payment method in order to pay for these services (Nazih, Benamar, & Younis, 2020; Ojha, Jackowski, Snášel, & Abraham, 2014).

In (Goka & Shigeno, 2018), employed the concept of nuggets (also denoted as beans) in exchange for packet forwarding fees. In this theory, two models were proposed: The Packet Purse Model and the Packet Trade Model (Khan, Olanrewaju, Anwar, Najeeb, & Yaacob). The initial proposal, the packet purse Model, the sender will dispense several nuggets on the data packet before it is sent. Therefore, any node that participates in the packet forwarding will earn nuggets. Nevertheless, given that the nuggets run out before the packet has reached its destination, the packet will then be released. In the Packet Trade Model, a node will “buy” the packet from the prior node, and “sell” it to the subsequent node for additional nuggets.

2.2 Reputation-Based Schemes

Consider these types of methods used in the attempt to prevent node misbehavior in MANETs, (Poongodi, Khan, Patan, Gandomi, & Balusamy, 2019; Shrivastava & Srivastava). These techniques involve the group work of the network nodes, whereby the nodes cooperatively identify and publicly announce the misbehavior of a suspect node. This announcement is broadcasted throughout the entire network so that the identified misbehaving node will then be removed and disconnected. One of the earlier proposed schemes to minimize the improper routing behavior included the watchdog and pathrater modules . In this technique the watchdog element overhears the medium determining if the data packet is sent by the next-hop node. Concurrently, it also keeps a buffer which keeps a record of recently sent packets. Only when the watch dog notices the same packet being transmitted by the next-hop node, the data packet is emptied out of this buffer. However, if a data packet remains in the buffer

for an extended period of time, the watchdog blames the next-hop node for misbehaving and thus acting improperly. Bearing in mind, based on the watchdog allegations, the pathrater module will start rating every path cache and then selects the path with the highest rate for the next packet routing in order to avoid the misbehaving or selfish nodes.

3. PROPOSED SOLUTION

3.1 Dynamic Source Routing

DSR is an "on-demand", source routing protocol. Every packet that is being sent through a MANET contains the addresses of all nodes that have agreed to contribute in the routing path. DSR is called "on-demand" due to that the routing path for a packet is being discovered at the time the source node wishes to transmit a packet to the destination node if the source node lacks a known path to take.

The two primary purposes of DSR are route discovery and route maintenance. According Figure 1 (a), (b) and (c), Node S intends to deliver a data packet to node D. It starts a route discovery and directs a route request by broadcasting the route request to all its neighbor nodes, where the neighbor nodes in return broadcast the route request to its neighboring nodes until the request reaches node D. Node D then replies with a route reply packet to notify Node S with the discovered route. DSR then saves the discovered route in a route cache for further use.

Route maintenance is DSR's other primary duty, which takes care of links failure and breaks. A link failure may occur if two mobile nodes on a routing path are no longer available and they are out of range. If one of the intermediate nodes detects a failure link, it will notify the source node about the failed link, so that source node can choose another routing path or initiate another discovery route.

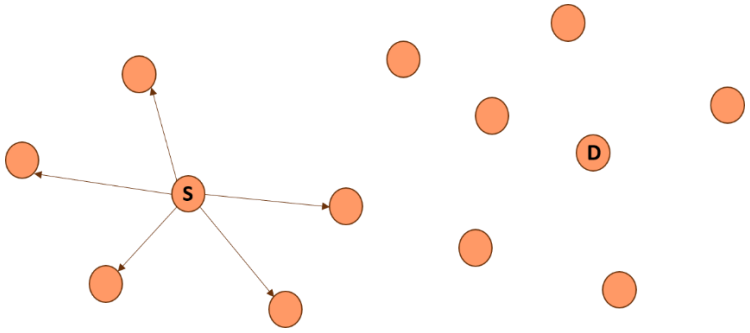

Fig. (1-a): Packet Transmission

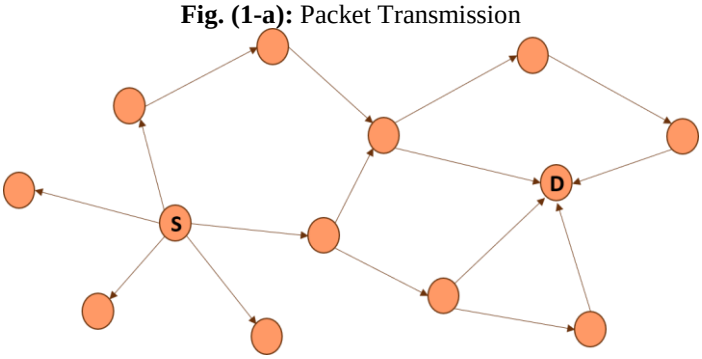

Fig. (1-b): Route discovery

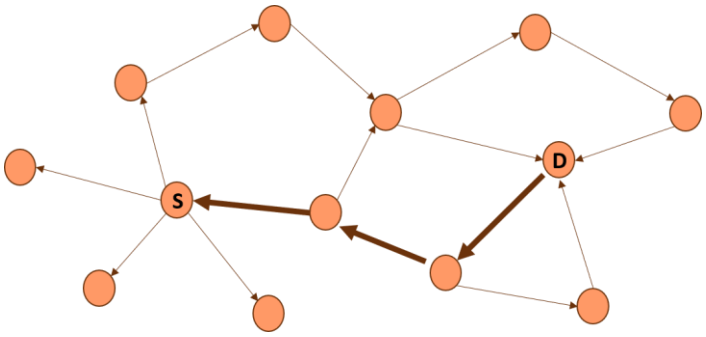

Fig. (1- c): Packet Reception

3.2 PathRater and 2ACK

In this section we will introduce in details the 2ACK scheme and Pathrater scheme, our tools to detect and alleviate routing misbehavior; these tools will be implemented on top of the DSR protocol.

3.2.1 Two-Acknowledgement scheme (2ACK)

The 2ACK scheme involves the process of sending back a particular two-hop acknowledgment to the node that sends out a packet, in order to indicate the success of a received data packet at the next (destination) node(Jain & Khuteta, 2015).

As soon as a Source node S transmits a data packet through the routing nodes N1, N2and N3 which were selected by the discovery route of DSR to the Destination node D, N1 will receive the Packet and forward it to N2. However, it will not have any information on whether or not N2 forwarded the packet to N3. In the case of watchdog technique N1 will be able to know if N2 forwards the packet to next hop node N3 by over hearing the medium but it will not be able to detect whether N3 has received the packet or not. This is one of the disadvantages of using the watchdog module as it can still cause incorrect assumptions on N3 being a behaving or a misbehaving node. The watchdog is influenced by a few issues including vague collisions, receiver collisions and low transmission power.

Thus, the 2ACK scheme can overcome these limitations as shown in Figure 2. To correct some of these limitations, N3 will send a two-hop acknowledgment in response, so that N1 will be aware that the packet was successfully received by N3.

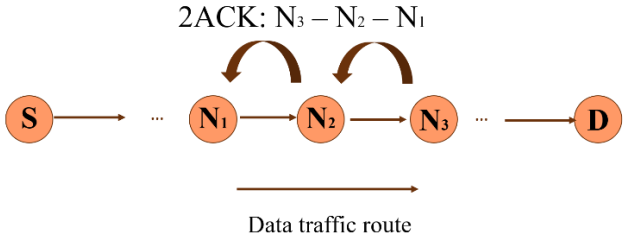

Fig. (2): The 2ACK Scheme

3.2.2 PathRater (PR)

With the help of the 2ACK scheme combined with the pathrater, we can try and avoid the routing path with misbehaving or selfish nodes. The main idea behind the pathrater module is that it combines the familiarity of misbehaving nodes with the link reliability data in the attempt to select the route which is presumably trustworthy. Furthermore, all nodes will keep a rating for every node that it is aware of within the network. As a result, it will calculate a path metric through averaging the rates of the nodes in the pathway. If there is more than one path towards the same location, the pathrater will select the path with the highest metric.

4. MATHEMATICAL MODEL FOR ROUTING MISBEHAVIOR

4.1 Probability of misbehaving routes

To clarify the undesirable effects of routing misbehaviors we first need to approximate the likelihood of the network's misbehaving routes (). A route is considered disruptive and disorderly, when at least one router on this route is ineffective. Consider the following measurements:

N Nodes are arbitrarily distributed over a network area of size X*Y. Each operation's source and destination are selected at random. Excluding the source and destination, the nodes are autonomously chosen as corrupt nodes with a probability p_m.

Assuming that a route has an average of h hops, there will h-1 routers along that route, in between the source and the destination. Therefore, with this information, we can conclude that the probability of the route having at least one faulty node is:

$$P_r=1-(1-p_m)^{h-1} \quad (1)$$

The average number of hops h is essential in calculating the pr. Thus, to estimate h, we have to determine the average progress of each hop, l, within the network as well as the average distance between the source and destination nodes(Narayana & Bharathi, 2019). This gives us the measurement h=d/l.

ε_t represents the average number of nodes within the transmission circle and can be calculated using the following equation:

$$\varepsilon_t=\frac{N}{X*Y} * \pi r^2 \quad (2)$$

Where, $\frac{N}{X*Y}$ is the density of the node. For arguments sake, we will assume that ε_t is a numeral and calculate the probability that all ε_t nodes located a distance r from the transmission circle center (Raju, 2017):

$$F(r) = [\text{prob (a node exists within r)}]^{\varepsilon_t}$$

$$=[\frac{\pi r^2}{\pi R^2}]^{\varepsilon}$$ (Buttyan & Hubaux, 2007)

$$=\frac{r^{2\varepsilon_t}}{R^{2\varepsilon_t}}$$

In figure 3, an assumed structure of a network that expands circularly has been denoted. The center of the network (i.e. source of the network) is located inside the circle as shown in the figure below. It is presumed that the nodes are distributed evenly across a square area whereby the distance between each neighboring node is known. However, since the expansion has a circular shape, it is required to find the distance of the new node (N2) from a node (N1) that is not directly adjacent to it. For that reason, rather than finding it directly, it is required to find the diagonal distance between the two nodes using the Pythagoras theorem. It is worth noting that the distance between the origin and the first node in the network is already known, represented as O. So, for a network size of X*Y, an average distance between source and destination can be estimated(Buttyan & Hubaux, 2007):

$$d \approx (O+\sqrt{X^2+Y^2})/2 \quad (3)$$

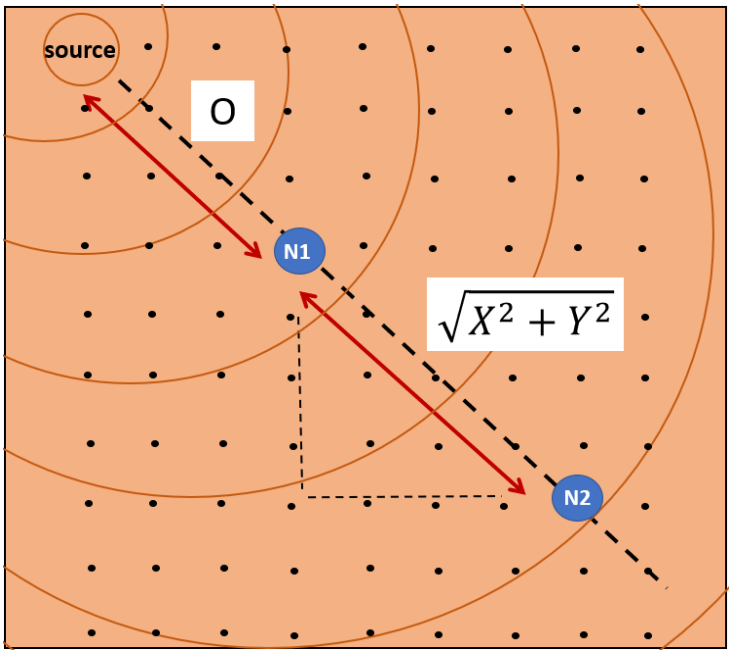

Fig. (3): Self-created: Average Distance between Source and Destination

Consequently, the anticipated number of hops is:

$$h \approx \frac{d}{l} \approx \frac{\sqrt{X^2+Y^2}}{2l} \approx \frac{(2\varepsilon+1)*\sqrt{X^2+Y^2}}{4\varepsilon R} \quad (4)$$

By combining equations (1) and (4), we will obtain the following results:

$$P_r = 1-(1-P_m)^{\frac{(2\varepsilon+1)*\sqrt{X^2+Y^2}}{4\varepsilon R}-1} \quad (5)$$

5. DISCUSSION AND FUTURE WORK

Many studies including a research paper published by (Buttyan & Hubaux, 2007) on an improved DSR protocol called the ST-DSR has shown outstanding performances in terms of lower latency, power efficiency, and in general the overall performance.

This improved protocol has been designed to lower or even mitigate the vulnerabilities of the DSR protocol. However, in this study and others, while performance has been a huge outcome, the delay consequently increases until packets reach their destinations.

As aforementioned, a DSR protocol is known to use the shortest path assuming it to be optimal, which has been proven otherwise in other studies including the one mentioned. For this paper, a different scheme has been suggested in the attempt to also improve the DSR protocol using the methods of the pathrator and 2ACK scheme. It is anticipated that the method of using DSR along with 2ACK and Pathrater will also improve and expand the DSR Protocol's performance in the attempt to route packets in safer paths and therefore minimize the re-routing scenarios that may typically occur otherwise.

For future work, the objective of this research study is to develop a mathematical representation that is subjected to the improved DSR protocols and in turn create a simulation using the Network Simulator 3 (NS-3) to examine the general performance of the DSR protocol after improvements. While many have improved the DSR protocol, an issue often faced is the time delay. Having said that, to further enhance the performance of the DSR protocol, performance delay will be considered.

CONCLUSION

Mobile Ad Hoc networks comprises of a number of distributed mobile nodes with an absence of a centralized infrastructure. Consequently, routing becomes a challenge. Although DSR attributes benefit such networks, it also comes with vulnerabilities. To overcome these vulnerabilities, the DSR protocol will be used the basic protocol with a recommended 2-add on schemes: Pathrater and 2ACK. With these extensions added to the DSR protocol, acknowledgements will be sent to to indicate packet reception along with a module (Pathrater) that syndicates the knowledge of the misbehaving nodes with link reliability so that a route is selected according to its trustworthy likeliness. With these two schemes used as extensions to the DSR protocol we anticipate a mitigation of the adverse effects of misbehaving nodes while tackling the delay outcomes that usually come with better performances of the protocol.

REFERENCE.

Buttyan, L., & Hubaux, J.-P. (2007). *Security and cooperation in wireless networks: thwarting malicious and selfish behavior in the age of ubiquitous computing*: Cambridge University Press.

Goka, S., & Shigeno, H. (2018). *Distributed management system for trust and reward in mobile ad hoc networks.* Paper presented at the 2018 15th IEEE Annual Consumer Communications & Networking Conference (CCNC).

Jain, S., & Khuteta, A. (2015). *Detecting and overcoming blackhole attack in mobile Adhoc Network.* Paper presented at the 2015 International Conference on Green Computing and Internet of Things (ICGCIoT).

Khabir, K. M., Siraj, M. S., Habib, M. A., Hossain, T., & Ahad, M. A. R. (2018). *A study on DSR routing protocol in Adhoc network for daily activities of elderly living.* Paper presented at the 2018 Joint 7th International Conference on Informatics, Electronics & Vision (ICIEV) and 2018 2nd International Conference on Imaging, Vision & Pattern Recognition (icIVPR).

Khan, B. U. I., Olanrewaju, R. F., Anwar, F., Najeeb, A. R., & Yaacob, M. (2018). A survey on MANETs: architecture, evolution, applications, security issues and solutions. *Indonesian Journal of Electrical Engineering and Computer Science, 12*(2), 832-842.

delan.alsofi@uod.ac

Najafi, G., & Gudakahriz, S. J. (2018). A stable routing protocol based on DSR protocol for mobile ad hoc networks. *Int. J. Wirel. Microw. Technol*, *8*(3), 14-22.

Narayana, V. L., & Bharathi, C. (2019). Multi-mode routing mechanism with cryptographic techniques and reduction of packet drop using 2ACK scheme MANETs *Smart Intelligent Computing and Applications* (pp. 649-658): Springer.

Nazih, O., Benamar, N., & Younis, M. (2020). An evolutionary bargaining ‐ based approach for incentivized cooperation in opportunistic networks. *International Journal of Communication Systems, 33*(9), e4377.

Ojha, V. K., Jackowski, K., Snášel, V., & Abraham, A. (2014). *Dimensionality reduction and prediction of the protein macromolecule dissolution profile.* Paper presented at the Proceedings of the Fifth International Conference on Innovations in Bio-Inspired Computing and Applications IBICA 2014.

Poongodi, T., Khan, M. S., Patan, R., Gandomi, A. H., & Balusamy, B. (2019). Robust defense scheme against selective drop attack in wireless ad hoc networks. *IEEE access, 7*, 18409-18419.

Rajeshkumar, V., & Sivakumar, P. (2013). Comparative study of AODV, DSDV and DSR routing protocols in MANET using network simulator-2. *International Journal of Advanced Research in Computer and Communication Engineering, 2*(12), 2319-5940.

Raju, D. K. B. (2017). A Framework for Routing Misbehavior

Recognition in MANETS. *International Journal of Electrical, Electronics and Computers (EEC Journal), Vol-2*(Issue-1, Jan-Feb, 2017). doi:https://dx.doi.org/10.24001/eec.2.1.1

Shrivastava, A. K., & Srivastava, R. Optimization of cooperation in wireless Ad-hoc Network.

Zhang, X., Anpalagan, A., & Guo, L. (2014). *Performance improvement of energy-aware MANET routing algorithm using load-balancing.* Paper presented at the 2014 IEEE 17th International Conference on Computational Science and Engineering.