NC2H: Cooperation Among Nodes through Cluster Head in Ad Hoc Network

Abu Sufian, Anuradha Banerjee and Paramartha Dutta

Abstract In civilian data communication using mobile ad hoc networks (MANETs), all mobile nodes cannot be of homogeneous type and these nodes do not do one specific job or communication. Therefore, cooperation among these nodes is a big issue, which is very essential to successfully run a MANET for this type of data communication. Denial of service and malicious behavior of a node are the main obstacles to a secure and successful communication in this type of a network. This scheme proposed a generic idea to avoid and prevent selfish behavior of a node as well as encourage to increase cooperation among nodes by the cluster head using a single-hop clustering strategy.

Keywords Ad hoc networks · Clustering · MANETs · Networks security · Node cooperation · Selfish attack · Wireless network

1 Introduction

Mobile ad hoc network (MANET) is a kind of network consisting of a collection of mobile nodes which could quickly set up a temporary network, where nodes must be capable of transmitting and receiving radio signals. This MANET is infrastructure-less, self-organizing where nodes are mobile in nature, and could play three kinds of roles: sender, receiver, and router [1]. This type of network has many applications such as data communication in battlefield, communication for rescue operation after a natural disaster, vehicle-to-vehicle communication, communication in a large conference room, and many more [2]. There are several underlined protocols that have

A. Sufian (✉)
University of Gour Banga, Malda, West Bengal, India
e-mail: sufian.csa@gmail.com

A. Banerjee
Kalyani Government Engineering College, Kalyani, West Bengal, India

P. Dutta
Visva-Bharti University, Santiniketan, West Bengal, India

S. Kundu et al. (eds.), *Proceedings of the 2nd International Conference on Communication, Devices and Computing*, Lecture Notes in Electrical Engineering 602, https://doi.org/10.1007/978-981-15-0829-5_14

become standard to set up and exploit this type of network [3]. All these protocols can be broadly classified into three categories: one is proactive where routes are always maintained such as in DSDV [4], WRP [5], FSR [6]; the second category is reactive where a route is established when required such as AODV [7], DSR [8]; and the third category is a mix of the above two where some portion of the network is proactive and the remaining portion is reactive, such as TORA [9], EMR-PL [10], WTMR [16].

In most of the classical routing protocols of MANETs, cooperation among nodes is overlooked. It is a true fact that MANETs are not successfully applied in civilian data communication, and one of the main reasons is the lack of cooperation among participating nodes although it is very successful in specific types of communication such as data communication in battlefield and communication among team members at the time of rescue operation after a natural disaster. As we know, a mobile node has limited resources such as limited residual energy and low bandwidth, some node(s) could be selfish to save these limited resources. This node cooperation problem does not arise in military data communication or any other specific communication using MANETs, because all the nodes in such type of communication are dedicatedly designed for that communication. But in civilian data communication, mobile nodes are of different types such as cell phone, laptop, palmtop, and PDA and these are not designed for specific work. Therefore, cooperation among nodes is very much important here in order to establish a MANET using these nodes of heterogeneous type.

Here, we used a single-hop clustering strategy as a generic mechanism to increase cooperation among nodes through cluster head (CH) by giving reward and punishment in terms of trust value. We know that the clustering scheme is more stable and scalable in nature, especially single-hop clustering schemes [11, 21]. All the nodes are attached with the respective CH directly and the entire network made into different partitions called clusters in the single-hop clustering scheme. All CHs are connected to each other through some gateway nodes and a network is established. CHs will take responsibility for increasing the cooperation among nodes within networks by increasing or decreasing the trust value of the member nodes. This scheme proposes an idea to avoid and prevent the three main selfish attacks, namely **Link Breakage Attack**, **Deleting Route Cache Attack**, and **Deliberately Delay Forward Attack**.

Rest of the paper is organized as follows: in Sect. 2, we discussed the literature review, clustering strategy is briefly discussed in Sect. 3, whereas Sect. 4 explains the proposed solutions to some selfish attacks, and conclusion and future scope in Sect. 5.

2 Literature Survey

So far many node cooperation schemes have been suggested by many researchers. Some prominent schemes are as follows:

L. Buttyan and J.P. Hubaux proposed a scheme called Nuglets [12] to increase cooperation among nodes. They used virtual currency which makes cooperative

nodes to increase node cooperation among the nodes in MANETs. This scheme uses two purse models: one is a Packet-Purse-Model (PPM) where a Nuglet is debited from the source node and the other is Packet-Trade-Model (PTM) where a Nuglet is debited from the destination node of the packet. These authors also explained the utilities and necessity of increasing Nuglets for a node, and also explained the required security of these Nuglets. S. Marti et.al. proposed a similar type of routing scheme based on popular routing DSR [8] to catch a misbehaving node using watchdog and add path quality labels using pathrater [13]. By this portraiture, all participating nodes are classified and then the misbehaving or malicious nodes are avoided. P. Michiardi and R. Molva suggested a scheme called CORE [14] where the reputation of a node is the main concern. This scheme invigorates selfish nodes to quit selfish behavior, for example, clipping denial of service attack. S. Zhong et.al. proposed a credit-based and cheat-proof scheme for MANETs by resolving the selfish behavior of nodes called SPRITE [15]. This is quite similar to the scheme of Nuglets and it is an incentive credit- or debit-based scheme without any tamper-proof hardware. Here, the node gets inceptive by producing acknowledgements of forwarded messages from Credit-Clearance-Service (CCS). F. Kargl et.al. proposed Advanced Detection of Selfish/Malicious Nodes in Ad hoc Networks [17]. In this scheme, activity-based overhearing, iterative probing, and unambiguous probing are used to detect malicious and selfish nodes in the MANETs. N. Kang et. al proposed a misbehaving node detection scheme [18] at the iiWAS 2010 conference. This scheme applies different Intrusion-Detection-System (IDS) equivalent to watchdog to detect malicious/selfish nodes. IDS has been used to overcome the limitation of the uses of watchdog.

E. Hernandez Orallo et.al. proposed a model called CoCoWa [19]. Here, the authors have used a collaborative contact-based watchdog to efficiently detect selfish nodes in a short period of time. The CoCoWa model uses collaborative work, based on the diffusion awareness of local selfish nodes instead of fully depending on watchdog because watchdog also could be selfish. J.M. Chang et.al. proposed another node cooperative called Cooperative Bait Detection Approach (CBDS) [20] on the concepts of DSR [8]. This scheme can be embedded in both proactive and reactive routing. A reverse tracing approach is used here to resist a collaborative attack by malicious or selfish nodes. S. Berri et.al. proposed another reputation-based node cooperation scheme [22]. They use a similar kind of approach to increase node cooperation by adding or deducting the reputation of nodes within the MANET. But here the amount of reputation, loss or increase depend on the service taker node. If a node denies giving service to a reputed node, then the reputation loss will be more compared to denying service to less-reputed nodes and vice versa.

In C3H [21], the same authors of this paper use the single-hop node clustering strategy to prevent the malicious activity of any internal node of the network through cluster heads. This scheme explains the prevention of malicious attacks by giving future scope to increase cooperation among nodes using the same strategy. The current scheme, NC2H based on the concepts of C3H and single hop clustering scheme FESC [11].

3 Clustering Strategy for Monitoring Behavior of Nodes

The two main challenges along with many challenges for routing in MANETs are lack of centralized control and high mobility of nodes. These are the reasons why classical routing protocol of infrastructure-based networks do not work for mobile ad hoc networks. Clustering routing protocols in MANETs try to get some benefit of those classical routing protocols by mimicking the topology of these classical routing protocols. Here, we have adopted FESC [11], a single-hop clustering strategy, and some modifications made to cheat proof in C3H [20] for increasing the cooperation among nodes in ad hoc networks. There are three types of nodes in this scheme, namely cluster head (CH), ordinary member node, and gateway node. This single-hop clustering scheme proposed a technique where a member node is directly attached to the elected CH and breaks the entire network into some clusters. The cluster heads (CHs) are elected temporarily among member nodes. The election is done according to high residual energy, high trust value, low mobility of nodes, and strong connectivity to downlink nodes compared to other nodes of the cluster. Electing a good candidate as the cluster head is very important as this node will monitor the activities of the other nodes; this procedure is clearly defined in our earlier scheme C3H [21].

3.1 Graphical Explanation of the Strategy

Let us consider Fig. 1 where a small MANET containing two selfish nodes *a* and *q* have been shown. These two selfish nodes could carry out three kinds of selfish attacks which are mentioned in Sect. 4.

In this scheme, selfish attacks could be prevented through CHs. The nodes *p*, *r*, and *c* mentioned in Fig. 1 become cluster heads CH1, CH2, and CH3 in Fig. 2. CH1

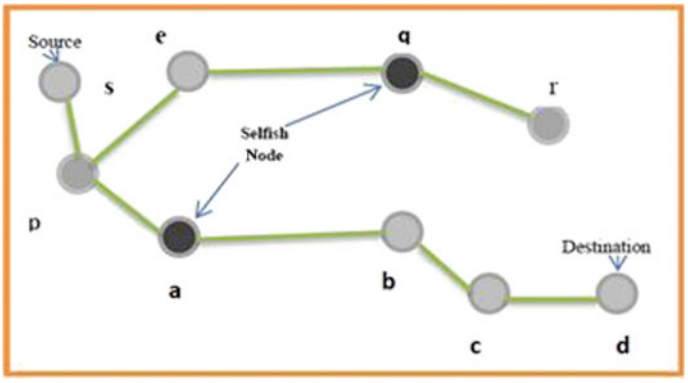

Fig. 1 A small MANET with two selfish nodes

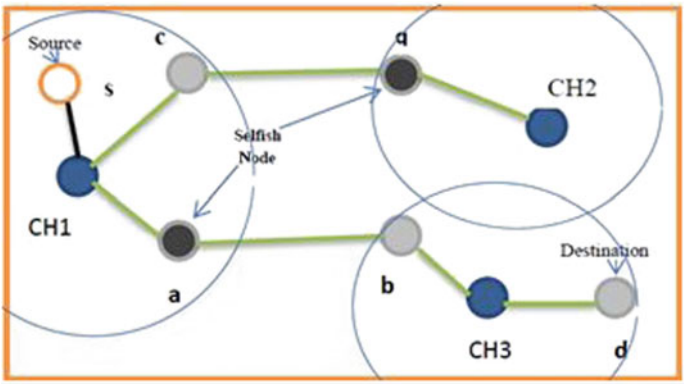

Fig. 2 Selfish nodes controlled by CHs

and CH2 could monitor the selfish nodes a and q as their respective cluster heads. The cluster heads give reward or punishment to the respective member nodes according to their participation or selfishness. The objective is clear that it is to increase node cooperation within networks and avoid selfish attacks.

3.2 Trust Value Calculation of Node

At the initial stage, that is when a node enters the network, 0.5 assigns as a default trust value, where $trust\_value$ is a variable whose values are between 0 and 1, which indicate the trust level of a node. There are two additional support variables, one is $earn\_trust$ which is a natural number starting from 2, and second one is $lose\_trust$ which is also a natural number starting from 1 up to the current $earn\_trust$.

Initial value assigned to $earn\_trust$ is 2 and $lose\_trust$ is 1 when a node joins the network for the first time. For a successful transfer of one packet, a node increases its $earn\_trust$ value by 1 unit. Similarly, if any kind of selfish behavior is shown, $lose\_trust$ value decreases by 1 unit from the responsible node. The entire activity is carried out by the cluster head. The current $trust\_value$ of a node is calculated by Eq. (1).

$$trust\_value = 1 - lose\_trust/earn\_trust \tag{1}$$

Trust value is very important for a node as this node will request for its own data packet transfer to the CH. Depending on the current $trust\_value$, a packet transfer request of a node could be granted by the respective CH.

4 Several Selfish and Security Issues and Respective Proposed Solutions

Besides many difficulties, MANETs face two serious difficulties which are selfish behavior and malicious behavior of the node. These difficulties arise within the network by some selfish or malicious node(s). According to the behavior of the mobile node, all nodes of a network can be classified into three categories, namely malicious node, selfish node, and normal node. The behavior of malicious and selfish nodes is the main concern. The malicious activity could be avoided using C3H [21], where a similar clustering tactic is used, and selfish activity can be prevented by motivating to increase the cooperation among nodes, which is the main objective of this proposed scheme.

Selfish node will try to save its resources such as energy and bandwidth as much as possible so that it could use them for its own communication in the near future. Therefore, these types of nodes try to avoid participating in communications with other nodes. Mainly, three types of selfish behavior or attack might come from selfish nodes, namely Link Breakage Attack, Deleting Route Cache Attack, and Deliberately Delay Forward Attack. These are discussed in Sects. 4.1, 4.2, and 4.3, respectively.

4.1 Link Breakage Attack

Some selfish node remains silent on receiving an RREQ packet from other nodes although it might have information about the intended destination. The objective of this kind of node is to save its own resources by avoiding to participate in the communication link of other nodes.

In this scheme, CHs identify those selfish nodes and reduce the trust values of those selfish nodes. The CHs also increase the trust value of those nodes which actually participate in communication with other nodes. Both increases and decreases in trust values are calculated by Eq. (1). As discussed earlier in this section that CHs are trustworthy nodes, link breakage attack can only arise from member nodes. Some member node selfishly tries to avoid becoming a gateway node. But in this scheme, the CH of a cluster monitors other cluster members. Whenever a route needs to be set up, the source node sends an RREQ packet to its CH, then the CH broadcasts this RREQ packet to the neighbor CHs through some member node called the gateway node (if the destination is not within the cluster). If some node remains silent after receiving the RREQ packet, the CH checks the residual energy level and the position of that node, then tries to find out the reasons why the node was unwilling to become a gateway node. If this reason is not sufficient to convince the CH, then CH reduces the trust value of that selfish node and informs the other stakeholders of this network. Similarly, CH also increases the trust value of the node for positive behavior.

4.2 Deleting Route Cache Attack

In MANETs, every node maintains a cache memory where information about the last few communications are stored. Selfish node could delete such information from its cache so that other nodes may avoid this node in future communication. In this way, the selfish node gets the chance to save its own resources.

As it was mentioned earlier, CH takes all the responsibility to store the routing information, and information not required from ordinary members. It is assumed that CHs are trusted nodes; therefore, the deleting route cache problem does not occur in this scheme. The role of the CH is very crucial, therefore, the optimum node must be the CH of a cluster at any instance. Whenever a CH hands over the charge to any other node, the routing information is also handed over.

4.3 Deliberately Delay Forward Attack

Selfish node could deliberately delay forwarding the packet of the other nodes so that those nodes could avoid this selfish node for future communication. In this way, a selfish node avoids participating in communication with other nodes.

In any instance of communication, a source node, a destination node, CH(s), and none or more gateway node(s) participate. But as mentioned earlier that CHs are the most trusted nodes and no question arises for a source and a destination node, if a delay arises, then gateway node(s) will be responsible. Any gateway node directly connects to its CH, so the gateway node either receives or delivers data packets to its CH. On the other hand, before communication starts, the route establishment phase has to complete, and at that time, the CH becomes aware of the possible time to get the data packets from the predecessor CH, and to send data packets to the successor CH. Later in communication time, if actual time does not match the estimated time approximately, then delay attack arises. The CHs then check their gateway node(s) whether the delay arises deliberately or for some other reasons. In both cases, an alternate gateway node can be selected if available, otherwise, communication will continue, but for deliberate delay, the identified gateway node gets punished by reducing the trust value of that selfish node using Eq. (1).

5 Conclusion and Future Scope

Through this NC2H single-hop clustering scheme for increasing cooperation among nodes, Link Breakage Attack, Deleting Route Cache Attack, and Deliberately Delay Forward Attack can be avoided. This NC2H could be useful to avoid other selfish attacks in ad hoc networks. The NC2H shall be implemented with standard baseline routing protocols. This scheme supposes that cluster head (CH) is the most trust-

worthy node, which is elected based on the single-hop clustering models, FESC, and C3H. In future work, election of CH node could be done in a more intelligent way where more parameters could be used so that the purpose of this NC2H scheme will be fulfilled more accurately.

References

1. Toh, C.K.: Ad Hoc Mobile Wireless Networks: Protocols and Systems, 1st edn. Prentice Hall PTR (2002)
2. Helen, D., Arivazhagan, D.: Applications, advantages and challenges of Ad Hoc networks. J. Acad. Ind. Res. (JAIR) **2**(8), 453–457 (2014)
3. Abolhasan, M., Wysocki, T., Dutkiewicz, E.: A review of routing protocols for mobile ad hoc networks. Ad Hoc Netw. **2**(1), 1–22 (2004)
4. Perkins C.E., Bhagwat P.: Highly Dynamic Destination-sequenced Distance-vector Routing (DSDV) for Mobile Computers, pp. 234–245. SIGCOMM ACM (1994)
5. Murthy, S., Aceves, J.J.G.L.: An efficient routing protocol for wireless networks. Mobile Netw. Appl. **1**(2), 183–197 (1996)
6. Pei, G., Gerla, M., Chen, T.W.: Fisheye state routing: a routing scheme for ad hoc wireless networks. In: IEEE International Conference on Communications. Global Convergence through Communications (2000). https://doi.org/10.1109/ICC.2000.853066.
7. Perkins C.E., Royer E.M.: Ad-Hoc On-demand Distance Vector Routing (1998). draft-ietf-manet-aodv-02.txt
8. Johnson, D.B., Hu, Y., Maltz, D.A.: The Dynamic Source Routing Protocol (DSR) for Mobile Ad Hoc Networks for IPv4. IETF Req. Comments **4728** (2007)
9. Park, V. Corson, S.: Temporary-Ordered Routing Algorithm (TORA). Internet Draft, draft-ietf-manettora-spec-04.txt, (2001)
10. Banerjee, A., Sufian, A., Duta, P.: EMR-PL: energy-efficient multipath routing based on link life prediction in ad hoc networks. J. Inform. Optim. Sci. **39**(1), 285–301 (2018). https://doi.org/10.1080/02522667.2017.1374733
11. Banerjee, A., Duta, P., Sufian, A.: Fuzzy-controlled energy-efficient single hop clustering scheme with (FESC) in Ad Hoc networks. Int. J. Inform. Technol. **10**(3), 313–327 (2018)
12. Buttyan, L., Hubaux, J. P.: Nuglets: a Virtual Currency to Stimulate Cooperation in Self-Organized Mobile Ad Hoc Networks (2001). http://infoscience.epfl.ch/record/52377
13. Marti, S., Giuli, T.J., Lai. K., Baker, M.: Mitigating Routing Misbehavior in Mobile Ad Hoc Networks, MOBICOM. ACM, USA (2000). 1-58113-197-6
14. Michiardi, P., Molva, R.: COre: a collaborative reputation mechanism to enforce node cooperation in mobile Ad Hoc Networks. Adv. Commun. Multimed. Secur., IFIP Int. Federation Inform. Process. (2002). https://doi.org/10.1007/978-0-387-35612-9_23
15. Zhong, S., Chen, J., Yang, Y.R.: SPRITE: A Simple, Cheat-Proof, Credit-Based System for Mobile Ad-Hoc Networks. IEEE INFOCOM (2003). 10-7803-7753-2/03
16. Sufian, A., Banerjee, A., Dutta, P.: Energy and velocity based tree multicast routing in mobile Ad-Hoc networks. Wirel. Personal Commun. **107**(4), 2191–2209 (2019). https://doi.org/10.1007/s11277-019-06378-y
17. Kargl, F., Klenk, A., Schlott, S., Weber, M.: Advanced detection of selfish or malicious nodes in Ad Hoc networks. Lect. Notes Comput. Sci. (2014). https://doi.org/10.1007/978-3-540-30496-8_13
18. Kang, N., Shakshuki, E. M., Sheltami, T. R.:Detecting misbehaving nodes in MANETs. In: Proceedings of the 12th International Conference on Information Integration and Web-based Applications and Services, pp. 216-222 (2010). https://doi.org/10.1145/1967486.1967522.

19. Orallo, E.H., Serrat, M.D., Olmos, Cano, J.C., Tavares De Araujo Cesariny Calafate, CM.; Manzoni, P, CoCoWa: A collaborative contact-based watchdog for detecting selfish nodes. IEEE Trans. Mobile Comput. **14**(6), 1162–1176 (2015). https://doi.org/10.1109/TMC.2014.2343627
20. Chang, J.M., Tsou, P.C., Woungang, I., Chao, H.C., Lai, C.F.: Defending against collaborative attacks by malicious nodes in MANETs: a cooperative bait detection approach. IEEE Syst. J. **9**(1) (2015)
21. Sufian, A., Banerjee, A., Dutta, P.: Cheat proof Communication through cluster head (C3H) in mobile Ad Hoc network. Pertanika J. Sci. Technol. **26**(3), 1513–1526 (2018)
22. Berri, S., Varma, V., Lasaulce, S., Radjef, M. S., Daafouz, J.: studying node cooperation in reputation based packet forwarding within mobile Ad Hoc networks. In: International Symposium on Ubiquitous Networking UNet 2017, vol. 10542. Morocco, LNCS (2017)