International Journal of Computer Science and Informatics

Volume 1 | Issue 4 Article 2

April 2012

Mathematical Model for the Detection of Selfish Nodes in MANETs

Md. Amir Khusru Akhtar
Department of Computer Science & Engineering, ICFAI University, Ranchi, Jharkhand, India, akru2008@gmail.com

G. Sahoo
Department of Information Technology, BIT Mesra, Ranchi, Jharkhand, India, gsahoo@bitmesra.ac.in

Mathematical Model for the Detection of Selfish Nodes in MANETs

Md. Amir Khusru Akhtar[1] & G. Sahoo[2]

[1]Department of Computer Science & Engineering, ICFAI University, Ranchi, Jharkhand, India
[2]Department of Information Technology, BIT Mesra, Ranchi, Jharkhand, India
E-mail : akru2008@gmail.com[1], gsahoo@bitmesra.ac.in[2]

Abstract **-** A mobile ad hoc network, is an independent network of mobile devices connected by wireless links. Each device in a MANET can move freely in any direction, and will therefore change its links to other devices easily. Each must forward traffic of others, and therefore be called a router. The main challenge in building a MANET is in terms of security. In this paper we are presenting the mathematical model 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 **-** *MANETs, Regular node, Selfish node, Prior Probability, Density function.*

I. INTRODUCTION

A mobile Ad hoc network (MANET) is a type of wireless network that is self configuring network of mobile nodes connected by wireless links and forms an arbitrary topology. Nodes are free to move randomly and organize themselves arbitrarily; thus, the network topology may change unpredictably. Such a network may operate in a standalone fashion, or may be connected to the Internet. These networks can be quickly deployment and these networks use multi-hop topologies. It is short lived networks. Nodes uses any of the routing algorithms presented in [1, 2, 3, 4, 5, 6, and 10] to forward packets in an ad hoc network. Applications such as military exercises, disaster relief, and mine site operation, for example, may benefit from ad hoc networking, but secure and reliable communication is a necessary prerequisite for such applications. Every node in an ad hoc network participates in the routing process of the packets which use any of the routing algorithms present [1-6, 10]. Attacks in ad hoc routing protocols are a major factor of concern. A variety of attacks like modification, fabrication, wormhole attack (tunneling), blackhole attack, denial of service attack, invisible node attack, sybil attack, rushing attack and non-cooperation reduce the reliability of these routing protocols. To overcome these security threats the concept of secured routing protocols came into existence. Some popular secured 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]. But when nodes simply drop packets, or show its selfishness all of the secure routing protocols fail, as they focus only on the detection of modifications to routing data but not on the concealment of existing links. 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 the simulation. We used OPNET to find this mathematical expression, and we verified the result with different experimentations. Section IV concludes the paper.

II. BACKGROUND AND RELATED WORK

A. Background

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 the security threats, advantage and disadvantage of some common routing protocols.

AODV [10] is also on-demand routing protocol, hence the route is established only when it is required by the source for transmission of data packets. AODV uses destination sequence number (DestSeqNum) to identify the most recent path to the destination. A node updates its path information only if the DestSeqNum of the

current packet received is greater than the last DestSeqNum stored at the node.

DSR [6] uses source routing in which a data packet carries the complete path to be traversed, whereas in AODV the source node and intermediate nodes store the next-hop information.

Authenticated Routing for Ad-hoc Networks (ARAN)[2,3] is an on-demand routing protocol that detects and protects against malicious actions carried out by third parties and peers in particular ad-hoc environment. This protocol introduces authentication, message integrity and non-repudiation as a part of a minimal security policy. Though ARAN is designed to enhance ad-hoc security, still it is immune to rushing attack and cannot identify selfish nodes.

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.

However, by doing more research in the field of MANETs, one major flaw in any of the existing secure routing protocols was discovered. This is that all of these secure routing protocols do not account for selfish nodes whether by detecting or isolating them from the network.

B. Related Work

In ad hoc networks, a node performs terminal and routing functions. Therefore, it is necessary for adho c 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, blackhole or wormhole attack, network congestion. A selfish Node minimise efficiency of packet transfer and maximises the packet delivery time and packet loss rate that divides a network into smaller network.

There are various methods to detect selfish nodes. These methods are categorized in incentive-based methods or reputation-based methods. In the first method it discourages a node to become selfish by giving virtual money or credits when a node forward packets of others because to send or receive its own packets the node requires enough credit. Buttayan and Hubaux [16] method uses virtual currency, called nuglets to detect selfish node. In this method a nuglet counter is incremented monotonically when it forwards a packet for others. When a node wants to send its own packet, it requires enough credit because if it is less than certain threshold it is not allowed to send packets. But this method requires tamper proof hardware to maintain the nuglet.

In reputation-based method it detects a selfish node and performs proper action by using a reputation system that detect and rate a selfish node. The reputation is defined by the participation seen by others [17]. When node's reputation is good it participate in network activity otherwise it is marked as selfish.

III. PROPOSED WORK

In this paper, we will show via a simple model and with existing routing protocols that in an Adhoc network we can detect selfish nodes using the probability density function [15].

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

The incidence of S_TEST is defined as follows:

Let S be the event that a node has selfishness, $\bar{S}$ 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 is $P(S \mid Pos)$?

Using Bayes' theorem, we find that

$$P(S \mid Pos) = \frac{P(S)P(Pos \mid S)}{P(S)P(Pos \mid S) + P(\bar{S})P(Pos \mid \bar{S})} \qquad (1)$$

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

$$S = \frac{P(S)P(Pos \mid S)}{P(S)P(Pos \mid \overline{S})} \quad (2)$$

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:

$$P(S \mid Pos) = \frac{S}{1+S} \quad (3)$$

This agrees with (1).

If $P(R \mid Pos)$ or $P(S)$ had been so small that $P(S \mid Pos) < P(\overline{S} \mid Pos)$, 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, $\overline{R}$ 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($\overline{R}$)

$$P(x \mid R) = \frac{1}{\sigma_R \sqrt{2\prod}} e^{-1/2\left(\frac{x-\mu R}{\sigma_R}\right)^2} \quad (4)$$

and

$$P(x \mid \overline{R}) = \frac{1}{\sigma_{\overline{R}} \sqrt{2\prod}} e^{-1/2\left(\frac{x-\mu \overline{R}}{\sigma_{\overline{R}}}\right)^2} \quad (5)$$

By continuous version of Bayes' Theorem

$$P(R \mid x) = \frac{P(R)P(x \mid R)}{P(R)P(x \mid R) + P(\overline{R})P(x \mid \overline{R})} \quad (6)$$

So the node is slightly less likely to regular than not to regular.

We can also use the ratio

$$R = \frac{P(R \mid x)}{P(\overline{R} \mid x)}$$

If R<1, the node is more likely not to be regular than to regular. Using $\frac{R}{1+R}$, this agrees with (6).

This model classified the regular and the selfish nodes.

The densities are shown in figure 1.

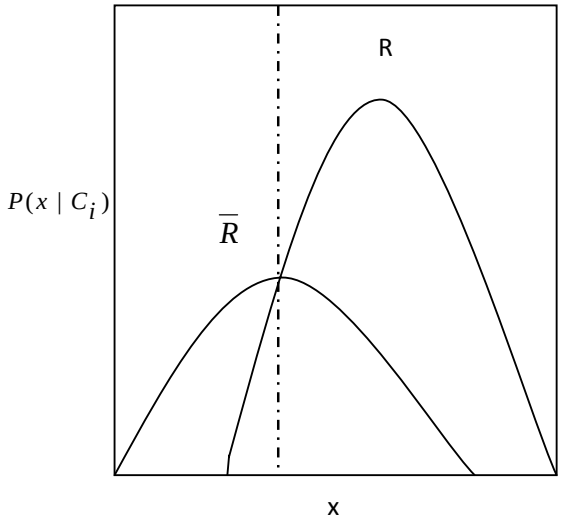

Fig. 1 : The conditional density function of network

IV. CONCLUSION

MANETs are not perfect. The challenges of security, scalability, mobility, bandwidth limitations, and power constraints of these networks have not been completely alleviated to date. But the security problem can be minimized by using the proposed mathematical model that expresses the detection of selfish node in MANETs to secure the network. This mathematical model is verified by experimentation and gives acceptable accuracy and provides a solution for secured routing in independent environment, because it uses heuristic model rather than deterministic. So, this model gives more accurate information using the defined probabilistic mathematical model.

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-papadimitratos-securerouting- 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] Tanapat Anusas-Amornkul, "On detection mechanisms and their Performance for packet dropping Attack in ad hoc networks", University of Pittsburgh, 2008, www.google.com, Date of Access 09/09/09.

[8] F. Kargl, A. Klenk, S. Schlott, and M.Weber, "Advanced detection of selfish or malicious nodes in ad hoc networks", University of Ulm, Dep. of Multimedia Computing, Ulm, Germany August 2004, www.google.com, Date of Access 09/02/09.

[9] Dharma, Agrawal, "Selfishness in Mobile Adhoc Networks", Department of Computer Science, University of Cincinnati, Cincinnat, www.google.com, Date of Access 09/03/09.

[10] C.E. Perkins, and E. Royer, "Ad-hoc on-demand distance vector routing", Proceedings of Second IEEE Workshop on Mobile Computing Systems and Applications, 90-100, 1999

[11] Deshpande Vivek, "Security in Ad-Hoc Routing Protocols", Maharashtra, India, www.google.com, Date of Access 09/03/09.

[12] S. Yi, P. Naldurg, and R. Kravets, "Security-Aware Ad Hoc Routing for Wireless Networks", in Proc. MobiHoc, Oct. 2001, www.google.com, Date of Access 09/09/09.

[13] List of ad-hoc routing protocols, Wikipedia the free encyclopedia.htm, en.Wikipedia.org, Date of Access 20/02/2009.

[14] Md. Amir Khusru Akhtar, V. S. Shankar Sriram, G. Sahoo, "A Methodology to overcome Selfish Node Attack in MANETs", Knowledge Management and E-learning: An International Journal, Serial Publication-2009.

[15] Earl Gose, Richard Johnsonbaugh, Steve Jost, "Pattern Recognition and image Analysis", Prentice Hall of India Private Ltd., New Delhi 2006.

[16] L. Buttyan and J.-P. Hubaux, "Stimulating cooperation in self-organizing mobile ad hoc networks", in Mobile Networks and Applications, 2003, 579-592.

[17] S. Buchegger and J.-Y. L. Boudec, "Self-policing mobile ad hoc networks by reputation systems", in IEEE Communications Magazine, ser. 7, vol. 43, July 2005, 101-107.

◈◈◈