International Journal of Advance Research in Science and Engineering
Vol. No.4, Special Issue (01), August 2015
www.ijarse.com
IJARSE
ISSN 2319 - 8354

PPN: PRIME PRODUCT NUMBER BASED MALICIOUS NODE DETECTION SCHEME FOR MANETS

Nusrat Inamdar[1], Aliya Inamdar[2]

[1,2]Student, Dept. of Computer network Engineering, S.I.E.T College of Engineering and Technology, Vijaypur, Karnataka, (India)

ABSTRACT

A mobile adhoc network is an autonomous network that consists of nodes which communicate with each other with wireless channel. Due to its dynamic nature and mobility of nodes, mobile adhoc networks are more vulnerable to security attack than conventional wired and wireless networks.In MANET,A routing protocol plays important role to handle entire network for communication and determines the paths of packets. A node is a part of the defined network for transferring information in form of packets. If all packets transferred from source to destination successfully, it has been assumed that the routing protocol is good. But, an attacker turns this dealing as a speed breaker and turning point of a highway. One of the principal routing protocols AODV used in MANETs.The security of AODV protocol is influence by malicious node attack. In this attack, a malicious node injects a faked route reply claiming to have the shortest and freshest route to the destination. However, when the data packets arrive, the malicious node discards them. To preventing malicious node attack, this paper presents PPN (Prime Product Number) scheme for detection and removal of malicious node.

I. INTRODUCTION

A wireless or mobile adhoc network (MANET) is formed by agroup of wireless nodes which agree to forward packets for eachother. One assumption made by most adhoc routing protocols isthat every node is trustworthy and cooperative. In other words, if anode claims it can reach another node by a certain path or distance,the claim is trusted. If a node reports a link break, the link will nolonger be used. Although such an assumption can simplify the designand implementation of adhoc routing protocols, it does make adhocnetworks vulnerable to various types of denial of service (DoS) attacks,One class of DoSattacks is malicious packet dropping. A malicious node can silentlydrop some or all of the data packets sent to it for further forwardingeven when no congestion occurs. Malicious packet dropping attackpresents a new threat to wireless adhoc networks since they lackphysical protection and strong access control mechanism. Anadversary can easily join the network or capture a mobile node andthen starts to disrupt network communication by silently droppingpackets.If malicious packet dropping attack is usedalong with other attacking techniques, such as shorter distance fraud,it can create more powerful attacks,which maycompletely disrupt network communication.Other routing attacks are gray hole attack, worm hole attack

Prime Product Number (PPN) scheme is proposed to mitigate the adverse effects of misbehaving nodes. The basic idea of the PPNscheme is that, each node in the network has a specific prime numberwhich acts as Node Identity and this identity must not be changed. MANET can be organized into a number of clusters in such a waythat every node is a member of at least one cluster, and there will beonly one node per cluster that will take care of the monitoring issue,which is generally called cluster head. When any intermediatenode/Destination Node generates RREP packet to the Source Nodethen it has to reply with Prime Product Number i.e. the product ofprime numbers from destination node to the source node and someother information. If Prime Product Number is fully divisible andReplied information is right then declare node as trustworthy nodeotherwise Call the process Removal of Malicious nodes.In this paper, PPN scheme is presented in detail and evaluationof the PPN scheme as an add-on to the Adhoc On Demand DistanceVector Routing (AODV) protocol.

III. LITERATURE SURVEY

Adrian Perrig et. al. [1] developed a Rushing AttackPrevention (RAP), a generic defense against the rushing attack foron-demand protocols. A set of generic mechanisms that togetherdefend against the rushing attack: secure Neighbor Detection, secureroute delegation, and randomized ROUTE REQUEST forwarding.Author also describe a technique to secure any protocol using an ondemandRoute Discovery protocol. The protocols discussed in thispaper require an instantly-verifiable broadcast authenticationprotocol, for which we use a digital signature. However, anysignature used should be able to keep up with verification at linespeed, to avoid a denial-of-service attack. When RAP is enabled, itincurs higher overhead than do standard Route Discovery techniques,but it can find usable routes when other protocols cannot, thusallowing successful routing and packet delivery when other protocolsmay fail entirely.

Tamilselvan et. al. [2] proposed an enhancement of the AODVprotocol by introducing fidelity table. The RREPs are collected in theresponse table and the fidelity level of each RREP is checked andone is selected having the highest level. After acknowledgement isreceived, the fidelity level of the node is updated proving it safe andreliable. The fidelity level of the participating nodes is updated basedon their faithful participation in the network. On receiving the data packets, the destination node will send an acknowledgement to thesource, whereby the intermediate node’s level will be incremented. Ifno acknowledgement is received, the intermediate node’s level willbe decremented. However, updating the fidelity table of each node bybroadcasting it to other nodes results in congestion and also theselection of wrong RREP from the response table cause another routerequest flooding.

Vishnu K et al. [3] used the concept of Backbone network.Backbone nodes (BBN) are a group of nodes which are powerful interms of battery and range. Backbone network is formed with thesenodes which are permitted to allocate Restricted IP addresses (RIP)to newly arrived nodes. The author assumes that the environment isin Backbone network. When source node wants to transmit data, itasks the nearest BBN for an unused RIP. Then the source nodetransmits RREQ to both destination and RIP. If the source node justreceives the RREP from the destination, this situation means thenetwork is regular and safe. If the source receives RREP from RIP;however, this situation means there are black hole in this route.Therefore, the source node sends a monitor message to alarm theneighbor node to go into promiscuous mode and let them start tolisten the network. The source would send some dummy datapackets to destination. At the same time the neighbor node canmonitor the situation of the forwarding packets. If the packet lossof the monitored node is beyond the normal case, the neighbornode would alert source node about the situation. The sourcenode would identify the monitored node as black hole byreceiving the responded messages of the neighbors. The network environment is assumed that the normal nodes are more thanthe malicious nodes. The original design of MANETs does nothave Backbone network, therefore this concept and method onlycan suit special environment. If we only use the method of RIP,the method cannot lock the black hole and remain need tomonitor and observe the suspicious node.

Khalil et al. [4] introduces LITEWORP in which they usedthe notion of *guard node*. The guard node can detect the wormhole if one of its neighbour is behaving maliciously. The guard node is acommon neighbour of two nodes to detect a legitimate link betweenthem. In a sparse network, however, it is not always possible to find aguard node for a particular link.

Jaydip Sen et.al. [5] described the mechanism whichmodifies the AODV protocol by introducing two concepts, (i) datarouting information (DRI) table (ii) cross checking. DRI table hastwo bits information which is used by the nodes that respond tothe RREQ message of a source node during route discoveryprocess. Each node maintains an additional data routinginformation (DRI) table. The process of cross checking theintermediate nodes is a one-time procedure which should beaffordable for the purpose of security. The source node broadcasts aRREQ message to discover a secure route to the destination node.The intermediate node that generates the RREP has to provideinformation regarding its next hop node and its DRI entry for thatnext hop. Upon receiving the RREP message from intermediate node(IN), source node(SN) will check its own DRI table to see whetherIN is its reliable node. If SN has used IN before for routing datapackets, then IN is a reliable node for SN and SN starts routing datathrough IN. Otherwise, IN is unreliable and thus SN sends furtherroute-request (FRQ) message to next-hop-node (NHN) to check theidentity of the IN.

Saurabh Gupta et. al. [6] described a protocol BAAP foravoiding malicious nodes in the path using legitimacy tablemaintained by each node in the network. BAAP uses Adhoc OndemandMultipath Distance Vector (AOMDV) to form link disjointmulti-path during path discovery. When intermediate nodes reply tosource node, few nodes in the path may have multiple paths to thedestination but it eventually chooses only one path to destinationnode. In BAAP, each node maintains a legitimacy table to choose themost legitimate node to source node and next hop to destination)while sending RREP back to source node. Legitimacy table containsthree fields: NodeID, Pathcount and Sentcount. NodeID field storesthe IP address of the node whose legitimacy is being recorded.Pathcount field specifies the number of times the node has beenchosen in the route and the Sentcount field describes the number oftimes connection to destin0.ation have been successfull node throughthe NodeID. These two count field are also used to define theLegitimacy Ratio (Sentcount/(Pathcount +1)) of a NodeID whichindicates the confidence of node in performing its intended functionof correct routing. A higher legitimacy ratio means higher possibilityof a node being non-malicious.

Piyush Agrawal et. al. [7] proposed a complete protocol todetect a chain of cooperating malicious nodes in an adhoc networkthat disrupts transmission of data by feeding wrong routinginformation. Proposed techniques is based on sending data in termsof equal but small sized blocks instead of sending whole of data inone continuous stream. The flow of traffic is monitoredindependently at the neighborhoods of both source and destination.The results of monitoring is gathered by a backbone network oftrusted nodes. With assumption that a neighborhood of any node inthe adhoc network has more trusted than malicious nodes, ourprotocol can not only detect but also

IJARSE
ISSN 2319 - 8354

remove a chain of cooperatingmalicious nodes (gray/black hole) by ensuring an end-to-endchecking between the transmission of two blocks of data.

Rutvij H. Jhaveri et. al. [8] proposed a novel approach AdhocOn-demand Distance Vector (AODV) protocol for Gray Hole andBlack Hole Attacks. In this proposed mechanism, an intermediatenode receiving abnormal routing information from its neighbor nodeconsiders that neighbor node as a malicious node. The intermediatenode appends the information about the malicious node in the routereply packet and every node receiving that reply packet thenupgrades its routing table to mark the node as malicious node. Whenrouting request is sent, a list of malicious node is appended to thepacket and every node receiving the packet upgrades its routingtable to mark the listed nodes as malicious. The proposed schemenot only detects but also removes malicious node by isolating it, tomake safe and secure communication.

Black hole attack is Denial Of Service (DoS) attack on routingtraffic.In this attack, a malicious node tries to capture the path towarditself by falsely claiming larger sequence number and smaller hopcount to the destination and then absorb all data packet withoutforwarding them to destination node. Progress of a black hole attackis illustrated as when Source node intends to establish a route todestination node, by broadcasting route request (RREQ) packet.However, when black hole node (BH) receives an RREQ, itimmediately sends an RREP which is having larger sequence numberand smaller hop count to source node. On receipt of RREP from BH, the source starts transmitting the data packets, which BH simplydrops instead of forwarding to the destination. A black hole can beformed either by a single node or by several nodes in collusion [9].

A Gray hole attack is a variation of the black hole attack, wherethe malicious node is not initially malicious, it turns malicioussometime later. During Worm hole attack, a malicious node capturespackets from one location in the network and “tunnels” them toanother malicious node at a distant point which replays them locally.The tunnel can be established in many ways e.g. in-band and out-ofbandchannel[10].

The former is an exposed or open wormhole attack [11]while the latter is a hidden or close one. This makes the tunneledpacket arrive either sooner or with a lesser number of hops comparedto the packets transmitted over normal multi hop routes. Whenmalicious nodes form a wormhole they can reveal themselves or hidethemselves in a routing path. In general terms, an attacker that canforward ROUTE REQUESTs more quickly than legitimate nodes cando so, can increase the probability that routes that include theattacker will be discovered rather than other valid routes.

III.METHODOGOLY

In MANETs, routing misbehavior can severely degrade theperformance at the routing layer. Specifically, nodes may participatein the route discovery and maintenance processes but refuse toforward data packets. How do we detect such misbehavior? How canwe make such detection processes more efficient (i.e., with lesscontrol overhead) and accurate (i.e., with low false alarm rate andmissed detection rate)? Prime Product Number (PPN) scheme is proposed to mitigate the adverse effects of misbehaving nodes. The basic idea of the PPNscheme is that, each node in the network has a specific prime numberwhich acts as Node Identity and this identity must not be changed. MANET can be organized into a number of clusters in such a waythat every node is a member of at least one cluster, and there will beonly one node per cluster that will take care of the monitoring issue,which is generally called cluster head. When any intermediatenode/Destination Node generates RREP packet to the

Source Nodethen it has to reply with Prime Product Number i.e. the product ofprime numbers from destination node to the source node and someother information. If Prime Product Number is fully divisible andReplied information is right then declare node as trustworthy nodeotherwise Call the process Removal of Malicious nodes.In this paper, PPN scheme is presented in detail and evaluationof the PPN scheme as an add-on to the Adhoc On Demand DistanceVector Routing (AODV) protocol.

In PPN scheme,every Cluster head node maintains the neighbor table which is usedo keep information about all the nodes In the path discovery of PPNscheme, an intermediate node will attempt to create a route that doesnot go through a node whose replied information is wrong and PPNis not fully divisible. Therefore, malicious nodes will be graduallyavoided by other non-malicious nodes in the network.

3.1 RREQ Packet

Type	J	R	D	G	U	Reserved	Hop Count
RREQ ID							
Originator IP Address							
Originator Seq Number							
Destination IP Address							
Destination Seq Number							

Figure 3.1 RREQ Packet in PPN

3.2 RREP Packet

In the proposed scheme RREP has additional Node ID, PrimeProduct Number and Cluster Head Node ID of NRREP fields shown inFigure 2. Node ID field is used to store ID of NRREP , Prime productnumber is used to store the prime product of all the nodes fromdestination to source in the path and cluster head node ID of NRREPfield contains the cluster head Node ID of the node which originatesthe RREP.

Type	R	A	Reserved	Prefix Size	Hop Count
Source IP Address					
Destination IP Address					
Destination Seq Number					
Life Time					
Node ID		Prime Product Number		Cluster Head Node ID Nrrep	

Figure3.2 RREP Packet in PPN

3.3 NeighbuorsTable

In PPN scheme each cluster head maintains a neighbor tablewhich is used to keep information about all the nodes as shown inTable 1. Neighbor table contains two fields Node ID and ClusterHead Node ID. Each node in the network has a specific primenumber which acts as Node Identity and this identity must not bechanged.

Every node is associated with a Cluster Head into thenetwork. Each node's ID and its Cluster Head ID are stored into thetable.

TABLE 3.3 :Neighbor Table

Node ID	Cluster head node ID

The proposed scheme relies on reliable nodes (nodes through which source has routed data previously and knows them to be trustworthy) to transfer data packets. The algorithm for the proposed mechanism is depicted in Fig. 4.3 and Fig 4.4 In the modified protocol, the source node (SN) broadcasts a RREQ message to discover a secure route to the destination node. The intermediate node (IN) that generates the RREP has to provide information regarding its cluster head and product of all prime numbers from destination to source node in the form of Prime

Product Number (PPN). Upon receiving the RREP message from IN, SN with the help of its cluster head (CH) will divide the PPN with the Node IDs stored in neighbor table at CH to see whether IN is its reliable node. If SN finds that IN replied information is right and PPN is fully divisible, then IN is a reliable node for SN and SN starts routing data through IN. Otherwise, IN is unreliable and thus SN calls the malicious node removal process and Subsequently SN ignores any other RREP from the malicious node.

3.4 Algorithm to Detect Malicious Node Attack in MANET's

Notation :

MN: malicious node N_{RREP} :RREP from an intermediate node

1. Begin
2. For (source node)
3. {
4. Broadcast RREP packet to every neighbor node
5. Receive RREP
6. RREP will be choose among various reply having largest sequence number &minimum hop count and all other RREP buffered at originating node
7. Process RREP
8. }
9. If (prime product team if fully divisible && replied info is right)
10. Declare node as trustworthy node
11. Else
12. {
13. Declare N_{RREP} as MN
14. Call removal of malicious node();
15. }

3.5 Removal Process of Malicious Nodes and Algorithm to Remove Malicious Nodes from MANET's

1) Cluster Head Node 5 adds Malicious Node M to themalicious list. Now, Node 5 broadcasts the malicious list tothe whole network

CH : Cluster Head MN: Malicious node

1. Begin
2. Respective CH adds MN to malicious node
3. Broadcast this list to the whole network
4. All nodes of the network after getting the malicious list finds the node ID's of the malicious node in their table.
5. Each node flushes all the enters related to these node ID's from the respective tables
6. End

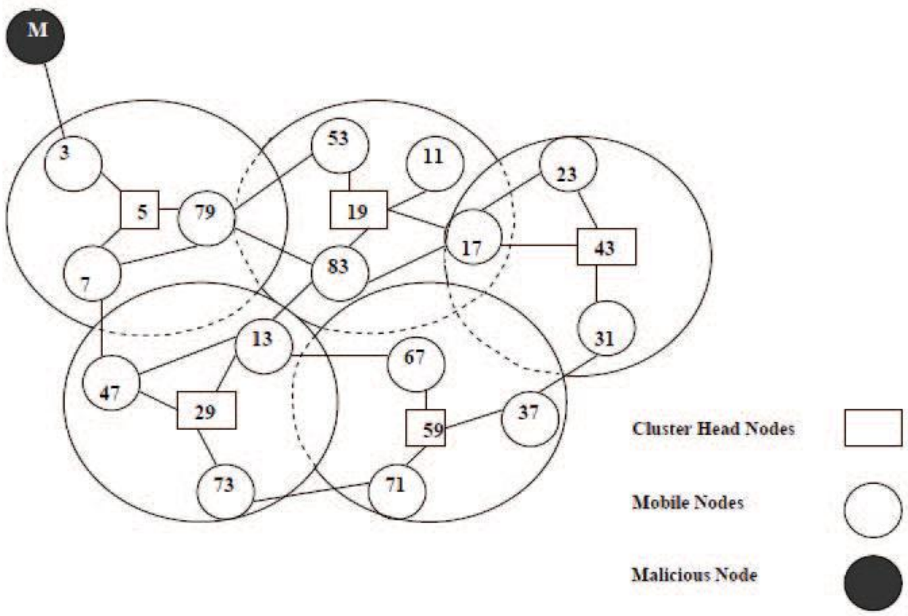

Figure 4.5 Network Topology of PPN Scheme

2) All nodes of the network after getting the malicious listfinds the Node M in their tables and each node flushes allthe entries related to Node M from the respective tables.

V. CONCLUSION

In this paper, A security protocol has been proposed that can be utilized to identify malicious nodes in aMANET and thereby identify a secure routing path from a source node to a destination node avoiding the malicious nodes(i.e Prime Product Number (PPN) scheme is proposed to mitigate the adverse effects of misbehaving nodes. The basic idea of the PPN scheme is that, each node in the network has a specific prime number which acts as Node Identity and this identity must not be changed). As future work we intend to include that the proposed security mechanism may be extended so that it can defend against themalicious nodes which are present inside the clusters. The nextstep is to simulate more scenarios in which more complicatedmisbehaviors exist and other metrics need to be measured suchas latency and end-to-end delay.

REFERENCES

[1] Yih ChunHu, Adrian Perrig, David B. Johnson" Rushing Attacks and Defense in Wireless Adhoc Network Routing Protocols", San Diego,California, USA September 19, 2003.

[2] L. Tamilselvan, and V. Sankaranarayanan, "Prevention of Cooperative black hole attack in manet", Journal of Networks, Vol. 3 (5), pp.13-20,2008.

[3] Amos J Paul ,Vishnu K "Detection and Removal of Cooperative Black/Gray hole attack in Mobile Adhoc Networks" International Journal of Computer Applications (0975 - 8887) Volume 1 – No. 22 ,2010.

[4] Issa Khalil, Saurabh Bagchi, Ness B. Shroff' LITEWORP: A Lightweight Countermeasure for the Wormhole Attack in Multihop Wireless Networks" Proceedings of the 2 International Conference on Dependable Systems and Networks (DSN'05).

[5] Jaydip Sen, Sripad Koilakonda, Arijit Ukil, "A Mechanism for Detection of Cooperative Black Hole Attack in Mobile Adhoc Networks" IEEE Second International Conference on Intelligent Systems, Modeling and Simulation, 2011.

[6] Saurabh Gupta, Subrat Kar, S Dharmaraja , "BAAP: Black hole Attack Avoidance Protocol for Wireless Network" IEEE proceedings of the International Conference on Computer & Communication Technology (ICCCT),2011.

[7] Piyush Agrawal and R. K. Ghosh "Cooperative Black and Gray Hole Attacks in Mobile Adhoc Networks" Indian Institute of Technology,Kanpur - 208 016, INDIA.

[8] Rutvij H. Jhaveri, Sankita J. Patel and Devesh C. Jinwala "A Novel Approach for GrayHole and BlackHole Attacks in Mobile Adhoc Networks" Second International Conference on Advanced Computing & Communication Technologies, 2012.

[9] M. Al-Shurman, S.-M. Yoo, and S. Park, "Black hole attack in mobile adhoc networks," in Proceedings of the 42nd annual South east regional conference. New York, NY, USA: ACM Press, pp. 96-97, 2004.

[10] M. Al-Shurman, S.-M. Yoo, and S. Park, "Black hole attack in mobile adhoc networks," in Proceedings of the 42nd annual South east regional conference. New York, NY, USA: ACM Press, pp. 96-97, 2004.

[11] M. Al-Shurman, S.-M. Yoo, and S. Park, "Black hole attack in mobile adhoc networks," in Proceedings of the 42nd annual South east regional conference. New York, NY, USA: ACM Press, pp. 96-97, 2004.