International Journal of Knowledge Based Computer Systems
10 (1) June 2022, 10-16
http://www.publishingindia.com/ijkbcs/

Find_S Algorithm: To Detect Node Behaviour in Ad Hoc Network

Samara Mubeen
Assistant Professor, Department of IS&E, Jawaharlal Nehru National College of Engineering, Shivamogga, Karnataka, India. Email: samaramubeen@jnnce.ac.in

Abstract: As humans have different behaviour good and bad. Some of the behaviour the human has kind, selfish, cooperative, uncooperative, gentle, soft hearted, back biting, jealous etc. Similarly, nodes in the Ad Hoc network have different behaviour like selfish nodes, regular nodes, malicious nodes etc. Transferring the information from the source node to the destination node via intermediate nodes is done using different routing algorithms. Routing algorithms find out the optimal path to reach the destination. They fail to identify the behaviour of the nodes when transferring the information. Identification of the nodes whether they are good or bad is a difficult task. In this paper different dataset having different behaviour are collected. Find_S algorithm is used to analyze the dataset and give the correct hypothesis as output. The hypothesis consists of different attributes like nature of the agent, energy level, type of agent, and finally, is the decision of the node.

Keywords: Dataset, Find_S algorithm, Node behaviour, Regular node, Selfish node.

I. Introduction

Ad Hoc network is infrastructure less network in which the nodes communicate with one another directly. The device themselves act as the router for forwarding of the packet from one node to another node until it reach the destination. As human being has different behaviour at different time, even the nodes in the Ad Hoc network have different behaviour. Some of the behaviour of the nodes is regular node, selfish node and malicious node. The regular node is the one which forwards the packet to neighbouring node until all the energy within it is exhausted. The selfish node is the one which behaves as regular node but after sometime the node stop forwarding the packet even the energy is there for forwarding. The selfish nodes want to preserve their resource. The malicious node is the one which will cause many problems in the network. Some of the behaviour exhibited by the malicious node are dropping of the packet, by performing unnecessary operation draining of the battery, simply consumes or drops the packet and does not forward it. To analyze this behaviour, the different dataset are considered.

Ever since computers were invented, the question arises whether they might be made to learn. To understand how to program them to learn, to improve automatically with experience, imagine computers learning from medical records which treatments are most effective for new diseases, houses learning from experience to optimize energy costs based on the particular usage patterns of occupants, or personal assistants learning the evolving interests of their users in order to highlight especially relevant stories from the online morning newspaper. A successful understanding of how to make computers learn would open up many new uses of computers and new levels of competence and customization. As the understanding of computers continues to mature, it seems inevitable that machine learning will play an increasingly central role in computer science and computer technology.

Find_S algorithm is used for finding the best hypothesis. The Find_S algorithm illustrates a way in which the more_general_than partial ordering can be used to organize the search for an acceptable hypothesis. The search moves from hypothesis to hypothesis, searching from the most specific to progressively more general hypotheses along one chain of the partial ordering. The algorithm of Find_S is given below.

Algorithm 1: Find_S Algorithm

1. Initialize h to the most specific hypothesis in H.
2. For each positive training instance x
   For each attribute constraint a_i in h
   If the constraint ai is satisfied by x
   Then do nothing
   Else replace a_i in h by the next more general constraint that is satisfied by x
3. Output hypothesis h

Paper is organized as follows: Introduction in Section I, Literature Review in Section II, System Design of Regular and Selfish Nodes in Ad Hoc Network considered in Section III,

in Section IV Implementation and Result Analysis followed by Conclusion in Section V.

II. Literature Review

Mohammad Ahmed Ahmed Al-JAoufi *et al.*, "Study of selfish node incentive mechanism with a forward Game node in wireless Sensor Networks", International Journal of Antennas and Propagation. Selfish node do not cooperate in forwarding of the packets and preserve their own limited resource [1]. Evolutionary game theory concept implemented into the nodes of the wireless sensor network to improve the reliability and stability of the network. The results of the simulation show that they use incentive mechanism for forwarding packets. By this stability and reliability of wireless sensor networks are improved.

Enrique Hernandrez Oralla *et al.*, "Improving selfish node detection in MANETs using a collaborative watchdog", IEEE Communications Letters, vol. 16, No. 5 May 2012 [2]. MANET do not use pre existent infrastructure. To save its resource selfish nodes will not forward their packets. Watchdogs are used to detect selfish nodes to improve accuracy and reduction of detection time. Collaborative watchdog can reduce the overall detection time with a reduced overhead.

Sonja Buchegger and Jean-Yves Le Boudee, "Self policing Mobile Ad Hoc Networks by Reputation System", The performance of the Mobile Ad Hoc network decrease due to the presence of selfish or malicious nodes. Some problems are eliminated by using incentives or secure routing by crypto-graphy [3]. By using a reputation system in all nodes makes them detect misbehaviour and use of second hand information.

Neenavath Veeraiah and B. T. Kaishna, "Selfish node detection IDSM based approach using Individual master cluster node", Manet is a group of infrastructure less network. Every node in the network is responsible for forwarding packets to its neighbouring nodes. The selfish node behaviour presence leads to partition of the network and makes a negative impact in the operation of the network. There are lots of techniques to identify the selfish node where more computational resources and time consuming process to identify selfishness of the node [4]. The selfish node is detected for single node and the clustering is used to increase the efficiency and also reduces the network energy consumption which leads in the reliable quality services throughout the network.

Shailender Gupta, C. K. Nagpal and Charu Singla, in MANET node should perform the community service truthfully [5]. In community service each node relays data packets of other nodes by spending their resources. A selfish node present in the MANET uses the network resources for its own profit but avoid helping others for preserving its resources. If number of selfish nodes increases in MANET, will eventually disrupt the network. Here the impact of selfish nodes concentration on quality of service in MANETs.

Naveen Kumar Gupta, Ashish Kumar Sharma and Abhishek Gupta [6], Wireless interfaces will be common in Ad Hoc networks, here relaying of packets among nodes are done without base stations. Selfish nodes are present in the Ad Hoc network that will degrade the whole network. A comparison study of different methods which will detect the increase in selfish node and decrease in the false detection rate. To detect them a simulation model is used which will detect the increase of selfish node and decrease of false detection rate.

Ashraf Al Sharah, Mohammad Alhaj and Mohammad Hassan [7], In mobile Ad Hoc network nodes organizing themselves in a non-centralized form for forwarding of the information. Selfish node exists in the network which will utilize the resource from for their own benefits. In this paper a selfish dynamic punishment scheme is used for using the cooperative repeated game in Mobile Ad Hoc network, by using this approach the selfish nodes are motivated to cooperate. The cooperative punishment is pertain to all network nodes, so that punished node is simulated for cooperating with other nodes in the MANET.

MANET becomes an encouraging area for innovative work of wireless communication system [8]. The Intrusion detection system observes for doubtful actions inside a system and takes action against them. In their research work a specially designed MANET's known as Enhanced Adaptive Acknowledgement system is discussed. This scheme solves all the problems of existing intrusion detection systems and the presence of false misbehaviour report.

New routing techniques which incorporate security attributes as parameter into Ad Hoc route discovery called Security-Aware Ad Hoc routing [9]. SAR enables the use of security as a metric to improve the relevance of the routes discovered by Ad Hoc routing protocols. Framework enables applications to adapt their behaviour according to the level protection available on communicating nodes in an Ad Hoc network. A wireless Ad Hoc network is a temporary network in which nodes are moving arbitrary in the places that have no network infrastructure [10]. Here a new routing algorithm Ad Hoc On-Demand Distance Vector with Black-hole Avoidance used to avoid black hole attack. Non-malicious nodes gradually isolate the black-hole nodes based on the values collected in their legitimacy table and avoid them while making path between source and destination.

A security threats against Ad Hoc routing protocols, examining AODV and DSR. A solution is proposed where no network infrastructure is pre-deployed [11]; a small amount of security coordination is expected. The protocol ARAN is based on certificates and successfully defeats for all identified attacks. In MANET's any node under attack exhibits an anomalous behaviour called malicious behaviour [12]. Here the entire operation of a network gets disturbed. In this work malicious node behaviour is defend and security solution are presented which are used in furnishing a secure and reliable communication in Ad Hoc.

III. System Design of Regular and Selfish Nodes in Ad Hoc Network

The Fig. 1 shows the behaviour of the regular node in Ad Hoc network, when the nodes are regular. The source node broadcast the hello packet to know the nodes welling to forward the packets, in response the nodes will send the acknowledgement to the source node willing to forward the packet. The source node will send the packet to the neighbouring node. The neighbouring node will send the packet to its neighbour until the final destination node is reached.

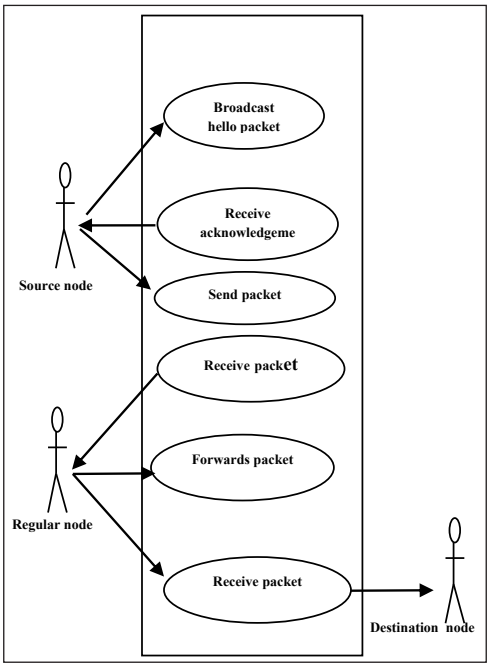

Fig. 1: Behaviour of Regular Node

Fig. 2 shows how the node will behave when selfish node is present in the network. The source node will broadcast the hello packet; the selfish node will send the acknowledgement will to forward the packet. Selfish node will receive the packet forwarded from the source node, due to its selfish behaviour it will not forward the packet to the neighbouring node as result the packet will not be received by the destination node. If the source node identifies the presence of selfish node the packet can be forwarded to the regular present in the network and the packet will reach the destination node.

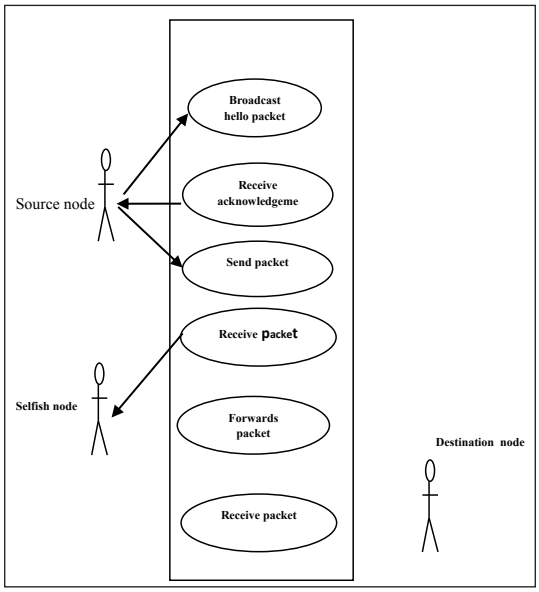

Fig. 2: Behaviour of Selfish Nodes

IV. Implementation and Result Analysis

The Fig. 3 shows the flowchart which represents the implementation done in order analysis the behaviour of the nodes in Ad Hoc.

The flowchart begins with dataset set given as input to the Find_S algorithm. A hypothesis is generated as output; this is checked with the regular behaviour of the node. If the node is regular then the packet is forwarded to the node and if not the packet is not forwarded to the node in the Ad Hoc network.

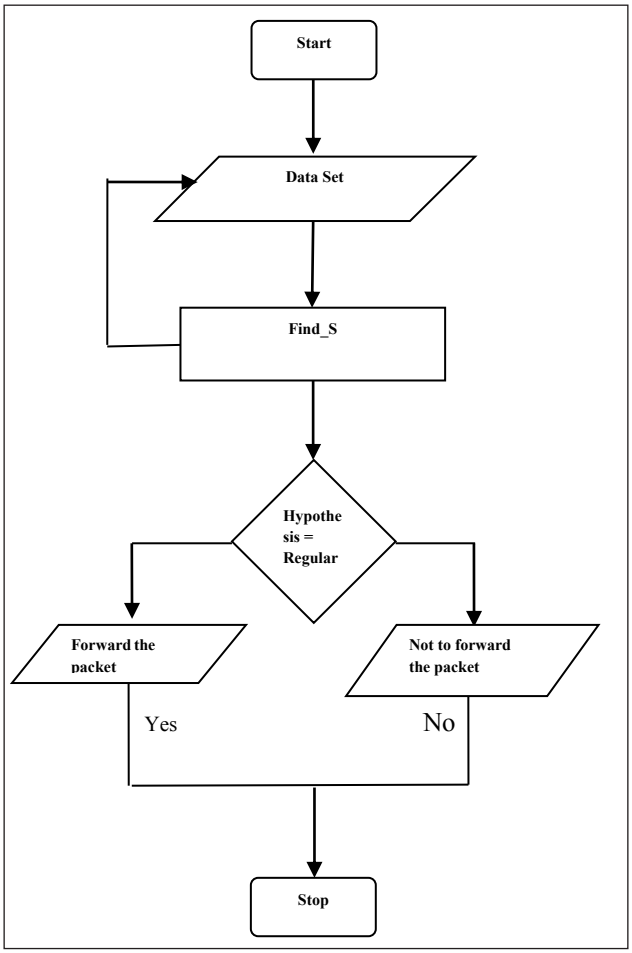

Fig. 3: Flowchart for Making Decision for Forwarding of the Packet

Case Studies on Different Dataset for Finding the Behaviour of the Node using Find_S Algorithm

In implementation four different cases are discussed having same attributes and different values. The attributes considered for dataset for finding the behaviour of the nodes are nature of the agent of the node whether they are good or bad, good means these nodes always helps in forwarding of the information to other nodes, bad means these nodes are not involved in forwarding of the information. The second attribute considered is the energy level in which the energy level can be high or medium represented as HM, energy level low is represented as L. The type of agent is classified as regular node represented as R or selfish node represented as S. Decision of node is last attributes in the table which justify the node behaviour whether to forward the information to next node is represented by F or not forwarding of the information is represented by NF which not forwarding.

Case 1: When Nodes are Regular and Packets can be Forwarded

The Table I shows dataset of the behaviour of regular and selfish nodes. The dataset consist of good and bad nodes by nature having energy level high or medium or low level, agent type is regular or selfish and the behaviour of the node is given by F or NF. The dataset consist of good natured nodes, bad natured nodes are countable. This dataset is given as input to the Find_S algorithm.

Table I: Behaviour of Regular Nodes Chosen to the Forward the Packet

Nature of the Agent	Energy Level	Type of Agent	Decision of Node
Good	HM	R	F
Good	HM	R	F
Bad	HM	R	NF
Good	HM	R	F
Good	L	R	NF
Bad	HM	R	NF
Good	L	S	NF
Bad	HM	R	NF
Good	HM	R	F
Good	HM	R	F
Good	HM	R	F
Good	HM	R	F
Bad	HM	R	NF
Good	HM	R	F
Good	L	S	NF
Good	HM	R	F
Good	L	S	NF
Bad	HM	R	NF
Bad	L	S	NF
Good	HM	R	F
Good	H	R	F
Good	L	S	NF
Bad	L	R	NF
Good	H	S	NF
Good	H	S	NF
Bad	H	S	NF
Good	H	R	F

The output of the Find_S algorithm is given below:

OUTPUT: [Good,?, R], Decision to forward = F

The hypothesis obtained as output shows that if the dataset has good nodes by nature along with energy level can be low, high or medium and the agent is regular. The final decision is to forward the information to next node in the network.

Case 2: When Nodes are not Regular and Forwarding of Packets can be Avoided

Table II is the dataset which consist of same attributes with different values. The dataset consists of bad and good natured nodes.

Table II: Behaviour of Regular Nodes Chosen to the Not to Forward the Packet

Nature of the Agent	Energy Level	Type of Agent	Decision of Node
Good	L	S	NF
Good	HM	R	F
Bad	HM	SR	NF
Good	HM	R	F
Good	L	R	F
Bad	HM	SR	NF
Bad	L	S	NF
Bad	HM	R	NF
Good	HM	R	F
Good	HM	R	F
Bad	HM	R	NF
Good	HM	R	F
Bad	HM	R	NF
Good	HM	R	F
Good	L	S	NF
Good	HM	S	NF
Good	L	S	NF
Bad	L	R	NF
Good	H	S	NF
Good	H	S	NF
Bad	H	R	NF

This is fed to the Find_S algorithm the output obtained from the decision is given below:

OUTPUT: [Bad, ? ,?] Decision to forward = NF

The nature of the agent is bad, having energy level low, medium or high and the type of agent can either be selfish or regular, the decision is not to forward the packet to this node.

Case 3: When Nature of Nodes is Good and Energy Level is Low Forwarding of Packets can be Avoided

The Table III shows the dataset in which there are both good and bad natured nodes by nature, their energy level is low and type of node is selfish.

Table III: Behaviour of Regular Nodes Not Regular Chosen to the Not to Forward the Packet

Nature of the Agent	Energy Level	Type of Agent	Decision of Node
Good	HM	R	F
Good	HM	R	F
Bad	HM	R	NF
Good	HM	R	F
Good	L	R	NF
Bad	HM	R	NF
Good	L	S	NF
Bad	HM	R	NF
Good	HM	R	F
Good	HM	R	F
Good	HM	R	F
Good	HM	R	F
Bad	HM	R	NF
Good	HM	R	F
Good	L	S	NF
Good	HM	R	F
Good	L	S	NF
Bad	HM	R	NF
Bad	L	S	NF
Good	HM	R	F
Good	H	R	F
Good	L	S	NF
Bad	L	R	NF
Good	H	S	NF
Good	H	S	NF
Bad	H	S	NF
Good	H	R	F

When this dataset is given to the Find_S algorithm the hypothesis obtained is shown below:

Output: [?, ?, ?] Decision to forward = NF

The nature of agent is good, energy level is low, high or medium

and the type of agent is selfish or regular. These types of nodes having the behaviour pattern are avoided from forwarding of the information.

Case 4: When Nodes by Nature are Good, Energy Level is Low, Medium or High

Table IV shows the good or bad nature of nodes having energy levels low and high or medium represented by HM. This dataset is fed as input to the Find_S algorithm.

Table IV: Behaviour of Regular Nodes Not Regular Chosen to the Not to Forward the Packet

Nature of the Agent	Energy Level	Type of Agent	Decision of Node
Good	L	S	NF
Good	HM	S	NF
Bad	HM	SR	NF
Good	HM	S	NF
Good	L	S	NF
Bad	HM	SR	NF
Bad	L	S	NF
Bad	HM	R	NF
Good	HM	S	NF
Good	HM	R	F
Bad	HM	R	NF
Good	HM	R	F
Bad	HM	R	NF
Good	HM	R	F
Good	L	S	NF
Good	HM	S	NF
Good	H	S	NF
Good	H	S	NF
Bad	H	S	NF
Good	H	R	F

The hypothesis obtained is given below:

Output hypothesis [?, ?, ?] Decision to Not forward = NF

The node having these values is not allowed to forward the information.

Discussion on the Result Obtained

The above cases show the different behaviour of the nodes. By knowing the behaviour of the nodes in a particular environment, the presence of the selfish nodes can be completely eliminated. By taking precaution earlier from the test cases available. This will help to overcome problem of identification of the selfish nodes in the network of Ad Hoc network provided that the dataset of the about the behaviour of the nodes are available earlier.

V. Conclusion

As human have different behaviour similarly nodes in Ad Hoc network are having different behaviour, in this paper different dataset is used, having attributes like Nature of the Agent, Energy Level, Type of Agent and Decision of node are considered. Using Find_S algorithm the behaviour of the node is recorded for each run. By this we can classify the node as selfish or regular node in Ad Hoc network. The elimination of the regular node. If the nodes which are selfish can be completely eliminated from the network before forwarding of the packets or information is done, by doing in this way speed of the packet reaching the destination is speeded and along with that misbehaving nodes are completely eliminated from the Ad Hoc network.

References

[1] Mohd. A. A. Al-Jaoufi, Y. Liu, Z.-J. Zhang, and L. Uden, "Study on selfish node incentive mechanism with a forward game node in wireless sensor networks," *International Journal of Antennas and Propagation*, vol. 2017, 2017.

[2] E. Hern´andez-Orallo, M. D. Serrat, J.-C. Cano, C. T. Calafate, and P. Manzoni, "Improving selfish node detection in MANETs using a collaborative watchdog," *IEEE Communications Letters*, vol. 16, no. 5, pp. 642-645, May 2012, doi: 10.1109/LCOMM.2012.030912.112482.

[3] S. Buchegger, and J.-Y. Le Boudec, "Self-policing mobile ad-hoc networks by reputation systems," in National Competence Center in Research on Mobile Information and Communication Competence Center in Research on Mobile Information and Communication Systems (NCCR-MICS).

[4] Neenavath, and B. T. Krishna, "Selfish node detection IDSM based approach using individual master cluster node," in *2nd International Conference on Inventive Systems and Control*, 2018.

[5] S. Gupta, C. K. Nagpal, and C. Singla, "Impact of selfish node concentration," *International Journal of Wireless & Mobile Networks*, vol. 3, no. 2, Apr. 2011.

[6] N. K. Gupta, A. K. Sharma, and A. Gupta, "Selfish behaviour prevention and detection in mobile ad-hoc network using intrusion prevention system (IPS)," *International Journal of Research Review in Engineering Science and Technology*, vol. 1, no. 2, pp. 31-34, Sep. 2012.

[7] A. Al Sharah, Mohd. Alhaj, and Mohd. Hassan, "Selfish dynamic punishment scheme: Misbehavior detection

in MANETs using cooperative repeated game," *International Journal of Computer Science and Network Security*, vol. 20, no. 3, pp. 158-173, Mar. 2020.

[8] V. U. Raut, and M. S. Mahindrakar, "A comprehensive survey on intrusion detection in MANET," *International Journal of Information Technology and Knowledge Management*, vol. 2, no. 2, pp. 305-310, Jul.-Dec. 2010.

[9] S. Yi, P. Naldurg, and R. Kravets, "Security-aware ad hoc routing for wireless networks," in *Proceedings of ACM MOBIHOC*, Oct. 2001, pp. 299-302.

[10] Y.-C. Hu, D. B. Johnson, and A. Perrig, "SEAD: Secure efficient distance vector routing for mobile wireless ad hoc networks," in *Proceedings of the 4th IEEE Workshop on Mobile Computing Systems and Applications*, Callicoon, NY, Jun. 2002, pp. 3-13.

[11] K. Sanzgiti, B. Dahill, B. N. Levine, L. Y. Clay, S. Elizabeth, and M. Belding-Royer, "A secure routing protocol for ad hoc networks," in *Proceedings of the 10th IEEE International Conference on Network Protocols (ICNP'02),* Nov. 2002, pp. 78-87.

[12] Z. Alfawaer, and S. Al Zoubi, "A proposed security subsystem for ad hoc networks," *International Forum on Computer Science Technology and Applications*, IEEE, 2009.