A Probabilistic Approach to Detect Selfish Node in MANET

Suman Goswami
Department of CSE & IT,
University Institute of Technology,
The University of Burdwan,
Burdwan,WB,INDIA.

Saptarshi Das
Department of CSE&IT,
University Institute of Technology,
The University of Burdwan,
Burdwan, WB, INDIA.

ABSTRACT
A mobile ad hoc network, literally means a wireless link, which is ad-hoc by nature between several mobile nodes or devices. Each device in a MANET can move freely in any direction, and will therefore change its links to other devices easily. The main challenge in building a MANET is in terms of security. In this paper we are presenting a probabilistic approach to detect selfish nodes using the probability density function. The proposed model works with existing routing protocol and the nodes that are suspected of having the selfishness are given a Selfishness test. This model formulates this problem with the help of prior probability and continuous Bayes' theorem.

Keywords
Keywords are your own designated keywords which can be used for easy location of the manuscript using any search engines.

1. INTRODUCTION
Mobile Ad hoc network (MANET) is a self-configuring infrastructure less network of mobile devices connected by Wireless links and forms an arbitrary topology. Each device (node) in a MANET is free to move independently in any direction, and will therefore change its links to other devices frequently; thus, the network topology may change unpredictably. Each must forward traffic unrelated to its own use, and therefore be a router. The primary challenge in building a MANET is equipping each device to continuously maintain the information required to properly route traffic. Such networks may operate by themselves or may be connected to the larger Internet. Therefore, each node must act as both a host and a router at the same time. The network topology normally changes due to the mobility of mobile nodes in the network. In MANET each node can communicate with the help of its neighbor node that's comes in its radio range each node forward their packet to their neighbor node toward destination where path for transmitting massage packet is suggested by routing protocol as shortest path.MANETs are a kind of Wireless ad hoc network that usually has a routable networking environment on top of a Link Layer ad hoc network.Wormhole attack attract massage packet and play number of misbehave with that routing packet like scanning of confidential message, drop, corrupt and change transmitted massage over network. Some popular secure routing algorithms are SRP (Secure Routing Protocol)[5], ARAN (Authenticated Routing for Ad hoc Networks) [2, 3], Ariadne [1], SEAD (Secure Efficient Ad hoc Distance vector routing) [4] etc. Where as most of the attacks based on manipulations of routing data can be detected by the use of a secure routing protocol like ARAN [2, 3], Ariadne [1] and others [3-6].
In this paper we proposed a mathematical model for the detection of selfish node. This paper is organized as follows. Section II describers the background and related work. Section III. presents the mathematical model and Section IV. presents simulation. We used OPNET to find this mathematical expression, and we verified the result with different experimentations in Section V. Section VI concludes the paper.

2. BACKGROUND AND RELATED WORK
A lot of research has been done in the past but the most significant contributions have been the PGP (Pretty Good Privacy) and trust based security. None of the protocols have made a decent tradeoff between security and performance. In an attempt to enhance security in MANETs many researchers have suggested and implemented new improvements to the protocols and some of them have suggested new protocols. There are many attacks in MANET that target the particular routing protocols. This is due to developing routing services without considering security issues. In this section, we describe some common attacks, advantage and disadvantage of some common routing protocols.

Passive attack happened without the interrupting in the communication operations. For the Active attack node works as active node. It can perform the operations like interruption, modification, or fabrication, at the time of attack directly. In the Internal Attack nodes are the part of network in order to perform attack. Whereas External Attack nodes does not belong the network in order to perform attack. In the purpose of Black hole Attack , malicious user broadcast the message having the false information of shortest path. This shortest path is work for the attack. In Byzantine attack node participates alone in the network. Some time it also makes the set of intermediate nodes and works as an attacker. The operation can perform like routing loops and forwarding packets dropping packets. It will degrade the quality of services. The Routing protocols are responsible to perform dynamic routing and information sharing as well. Table Driven Protocol is the type approach the protocol will store the table in order to get the route of destination. With the help of that table the route will decides and forward the packet to the destination node. There are many table driven protocol has developed like DSDV, WRP etc. this approach is also known

as the proactive protocols. On Demand Protocol isthe another approach to route the packet in the wireless network. This approach does not have any pre decided route. This approach works on the basis of current status of request. TheHybrid Protocol is used the combination of both protocols. ARIADNE [1] is an on-demand secure ad-hoc routing protocol based on DSR that implements highly efficient symmetric cryptography. It provides point-to-point authentication of a routing message using a message authentication code (MAC) and a shared key between the two communicating parties. Although ARIADNE is free from a flood of RREQ packets and cache poisoning attack, but it is immune to the wormhole attack and rushing attack.

Specifically, SEAD[4] builds on the DSDV-SQ version of the DSDV (Destination Sequenced Distance Vector) protocol. It deals with attackers that modify routing information and also with replay attacks and makes use of one-way hash chains rather than implementing expensive asymmetric cryptography operations. Two different approaches are used for message authentication to prevent the attackers. SEAD does not cope with wormhole attacks. The ARAN protocol was observed to defend almost against all security attacks in MANETs.

In ad hoc networks, a node performs terminal and routing functions. Therefore, it is necessary for the ad-hoc network to forward packets of others but when a node drops packets of others due to honest or malicious cause these nodes are called selfish [7]. A node becomes selfish due to these causes either honest causes such as collisions, channel errors, or buffer overflows or malicious causes such as to save its energy or bandwidth, black hole or wormhole attack, network congestion. There are various methods to detect selfish nodes.

3. Our Proposed model

In our work, we elaborated a simple and efficient probabilistic model, which will be implemented with existing routing protocol in MANET, to detect a selfish node. In the work of [9] Md. Akhturet. al , we had seen their model using the normal probability density function [10]. Our proposed model is a improvement over this, we have used t-distribution function[11]. And the simulation result is shown in the section IV of this paper. In this section we have discussed in brief the mathematical model used in this concern.

In an adhoc Network, nodes who are suspected of having the selfishness are given a test, called the Nodes' Selfishness Test (NST), to detect selfishness of a node in a network.

The incidence of NST is defined as follows: Let S be the event that a node has selfishness, *S* be the event that the node does not have selfishness, Pos be the event that the node test is positive for the selfishness, and Neg be the event that the node test is negative for the selfishness; that is what will be the value of $P(S \mid Pos)$ =?

Using very basic concept of probability, we found Bayes theorem which states

$$P(S \mid Pos) = \frac{P(S)P(Pos|S)}{P(S)P(Pos|S)+P(S^{-})P(Pos|S^{-})} \quad \text{------(1)}$$

If the result is greater than 0.5, we conclude that the node is more likely than not to have selfishness. We can reach the same conclusion using the ratio

$$S = \frac{P(S)P(Pos|S)}{P(S)P(Pos|S^{-})} \quad \text{---------- (2)}$$

If the ratio is greater than 1, we again conclude that the node is more likely than not to have selfishness. After computing the ratio R, we can derive the probability that a node has the selfishness given a positive result:

$$P(S|Pos) = \frac{S}{1+S} \quad \text{---------- (3)}$$

This induces with (1). If $P(R \mid Pos)$ or $P(S)$ had been so small that $P(S \mid Pos) < P(S \mid Pos)$, a possible conclusion would be that the node did not have the selfishness even if the test were positive. Another interpretation would be that an error in the test is more likely possibility than the selfishness itself. Because $P(S)$ is very low for many test, giving a second test is standard procedure whenever a positive result occurs on the first test. We can formulate this problem with the help of prior probability and continuous Bayes' theorem as,

Let R be the event that a node is regular, *R* be the event that the node is not regular means selfish, and then $P(x \mid R)$ defines the normal density. The prior probabilities are P(R) and $P(R^{-})$

Again as per t-distribution function, the probability density function

$$P(x) = \frac{1}{\sqrt{n}\,B(\frac{1}{2},\frac{n}{2})}(1 + t^2/n)^{-(n+1)/2} \text{----------(4)}$$

By continuous version of Bayes' Theorem, then we need to evaluate $P(R|x) = \frac{P(R)P(X|R)}{P(R)P(X|R)+P(R^{-})P(X|R^{-})}$-------(5)

So the node is slightly less likely to regular than not to regular. We can also use the ratio $R=\frac{P(R|x)}{P(R^{-}|x)}$-------- (6)

regular. Using R/(1+R), this agrees with (5).

4. Simulation

To study the performance of our proposed algorithm simulation was conducted using OMNeT++ [15] which supports complete physical, data link and MAC layer models for simulating wireless ad hoc networks. OMNeT++ is a freely distributed, object-oriented, modular, discrete-event simulator written in C++. It is designed for general-purpose discrete-event simulation, and provides model libraries for communication protocols and network systems. We simulated network of mobile nodes placed randomly in an area of 450x450 square meters, which is divided into 3x3 cells, each cell having a virtual leader, with mobile nodes ranging from 10 to 65. A source and a destination is selected randomly. Free space propagation model is assumed as the channel model. Each node is assumed to have a constant transmission range of 100meters. Mobility pattern of the mobile nodes is generated using Random waypoint model [16]. A mobile selects another node in the network and constantly moves towards it at a given velocity. Once it reaches there, it waits for some pause time and selects another node and again starts moving. By observing the performance of the network under mobility we can test the stability of the design in real time

scenario. Speed of a mobile node is assigned a value between 0 to 5 meters/sec. Initially all the mobiles would be given some initial energy (10000). As the packets re to be transmitted through the nodes, they would loose some energy. A threshold (7000) would be selected. It is assumed from previous research [15] (as the size of each packet is constant), that the radio interference, when powered on, consumes 1.2W while actually receiving a packet and 1.6W while transmitting a packet.

5. Results

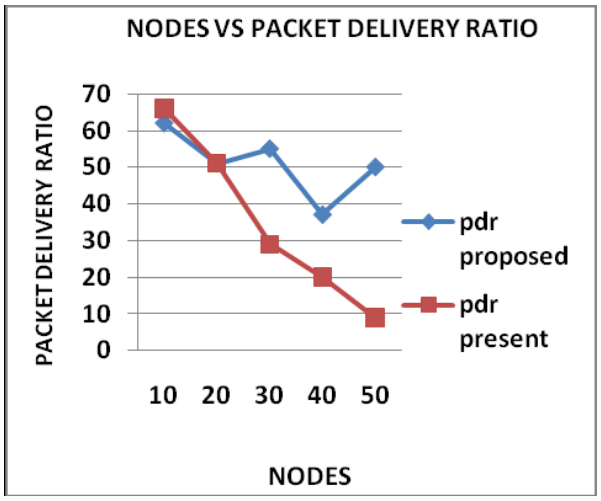

Fig 1: Achieved Packet Delivery Ratio by Varying Number of Nodes

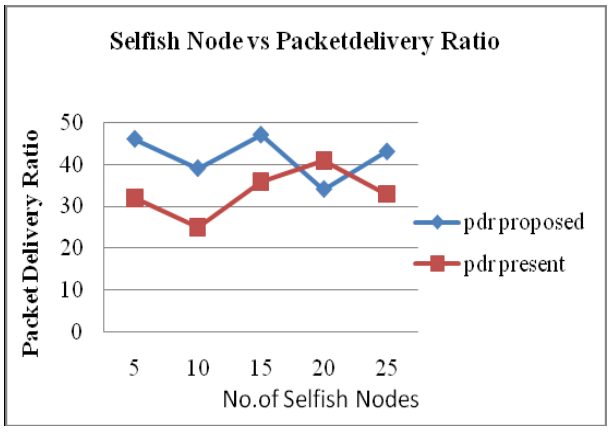

Fig 2: Number of Selfish Nodes vs. Packet Delivery Ratio

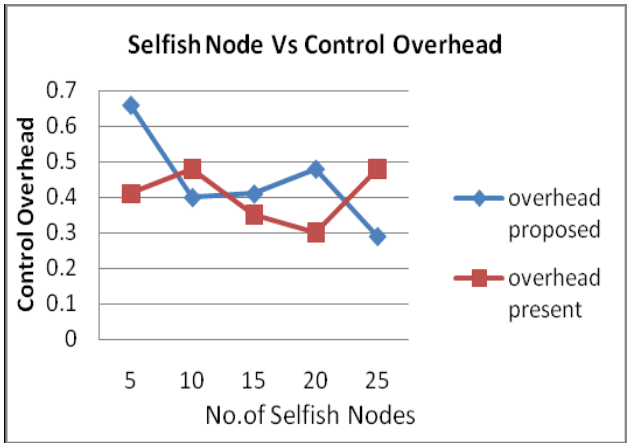

Fig 3: Number of Selfish Nodes vs. Control Overhead

Above Fig 1 shows packet delivery ratio achieved by proposed protocol. Improved packet delivery ratio is achieved due to the fact that proposed protocol is to choose stable paths. Increasing number of nodes does not affect the packet delivery ratio as is normally the case with other routing protocols**.**

In fig 2, The graph shows the packet delivery ratio (PDR) of the two different modules such as present and proposed system. We can observe that PDR of proposed system is better than present system.

From fig 3, we can say that the control overhead of the proposed technique is much lesser than the present technique.

6. Conclusion

The whole study and simulation have shown a better result over pre existing model of Akhtaret. Al. Although MANET cant' be free of challenges, thereby security in MANET is the cry of the day. And our proposed scheme implemented with existing routing algorithm optimizes the detection of selfish node in a MANET.

7. References

[1] Y. Hu, A. Perrig, and D. Johnson, Ariadne "A Secure On Demand Routing Protocol for Ad Hoc Networks", In Proceedings of the Eighth Annual International Conference on Mobile Computing and Networking, September 2002, 12-23.

[2] K. Sanzgiri, B. Dahill, B. Levine, C. Shields, and E. Belding-Royer, "A secure routing protocol for ad hoc networks", in the 10th IEEE International Conference on Network Protocols (ICNP), November 2002.

[3] K. Sanzgiri, D. LaFlamme, , B. Dahill, B. N. Levine, C. Shields, and E. M. Belding- Royer, "Authenticate routing for ad hoc networks", in IEEE Journal on Selected Area in Communications, ser. 3, vol. 23, March 2005.

[4] Y. Hu, D. Johnson, and A. Perrig. "SEAD Secure Efficient Distance Vector Routing in Mobile Wireless Ad Hoc Networks", In Fourth IEEE Workshop on Mobile Computing Systems and Applications, June 2002, 3-13.

[5] P. Papadimitratos, Z. Haas and P. Samar, "The Secure Routing Protocol (SRP) for Ad Hoc Networks", Internet-Draft, draft-papadimitratossecurerouting-protocol-00.txt, December 2002.

[6] D.Johnson, D. Maltz, and Y.-C. Hu, "The Dynamic Source Routing Protocol for Mobile Ad Hoc Networks (DSR)", IEEE Internet Draft, Apr. 2003.

[7] Yih-Chun Hu, Adrian Perrig, and David B. Johnson, "Wormhole Attacks in Wireless Networks" University of Illinois, Carnegie Mellon University, Rice University

[8] He Ronghui, Ma Guoqing, Wang Chunlei, and Fang Lan" Detecting and Locating Wormhole Attacks in Wireless Sensor Networks Using Beacon Nodes", World Academy of Science, Engineering and Technology, 55,2009

[9]Mathematical model for the detection of selfish node in MANET, Akhtar et al. IJCSI Vol-1 Issue-3..

[12] ZhiRen and Jing Su Wei Guo,"A Cross-Layer AODV Routing Protocol," Proceedings of the IEEE International Conference on Mechatronics & Automation Niagara Falls, Canada. July 2005.

[13] FanBai, Ahmed Helmy,"A survey of mobility models in wireless Ad Hoc Networks," University of Southern California, U. S. A.

[14] AndrasVarga, OMNeT++, www.omnetpp.org