Research Journal of Applied Sciences, Engineering and Technology 4(3): 201-205, 2012
ISSN: 2040-7467

Submitted: September 23, 2011 Accepted: November 02 , 2011 Published: February 01, 2012

Cooperative Reputation Index Based Selfish Node Detection and Prevention System for Mobile Ad hoc Networks

[1]Muhammad Arsalan Paracha, [2,3]Shiraz Ahmad, [1]Adeel Akram and [4]Muhammad Waqas Anwar
[1]Department of Computer Engineering, University of Engineering and Technology, Taxila 47080, Pakistan
[2]Pakistan Atomic Energy Commission (PAEC), Islamabad 44000, Pakistan
[3]Centres of Excellence in Science and Applied Technologies (CESAT), National Engineering and Scientific Commission (NESCOM), Islamabad 44000, Pakistan
[4]Department of Computer Sciences, COMSATS Institute of Information Technology, Abbottabad, Pakistan

Abstract: In Ad hoc networks every node plays an important part in the transmission of packets from sender to receiver. Most of the time packet delivery ratio of these networks depends on the behavior of intermediate nodes. Sometimes these intermediate nodes cooperate and forward the packets of their neighbor and some time they simply drop their packets and cheat their neighbors. We present a solution that not only detect these selfish nodes but also punish these nodes so that they avoid such misbehavior in future. To this account, we use an agent "Neighbor Monitor", running on every node, to monitor the traffic of neighbors and assign a value called "Reputation Index", associated with each node, based on its behavior.

Key words: Ad-hoc network, reputation index, reputation threshold, selfish node

INTRODUCTION

The wireless communication technology offers a great flexibility and seamless mobility. It will make computing even more pervasive in our lives, providing us a platform to develop novel applications for medical, security and entertainment. One significant paradigm of wireless communication is ad-hoc networks. These networks can be formed dynamically by a group of wireless mobile nodes, without assistance and fairly easily, and connect to fixed communication sites such as base stations or access points. In ad-hoc networks, power limitation is a major constraint in the packet transmission and the information communication of mobile nodes. Since there is no permanent infrastructure for communication of packets therefore transmission between the two potentially communicating nodes which are not in each other's range depends on the intermediate nodes for packet forwarding. This intermediate node plays a vital role in the transmission of packets from source to destination. Sometimes these intermediate nodes drop the packets to save their resources. These nodes are named as "Selfish Nodes" for their selfish nature of staying in the network only for their own welfare.

Selfish nodes can generate many problems in a network because they preserve their own resources while utilizing resources of the other nodes in the network. In modern mobile networks, selfish nodes exist in almost every network because every mobile node is interested in conserving its battery and computational, and try not to consume it to the benefit of others. This selfish behavior of nodes results in degradation of the overall performance of the network and network itself can become a non-cooperative network. Therefore, some sort of reputation mechanism needs be devised that not only identify these selfish nodes but also enforce these nodes to cooperate with other nodes in the network. Identification of selfish nodes, and enforcing cooperation among the nodes, is achieved in this paper by using the reputation index value and the Neighbor Monitor agent.

LITRATURE REVIEW

A lot of research for the detection of misbehavior of a selfish node has been done. Different strategies were introduced to prevent such behavior.

One approach is to punish the selfish nodes. Systems under this category are based on the assumption that every node in the network must transmit packets that they have received from their neighbor (Yoo and Agrawal, 2006). Misbehaving in the network can only be reduced by monitoring the neighbours continuously (Marti *et al*., 2000). Watchdog is used to monitor the neighbours and another tool pathrater is used to select reliable routes.

Corresponding Author: Muhammad Arsalan Paracha, Department of Computer Engineering, University of Engineering and Technology, Taxila 47080, Pakistan

Buchegger and Boudec (2002) designed a system called CONFIDANT. This system was based on the idea to make the misbehaving unattractive. It consists of four parts namely Monitor, Trust Manager, Reputation and Path Manager. (Lei *et al.*, 2006) came up with the idea of direct and indirect trust. Their study was based on the assumption that the reputation information about any node can be made available through two sources. One is through the monitoring node itself which is going to evaluate reputation of the neighbour, called direct trust and other is the information available from nodes which have reputation information about monitored node, called the indirect trust. Djenouri and Badache (2005) designed a system based on the mechanism of two-hop ACK P Michiardi and Molva (2002) proposed that reputation information can be made more real if we combine it from three different sources, Subjective, Indirect and Functional.

However, such reputation systems that are mentioned above may have certain issues. For example, in most cases it is assumed that the nodes sharing information are themselves trustworthy. Furthermore, with such reputation systems the composite decision making might not always result in unique decision because of extreme opinions.

Another approach is to prevent a node to become a selfish node. These systems are more focused towards cooperation than punishment. Selfish nodes can be turned into cooperative nodes if we pay them for their packet forwarding services. This payment is normally in the form of *virtual currency* called nuggets (Levente and Jean-Pierre, 2000). In such systems one unit of credit is received by a node for forwarding a message to another node. Two payment models have been proposed in the literature. One is *packet purse model* and other is *packet trade model*. In addition to the nugget approach, a credit counter based (Buttyan and Hubaux, 2002) scheme has also been proposed in the literature. Remaining battery and remaining credit of a node was tracked. For both the solutions tamper-proof hardware is required at every node for the addition and deduction of credit. Selfish Avoidance Routing Protocol ensures a node is not selected for routing having its residual energy low and traffic density high (Sundararajan and Shanmugam, 2010). This approach prevents a node become selfish in near future and enhances cooperation among the nodes of a MANET. The effect of power consumption and current traffic density at a node is captured with the help of drain rate but a temper proof hardware is required for the estimation of node's power.

REPUTATION MODEL

This section describes the proposed reputation model for the detection of the selfish nodes. This includes the description of reputation strategy and discussion about different parameters of the reputation system of our system.

Assumptions: The presented mechanism is based on few assumptions. One assumption is that each link between the nodes must be bidirectional. This is a valid assumption because bidirectional communication is required in many wireless protocols, including 802.11. Another assumption is of the support of promiscuous mode for the wireless interfaces. It is needed for a node to listen the transmission of its neighbor. Initially all the nodes of network are considered as cooperative having their Reputation Index values above the Reputation Threshold value. However, this will not remain true for a selfish node because its RI would drop according to its misbehavior.

Overview: In the presented scheme we have proposed an agent called "Neighbor Monitor". This agent runs on every node and is used to monitor the traffic of its neighbors. Furthermore, a variable called Reputation Index (RI), associated with each participating node in the network, is introduced. The value of the Reputation Index is dynamically assigned to the corresponding node by the agent running on its neighbors. The value of the RI is calculated when the node acts as a broker. The cooperation of the node depends upon the value of the reputation index. Nodes cooperate with each other if the value of the RI is equal or above the certain predefined value known as Reputation Threshold (RT). The value of the reputation index is increased or decreased by its neighbor using neighbor monitor agent. When a node act as a cooperative node its value is incremented by its neighbors and when a node acts as a selfish node its RI value is decremented by its neighbors. The proposed scheme has been designed in such a way that if a node falls into the type of selfish nodes then the other nodes are unable to forward the frames of such nodes. So if a node wants that other nodes must route its packets than it should forward other's traffic. This is the prevention part because this mechanism encourages the nodes to forward the traffic from the other nodes.

System architecture: In order to explain the proposed scheme we create a network scenario having N nodes where N = {1, 2, 3…n}. Any of the node S can send packet to some node D in the network through some intermediate node A also known as broker. In answer to this request node A can behave in two ways. One is the possibility of forwarding packet as it has been received from the node S, and the other option is to behave as a selfish node by dropping the packet. Figure 1 presents the basic flow diagram of the proposed reputation model.

First of all, the node A checks the address of the receiver of the frame. If the node itself is a receiver, it simply receives the frame. If A itself is not a receiver than the value of the Reputation Index (RI), present in frame header, is checked. If the value of RI is less than a

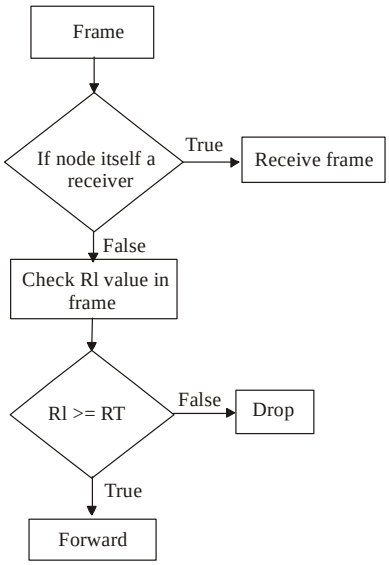

Fig. 1: Basic flow diagram of the reputation algorithm

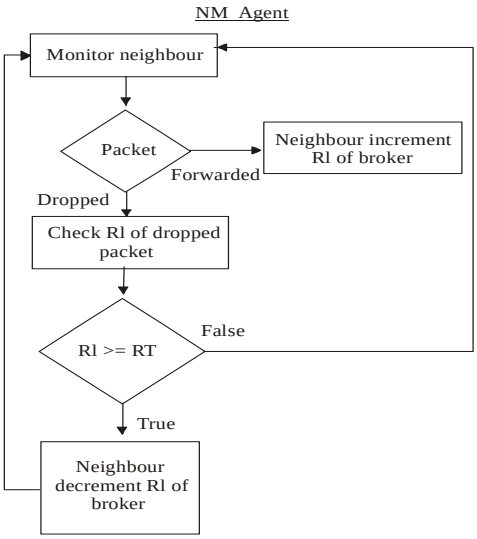

Fig. 2: Flow diagram of Neighbor Monitoring agent

predefined Reputation Threshold RT than the frame is dropped. And if the reputation index is greater than or equal to RT then node A (broker) forwards the frame to its intended recipient. As it forwards the frame, the Neighbor Monitor agent NM detects and increment the value of RI of node A. The function of NM agent is explained with the help of flow diagram presented in Fig. 2.

For the situation when broker behaves as a selfish node and does not forward the frame even besides having the value of RI greater than or equal to RT, then NM agent detect this misbehavior and decrements the value of RI of broker.

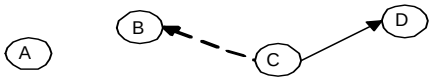

Fig. 3: Working of NM agent

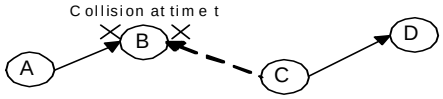

Fig. 4: Packet collision scenario

Components: This section defines the basic components of the proposed model.

Broker: The intermediate nodes receiving the packets and forwarding them to the other or intended recipient nodes are known as Broker.

Neighbor Monitor (NM): Neighbor monitor is an agent that runs on every node and is used to monitor the traffic of its neighbors.

Suppose that a sender node A wants to transmit a packet to a destination node D. A is connected to D via broker nodes B and C. When C forwards packet from A towards D, B can listen the transmission of C and confirm that node C tries to transmit the traffic towards node D. The solid line from C to D as shown in Fig. 3 represents the intended direction of the packet, while the dashed line from C to B points that B is in range of C and can listen the transmission.

To implement the mechanism of Neighbor Monitor a buffer is maintained that consists of newly sent packets and compare these packets with overheard transmission. If match is detected than packet is removed from the buffer and Reputation Index (RI) value of the corresponding neighbor is incremented. If the packet stays in the buffer for a specified time, the NM agent can conclude that the node is misbehaving and hence decrements the RI value of that node.

This Neighbor Monitor agent mechanism works well in normal behavior but in case of collision it might not detect misbehaving nodes. So in order to handle such problem we explain this phenomenon with the help of Fig. 4.

Figure 4 demonstrates, a packet collision situation that might occur at B. Suppose node A sends a packet to

B at time t and at the same time B is trying to overhear the transmission from C. The collision occurs and prevents B from overhearing transmissions from C. Due to this scenario the value of RI should not be decremented immediately but it should wait certain amount of specified

time. If node B repeatedly fails to listen from node C then it may be assumed that C is behaving as Selfish node and hence its RI value should be decremented.

Reputation Index (RI): This variable is associated with each participating node in the network. The value of the Reputation Index is dynamically assigned to the corresponding node by the agent running on its neighbors. It is an 8-bit variable which is saved in the MAC Header of a frame. The value of this variable is calculated using the function f(x).

To increment the value of RI:

$$f(x) = f(x-1) + i \quad (1)$$

To decrement the value of RI:

$$f(x) = f(x-1) - d \quad (2)$$

where, *i* and *d* are positive real valued constants. The decision about the nodes depends on these values. The greater the values are the faster you decide about the future of a node. We select the value of d slightly greater than i, just to timely detect the misbehavior of a node.

When the frame leaves the sender node this variable is attached with the frame. The value of the RI is calculated when the node acts as a broker. This value is incremented, using f (x), when the node behaves as a cooperative node and decremented, using f (x), when the node behaves as a selfish node. The cooperation of the node depends upon the value of the reputation index.

Reputation Threshold (RT): It's a predetermined value which is used to detect selfishness of a node. Nodes cooperate with each other if value of RI is equal or greater than certain predefined value known as the Reputation Threshold (RT). If the value of RI of a node is less than reputation threshold, the node is marked as selfish node.

This value plays an important role when the node serves as a broker or receiver. These broker or receiver nodes only accept the packet if value of RI is greater than or equal to RT, and drops the packet if the value of RI is less than RT.

SIMULATION RESULTS

Network simulator 2 NS-2 is used to simulate the complete scenario. A scenario consisting 15 mobile nodes, exchanging TCP traffic, has been created. The topology is a rectangular area with 1000 m length and 1000 m width. All the simulations were simulated for 100 seconds with AODV as a routing protocol. The values of i and d are set to 0.1 and 0.2, respectively. The parameters common for all simulations are given in Table 1.

Table I: Parameters used in simulation

Parameters	Value
Transmission range	250
Simulation time	100 sec
Topology size	1000 m × 1000 m
No of nodes	15
Traffic type	TCP
Number of sources and dest	2

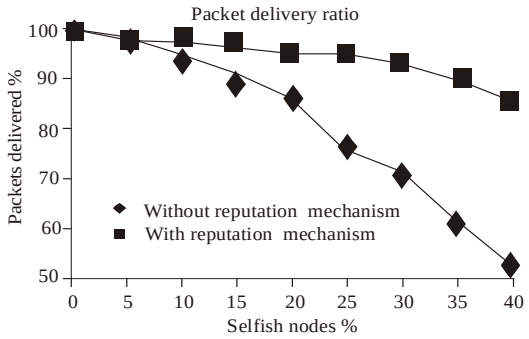

Fig. 5: Graph of packet delivery ratio

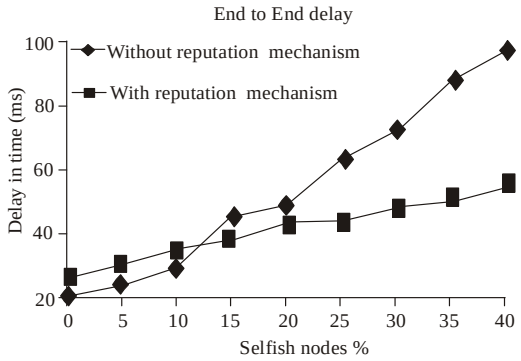

Fig. 6: Graph of end to end delay

All results are calculated with 30 different simulations. Performance of the system was analyzed by varying the number of selfish nodes. To obtain realistic results, maximum 40% of total nodes act as a selfish node at same time.

We have calculated average number of packets delivered (with reputation system) and compares it with average number of packets delivered when there is no reputation system installed in the network. From this result it is clear that performance of the network improves when we have a reputation system for the punishment of nodes as shown in Fig. 5.

Without reputation system, with an increase in percentage of selfish nodes, packet delivery decreases. And when 40% of the nodes are selfish then only 53% of the packets transmitted by the different sources reaches at the destination. But when the reputation system installed, it is observed that with increase in selfish nodes, packet delivery is not decreasing so sharply. Rather approximately 85% of the packets reached their destinations with 40% selfish nodes in a network. This is

only because we have a punishment and recovery phases in reputation system which helps in penalizing misbehaving nodes and then these nodes improve their behavior during recovery phase.

We also calculated end to end delay with and without reputation system as shown in Fig. 6.

Above result depicts that initially the delay is slightly greater with reputation system installed in the network but with the increase in number of selfish nodes the overall end to end delay is less than the delay without reputation system in the network. End to end delay increases with an increase in percentage of selfish nodes and this increase is sharp when we don't have any reputation system installed in the network.

CONCLUSION AND FUTURE WORK

Selfishness of the node creates a lot of problems in mobile ad-hoc networks including decrease in throughput. In this dissertation we have proposed a reputation system that can cope with this selfishness and can help in increasing overall performance of the network. Our scheme produces satisfactory results with AODV protocol. It should be tested for other protocols.

ACKNOWLEDGMENT

The valuable input from anonymous reviewers is greatly acknowledged to improve the quality of the manuscript.

REFERENCES

Buchegger, S. and J.L. Boudec, 2002. Performance Analysis of the CONFIDANT Protocol. In Proceedings of the 3rd ACM international symposium on Mobile ad hoc networking and computing, Lausanne Switzerland, pp: 226-236.

Buttyan, L. and J.P. Hubaux, 2002. Stimulating cooperation in self-organizing mobile ad hoc networks," ACM Journal for Mobile Networks (MONET), special issue on Mobile Ad Hoc Networks.

Djenouri, D. and N. Badache, 2005. New approach for selfish nodes detection in mobile ad-hoc networks", In 1st IEEE workshop on Security and Privacy for Emerging Areas in Communication Networks, pp: 288-294.

Lei, Z., D. Nyang, K. Lee and H. Lim, 2006. Fair reputation evaluating protocol for mobile ad hoc Network," In Proceedings of the International Conference on Computational Intelligence and Security, pp: 613-616.

Levente, B. and H.J. Pierre, 2000. Enforcing service availability in mobile ad-hoc WANS. In Proceedings of 1st IEEE/ACM Workshop on Mobile Ad Hoc Networking and Computing (Mobi HOC), Boston, MA, USA, pp: 87-96.

Marti, S., T.J. Giuli, K. Lai and M. Baker, 2000. Mitigating routing misbehaviour in mobile ad hoc networks. In Proceedings of the 6th annual international conference on Mobile computing and networking, pp: 255-265.

Michiardi, P. and R. Molva, 2002. CORE: A Collaborative Reputation Mechanism to enforce node cooperation in Mobile Ad hoc Networks. In Sixth International Federation for Image Processing (IFIP) conference on security communications and multimedia, Portoroz, Slovenia.

Sundararajan, T.V.P. and D.A. Shanmugam, 2010. Selfish avoidance routing protocol for mobile ad-hoc networks. Inter. J. Wireless Mobile Network, pp: 2

Yoo, Y. and D.P. Agrawal, 2006. Why does it pay to be selfish in a MANET. IEEE Wireless Communo, 13(6): 87-97.