IJCSN International Journal of Computer Science and Network, Volume 3, Issue 5, October 2014
ISSN (Online) : 2277-5420 **www.IJCSN.org**
Impact Factor: 0.274

Detection of Malicious Nodes in Ad Hoc Network using Statistical Method

[1] Rajib Das, [2] Bipul Syam Purkayastha, [3] Sanjeev Kumar Singh

[1, 2] Department of Computer Science
Assam University, Silchar – 788011, Assam

[3] Department of Mathematics,
Union Christian College, Ri-Bhoi-793122, Meghalaya

Abstract - The nature of wireless ad hoc and sensor networks make them very attractive to attackers. One of the most popular and serious attacks in wireless ad hoc networks is malicious node attack and most proposed protocols to defend against this attack used positioning devices, synchronized clocks, or directional antennas. 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 the statistical approach is presented to detect malicious nodes using the probability density function (PDF). The proposed approach works with existing routing protocol and the nodes that are suspected of having the malicious behaviour are given a behavioral test. This approach formulates this problem with the help of probability and continuous Bayes' theorem.

Keywords - *MANET, malicious node, PDF, probability, Bayes' theorem.*

1. Introduction

Mobile Ad hoc Networks (MANETs) are open to a wide range of attacks due to their unique characteristics like dynamic topology, shared medium, absence of infrastructure, multi-hop scenario and resource constraints. In such a network, each mobile node operates not only as a host but also as a router, forwarding packets for other nodes that may not be within direct wireless transmission range of each other. Thus, nodes must discover and maintain routes to other nodes. Data packets sent by a source node may be reached to destination node via a number of intermediate nodes. In the absence of a security mechanism, it is easy for an intermediate node to insert, intercept or modify the messages thus attacking the normal operation of MANET routing. This network is usually characterized by a dynamic topology, a limited bandwidth, energy constraints, the heterogeneity nodes, and a limited physical security. The applications having recourse to the ad hoc networks cover a very broad spectrum. For example in the tactical applications (fires, flood, etc.), in the soldier's field, in the monitoring systems, and the world of transport [1]. The working principle of ad hoc network is depicted in the fig 1.

The problem of the MANET is how to find the investment of lower costs in rated capacities and reserves which ensures the routing of the nominal traffic and guarantees its reliability in the event of any breakdown of arc or node. That's why several families routing protocols emerged. Each protocol can be classified as a reactive like AODV (Ad hoc One Demand Distance Vector) and DSR (Dynamic Source Routing), proactive like OLSR (Optimized Link State Protocol), or hybrid like ZRP (or Routing Protocol Zones) [1].

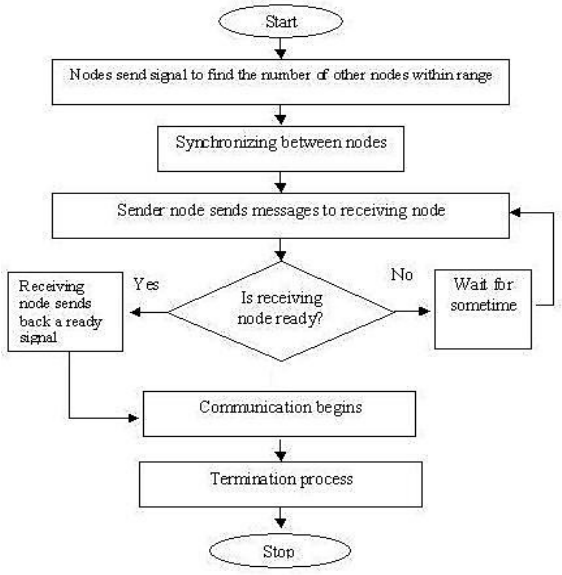

Fig 1: Working of Mobile Ad Hoc Network

In spite of the evolution of the ad hoc mobile networks during the last decade it still problems related security

which remain unsolved. Although some solutions were proposed but none of them satisfy all the constraints on the ad hoc networks.

In thispaperdifferent methods are being used to detect various security attacks in the MANET and propose a statistical approach for the detection of malicious node in NS-2[2][3]. The paper is organized as follows. Section 2 describers the background and related work. Section 3 presents the routing attack in ad hoc networks. In section 4, the proposed methodology using different mathematical expression have been discussed, and verified the result withdifferent experimentations. Section 5 concludes the paper.

2. Related Work

The primary goal of routing protocols in adhocnetwork is to establish optimal path or minhops between source and destination withminimum overhead and minimum bandwidthconsumption so that packets are delivered in atimely manner. A MANET protocol shouldfunction effectively over a wide range ofnetworking context from small ad-hoc group tolarger Mobile Multi-Hop networks [4].Routing protocols can be divided intoproactive, reactive and hybrid protocols,depending on the routing topology. Proactiveprotocols are typically table-driven e.g.Destination Sequenced Distance Vector(DSDV) protocol. Reactive or source-initiatedon-demand protocols, in contrary, do notperiodically update the routing information. Itis propagated to the nodes only whennecessary e.g. DSR and Ad-hoc On-DemandDistance Vector (AODV). Hybrid protocolsmake use of both reactive and proactiveapproaches e.g. Zone Routing Protocol (ZRP),Zone-Based Hierarchical Link State RoutingProtocol (ZHLS) etc. [5-7].The advantage of proactive routingprotocol is that node experiences minimaldelay when route is needed and unexpiredroute is available in the routing table but thedisadvantage of proactive routing is that theseare not scalable and maintenance of routingtable requires substantial network resources. Inthe case of reactive routing protocol, routebetween the nodes is searched only when nodewants to communicate with other node.

To discover the routes they use route discoveryprocedure which in turns uses the floodingmethod. In this, initiator forwards the RREQpacket to its entire neighbour's. If neighbour hasthe route for destination they reply otherwiseforward the RREQ to the next node. In thisway RREQ packet reaches to the destinationwhich sends the reply to RREQ. But themethod which is used to facilitate routediscovery are used by the Intruders or the malicious node to consume the networkresources which may lead to flooding attack.The DSR is a reactive unicast routingprotocol that utilizes source routing algorithm.In source routing algorithm, each data packetcontains complete routing information to reachits dissemination. Additionally, in DSR eachnode uses caching technology to maintainroute information that it has learnt [8].There are two major phases in DSR, theroute discovery phase and the routemaintenance phase. When a source node wantsto send a packet, it firstly consults its routecache. If the required route is available, thesource node includes the routing informationinside the data packet before sending it.Otherwise, the source node initiates a routediscovery operation by broadcasting routerequest packets. A route request packetcontains addresses of both the source and thedestination and a unique number to identify therequest.

Receiving a route request packet, anode checks its route cache. If the node doesn'thave routing information for the requesteddestination, it appends its own address to the route record field of the route request packet.Then, the request packet is forwarded to itsneighbours. To limit the communication

noverhead of route request packets, a nodeprocesses route request packets that both it hasnot seen before and its address is not presentedin the route record field. If the route requestpacket reaches the destination or anintermediate node has routing information tothe destination, a route reply packet isgenerated. When the route reply packet isgenerated by the destination, it comprisesaddresses of nodes that have been traversed bythe route request packet.

Otherwise, the routereply packet comprises the addresses of nodesthe route request packet has traversedconcatenated with the route in the intermediatenode's route cache. After being created, eitherby the destination or an intermediate node, aroute reply packet needs a route back to thesource. There are three possibilities to get abackward route. The first one is that the nodealready has a route to the source. The secondpossibility is that the network has symmetric(bi-directional) links. The route reply packet issent using the collected routing information inthe route record field, but in a reverse order. Inthe last case, there exists asymmetric (unidirectional)links and a new route discoveryprocedure is initiated to the source. Thediscovered route is piggybacked in the routerequest packet.

In DSR, when the data link layer detects a linkdisconnection, a ROUTE_ERROR packet issent backward to the source. After receivingthe ROUTE_ERROR packet, the source nodeinitiates another route discovery operation.Additionally, all routes containing the brokenlink should be removed from the route cachesof the immediate nodes when theROUTE_ERROR packet is transmitted to thesource. DSR has increased traffic overhead bycontaining complete routing information intoeach data packet, which degrades its routingperformance [9].

3. Routing Attacks

The malicious node(s) can attack MANETusing different ways, such as sending fakemessages several times, fake routinginformation, and advertising fake links todisrupt routing operations. In the followingsubsection, some of the current routing attacks inMANET protocols are discussed.

A. Flooding Attack: Flooding attack is a DoS type of attack inwhich the malicious node broadcast theexcessive false packet in the network toconsume the available resources so that validor legitimated user can not able to use thenetwork resources for valid communication.

Because of the limited resource constraints inthe MANET resource consumption due toflooding attack reduces the throughput of thenetwork. The flooding attack is possible in allmost all the on demand routing protocols.Depending upon the type of packet used toflood the network, flooding attack can becategorized in two categories.

a) RREQ Flooding: In the RREQ flooding attack, the attacker broadcast the many RREQ packets per timeinterval to the IP address which does not existin the network and disable the limited floodingfeature. On demand routing protocols uses theroute discovery process to obtain the routebetween the two nodes. In the route discoverythe source node broadcast the RREQ packetsin the network. Because the priority of theRREQ control packet is higher than datapacket then at the high load also RREQ packetare transmitted. A malicious node exploits thisfeature of on demand routing to launch theRREQ flooding attack.

b) Data Flooding: In the data flooding, malicious node flood thenetwork by sending useless data packets. Tolaunch the data flooding, first malicious nodebuilt a path to all the nodes then sends thelarge amount of bogus data packets. Theseuseless data packet exhausts the networkresources and hence legitimated user can notable to use the resources for validcommunication.

B. Blackhole Attack: In a blackhole attack, a malicious node sendsfake routing information, claiming that it hasan optimum route and causes other good nodesto route data packets through the malicious one.For example, in AODV, the attacker can senda fake Route Reply (RREP) (including a fakedestination sequence number that is fabricatedto be equal or higher than the one contained inthe RREQ) to the source node, claiming that ithas a sufficiently fresh route to the destinationnode. This causes the source node to select theroute that passes through the attacker.Therefore, all traffic will be routed through theattacker and the attacker can misuse or discardthe traffic.

4. Proposed Methodology

This paper will show via a simple statistical approach andwith existing routing protocols that in an Adhoc network malicious nodes can be detected using the probability densityfunction [10].In an adhoc Network, nodes who are suspected ofhaving the malicious are given a checking function, called the 'MCheck module' (malicious node testing), to detect selfishness of anode in a network.

The incidence of MCheck is defined as follows:

Let S be the event that a node has malicious, $\overline{S}$ 'bethe event that the node does not have selfishness, Pos bethe event that the node test is positive for the selfishness,and N be the event that the node test is negative for the malicious.
Using Bayes' theorem, $P(S \mid Pos)$ is calculated as follows-

$$(S|Pos)=\frac{P(S)P(Pos \mid S)}{P(S)P(Pos \mid S)+P(\overline{S})P(Pos \mid \overline{S})} \quad \ldots (A)$$

If the result is greater than 1, the conclusion is that thenode is more likely than not to have malicious. Same conclusion can be reached using the ratio –

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

If the ratio is greater than 1.5,the node is more likely than not to have malicious.After computing the ratio R, it canbe derived as theprobability that a node has the malicious given apositive result:

$$S=\frac{s}{1+s} \quad \ldots (C)$$

This agrees with (A): If $P(R/Pos)$ 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 malicious 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. This problem can be formulated with the help ofprior probability and continuous Bayes' theorem as, let R be the event that a node is regular, $\overline{R}$ be theevent that the node is not regular means malicious, and thenP(x | R) defines the normal density. The prior probabilities are $P(R)$ and $P(\overline{R})$

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

… (D)

and

$$P(x \mid \bar{R}) = \frac{1}{\sigma_{\bar{R}} \sqrt{2\pi}} e^{-\frac{1}{2}\left(\frac{x-\mu \bar{R}}{\sigma_{\bar{R}}}\right)^2}$$

… (E)

By continuous version of Bayes' Theorem

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

… (F)

So the node is slightly less likely to regular than not to regular. Another ratio that can be used is

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

If $R < 1.5$, the node is more likely not to be regular than to regular.

Using $\frac{R}{1+R}$ agrees with (F).

This statistical approach classified the regular and the malicious nodes. The densities are shown in figure 2.

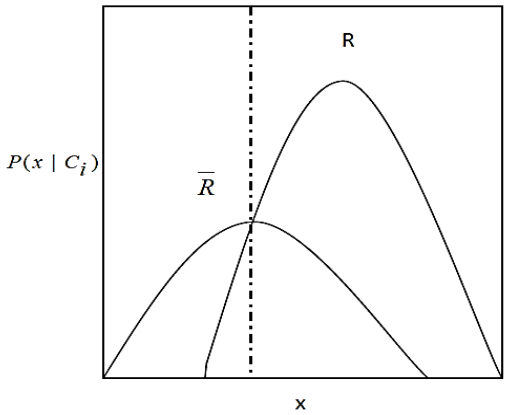

Fig. 2: The conditional density function of network

5. Conclusions

Mobile ad hoc networks exhibit new vulnerabilities to malicious attacks or denial of cooperation. This paper addresses the statistical approach to detect malicious nodes using the probability density function. The challenges of security, scalability, mobility, bandwidth limitations, and power constraints of these networks have not been completely unsolvedtill date. But the security problem can be minimized by using the proposed statistical approach that expresses the detection of malicious node like black hole node (single & multiple) and wormhole nodes in MANETs to secure the network. This statistical approach is verified by experimentation in NS-2 simulator 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 approach.

Reference

[1] H. Kim, R.B. Chitti and J. Song, "Novel defence mechanism against data flooding attacks in wireless ad hoc networks," IEEE Trans. on Consumer Electronics, Vol. 56, No. 2, pp. 579-582, 2010.

[2] W. Stallings, Wireless Communications and Networks, 2nd Edition, Pearson Education, 2007.

[3] M. Jensen, N. Gruschka and N. Luttenberger, "The Impact of Flooding Attacks on Network-based Services," 3rd Int. Conf. on Availability, Reliability and Security, ARES' 08, pp. 509-513, 2008.

[4] M. G. Zapata and N. Asokan, "Securing Ad-Hoc Routing Protocols," Proc. ACM Wksp. Wireless Sec., Sept. 2002, pp. 1–10.

[5] B. Kannhavong, H. Nakayama, Y. Nemoto, N. Kato and A. Jamalipour, "A survey of routing attacks in mobile ad-hoc networks," IEEE Wireless Communications, Vol. 14, No. 5, pp. 85-91, 2007.

[6] E. M. Royer and C. K. Toh, "A Review of Current Routing Protocols for Ad-Hoc Mobile Wireless Networks", IEEE personal communication, 1999.

[7] R. Bai and M. Singhal, "DOA: DSR over AODV Routing for Mobile Ad Hoc Networks," IEEE Trans. on Mobile Comp., Vol. 5, No. 10, pp. 1403-1416, 2006.

[8] D. B. Johnson and D. A. Maltz, "Dynamic Source Routing in Ad-Hoc Wireless Networks," Mobile Computing, T. Imielinski and H. Korth (eds.), Kluwer Academic Pub., pp. 153–181, 1996.

[9] S. K. Shandilya and S. Sahu, "A trust based security scheme for RREQ flooding attack in MANET," International Journal of Computer Applications, Vol. 5, No.12, 2010.

[10] Md. Amir KhusruAkhtar, 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.