Secure Zone Routing Protocol for Manet

Ranjeetha.S, Renuga. N, Sharmila. R

Department of computer science and engineering, Adhiyamaan College of engineering, Hosur

Abstract— *Secure Zone Routing Protocol is a contribution in the field of security analysis on mobile ad-hoc networks, and security requirements of applications. Limitations of the mobile nodes have enabled us to design a secure routingprotocolthat prevents different kinds of attacks. This approach is based on the Zone Routing Protocol (ZRP) the most popular hybrid routing protocol used for better performance, Intrusion Detection System, is based on the principle of network, nodes or information misuse detection system, which can accurately compare the signatures of known attacks. The importance of the proposed solution lies in the fact that it ensures security as needed by providing a comprehensive architecture of Secure Zone Routing Protocol (SZRP) based on efficient key management, secure neighbour discovery, secure routing packets, detection of malicious nodes, and preventing these nodes from destroying the network. In order to fulfil these objectives, both efficient key management and secure neighbour mechanisms have been designed to be performed prior to the functioning of the protocol.To validate the proposed solution, we use the network simulator NS-2 to test the performance of secure protocol and compare it with the conventional zone routing protocol over different number of factors that affect the network. Our result is a secure version of conventionalZone routing protocol in terms of packet delivery ratio while it has a tolerable increase in the routing overhead and average delay. Also, security analysis proves in details that the proposed protocol is robust enough to all classes of ad-hoc attacks.*

IndexTerms—ad-hoc networks,securerouting,secure neighbourdiscovery,digitalsignature,zone routing protocol, secure zoneroutingprotocol

I.INTRODUCTION

Mobile ad-hoc network is a wireless and baseless network which does not require any physical media or infrastructure to communicate between wireless ad-hoc network nodes. A mobile ad hoc network (MANET) is a self-configuring infrastructure less network of mobile devices which is connected by wireless. This Wireless is a technology that allows users to access information and services in spite of the geographic position. Mobile ad hoc network (MANET) is an autonomous group of mobile users who communicate with each other without any fixed infrastructure and centralized administration [2]. Since the hosts are mobile, the network topology may change rapidly and unpredictably over time.

Theattractive features ofad-hoc networks such as openmedium,dynamic topology,absenceof central authorities,anddistributedcooperationholdthead-hocnetworksacrossarangeof civil, scientific,militaryandindustrialapplications [1]. However,thesecharacteristicsmake ad-hocnetworks vulnerable todifferenttypesofattacksandmake implementingsecurity inad-hocnetworkachallenging task.Themainsecurityproblemsthatneedtobedealt with inad-hoc networks include: the identityauthenticationofdevicesthatwishtotalktoeachother, thesecure keyestablishmentofkeysamongauthenticated devices,the secureroutinginmulti-hopnetworks,andthe securetransferof data[22].Thismeansthatthe receivershould be abletoconfirmthattheidentityofthesourceor the sender(i.e.,one hoppreviousnode) isindeedwhoor whatitclaimstobe.Italsomeansthatthe receivershould beabletoverifythatthecontentofamessagehasnot beenalteredeithermaliciouslyoraccidentallyintransit Inthispaper, weproposesecuringoneofthemost popularhybridprotocols:zoneroutingprotocol(ZRP). ZRP [16] aims to address excess bandwidth and long route request delay of proactive and reactive routing protocols. It combines the advantages of these approaches bymaintaining an up-to-date topological map centred on each node. The separation of anode's local neighbourhood from the global topology of the entire network allows forapplying different approaches, and thus taking advantage of each technique's featuresfor a given situation. These local neighbourhoods are called zones; each node may be within multiple overlapping zones, and each zone may be of a different size. The nodes of a zone are divided into peripheral nodes whose minimum distance to the centre is exactly equal to zone radius, gray nodes, and interior nodes whose minimum distance to the centre is less than zone radius, white nodes.ConventionalZRPisnot secureas it doesnot consider securityrequirements.Wemodifyitbyusingfourstages asshowninFig.1.First,we use anefficientkey management mechanismthatisconsideredasa prerequisiteforany security mechanism. Then, we provide a secureneighbourdetectionscheme thatrelieson neighbourdiscovery,timeandlocationbasedprotocol s[3, 4].Securingroutingpacketsisconsidered asthethird stagewhichdependsonverifying theauthenticityofthe senderandtheintegrity of thepacketsreceived.Finally, detection ofmalicious nodesmechanism is usedto identifymisbehaving nodesandisolatethem using blacklist.Once thesegoalsareachieved,providing confidentialityoftransferreddatabecomesaneasy task which can be implemented using any cryptography system.

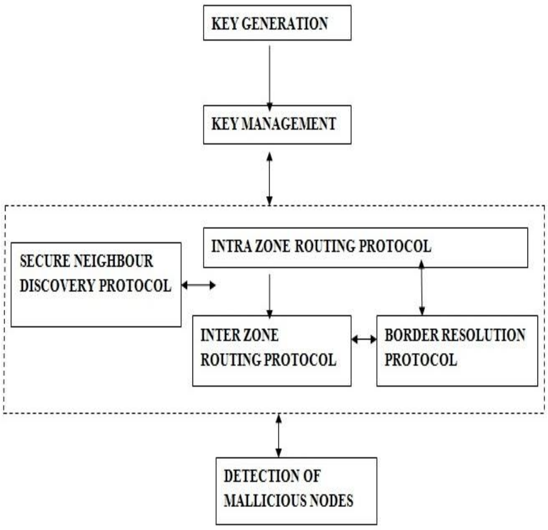

Fig1. Secure Zone routing protocol for MANET

II.DESIGNOFSECUREZONEROUINGPROTOCOL (SZRP)

A. Key Generation

Keygenerationistheprocessofcalculatingnew key pairsforsecurity purposes.Inourdesign,thisincludes generationofpublic/privatekey pairfordigitalsignature. Thegenerationprocessisperformedwhenthenode is created(bootstrapping phase).Algorithm for key generation is as follow

{

Select two large prime numbers p and q such that $p \neq q$

$n \leftarrow p*q$

$\Phi(n) \leftarrow (p-1)*(q-1)$

Select e such that $1 \leq e \leq \Phi(n)$ and e is a co-prime to $\Phi(n)$

$d \leftarrow e^{-1} \bmod \Phi(n)$

$K_A^- \leftarrow (e, n)$

$K_A^+ \leftarrow d$

Return K_A^- and K_A^+

Afterkeygeneration,the nodekeepsitsprivatekeyandannouncesthepublickey in aneighbour advertisement message in responseto a neighboursolicitationsmessageandafterverification ofits neighbours.

B. Key Management

Key management is the management of cryptographic keys in a cryptosystem. This includes dealing with the generation, exchange, storage, use, and replacement of keys. It includes cryptographic protocol design, key servers, user procedures, and other relevant protocols.Keymanagementisofthegreatestinterest,s inceitisa prerequisite for any security procedures of publicly- knowncryptographicalgorithms.For example,inSKC, sharedkeysor pre-sharedsecretsshouldbe arrangedfor involvednodesbeforetheycancommunicate. InPKC, senders should obtain the public-key of receiversand verifyitwith trustedthird-parties.

For communicationin MANETs, nodes need to identifyothernodesoftheir interest.Therefore,mobile nodescanbeidentifiedbytheirownidentityofspatial and temporal invariance. For example, nodes propose their identitywhenjoining MANET systems. Nodes shouldbeassistedwithadditional security proceduresto ensuretheconfidentiality,integrity,andauthenticity of their informationexchangewithintendednodes.Without thehelpofatrustedkey distributioncanter(KDC),ora trustedcertificationauthority (CA)oranypre-existing communicationandsecurityinfrastructures,nodes may havetodealwithunknownrelayingnodeswithoutthe pre-established trust worthiness, and hence becomevulnerable tovariouspassive andactiveattacks.To overcome this weakness, we base our design on the conceptofidentity-basedkeymanagementwhichserves as a prerequisite for various security procedures[1]. The basicideaisto useanidentifierthathasastrong cryptographicbinding with the publickeyand componentsofthemobilenodeinthesamemannerthat issuggestedfor MIPv6 in[14]. Wewillcallthisidentifier, UniqueIdentifier(UI).Thisidentifiershouldbeowned and used exclusivelybythecreatednode. An address (64-bits) that satisfies properties of required UIis obtainedasfollows:

(a) Themost32-bitsrefertotheMACaddressofthe node.

(b) Theleast32-bitsrefertocertainprocessingonthe publickey generatedby thenodeatbootstrappingphase, thesebitsareextractedby(1)computingthehashvalue ofthepublickeyusingSHA-1, (2) dividing the hash valueintofourpartseachof32-bits,and(3)performing anXORoperationonthedividedhash values andthe locationofthenode, L, usedasanevidence.

Algorithm used for generation of unique identifier is as follows

{

L <–Location of the node using GPS system

Digest <–H[K_A^-]

Break the digest into four chunks (D_0 – D_3)

UI<–Concatenate (MAC,(D_0⊕D1⊕D2⊕D3⊕L)

Return UI

Thisuniqueidentifiercomposedoftheconcatenation of theIPaddressandthehashvalue of thepublic keyis securebecauseanattackercannotproduceanew pairof keysthathasthesamehash valueduetosecondpre-imageresistanceofone-wayhashfunction,ordiscover theprivatekeyforthegivenpublickey.Afterobtaining theUI,keymanagementmechanism isperformedas follows:

(a) The mobile node sendsbinding update message MSG1containing theUI describedabovewithanonceto itscorrespondingnode.

(b) The corresponding node replies with MSG2 containingthesamenonceproducedbythemobilenode.

(c) WhenreceivingMSG2,themobilenodeverifiesthat thenonceisthesameaswhatitwassentinMSG1.It sendsMSG3thatcontainsitspublickey andtheevidence usedtogeneratetheUI.Thismessageissignedbythe private keyof themobilenode.

(d)Whenthecorresponding nodereceivesMSG3,it verifiesthesignatureusing theincludedpublickey,and verifiesthatthispublic keyandtheevidenceproducethe sameleast32-bitsoftheUI.Oncethemessagepassesthe twoverifications,itconcludesthatthemobile nodeowns thisaddressandthe publickey.Thecorrespondingnode storestheaddressandthekey ofthemobilenodetobe usedinfurthermechanisms.

Theproposedkeymanagementmechanismproposedis efficientsincenodescansafelytrustthecorresponding nodeswhentheyclaimownershipofthatidentifier.It also will not increase the complexity of the network because:(1)notallnodesneedtousethemechanisms, only thosenodes thatwishtoperformbindingupdates,(2) notallnodesneedtoverify MSG3,onlythosenodesthat wanttoacceptthebindingupdate,and(3)messagesare exchanged directly between the mobile node and its neighboursandarenotrouted toothernodes.

C. Secure neighbour Discovery

In wireless networks, eachnode needs to knowits neighbourstomakerouting decisions;itstoresneighbour informationinitsroutingtablethatcontainstheaddress oftheneighbour,andthelinkstate.InMANETs,nodes useneighbourdiscovery protocoltodiscoversurrounding nodes theycandirectlycommunicatewithacrossthe wirelesschannelwith signalpropagation speed by considering thelocationorroundtripinformation.Two differentnodes,AandB, areconsideredasneighboursand thuscanexchangeinformationdirectlyifandonly ifthe Euclideandistance,|AB|,betweenthem islessthanor equaltotheneighbourdiscovery range,R.TheNDP protocolrelieson HELLOmessage exchange.Hello messages are used to detect and monitor links to neighbours.IfHellomessagesareused, eachactive node periodicallybroadcastsaHellomessagethatincludesal l itsneighbours.Becausenodesperiodically sendHello messages, if a node fails to receive several Hello messagesfromaneighbour,alinkbreakisdetected[3]. Thenodesneedacorrectviewofneighbourinformation which raises the importance of applying a secure neighbourdetectionprotocol.NDPprotocoliswidelyused; however,itcanbeeasilyattackedduetolackofsecurity. A malicious node can easily relay or replay packets deluding other nodes that are communicated directly. Manymethodshavebeenproposedtoprotectneighbour informationinhostileenvironments[13].However,these methods can only protect neighbourrelation between benign nodes while compromised nodes can easily circumventthemand setupfalserelations.

Inourmodel,we use a combinationof twotechniques thatrelyon timeand locationbasedon secure neighbour discovery mechanisms. Webased ourdesign on NDP protocolandusethesameHELLOmessagetodecrease the number of message flows, and hence the loss of power.Time basedprotocol(T-based),requiresnodesto transmitauthenticatedmessagescontainingatime-stamp setatthetimeofsending.Upon receiptofsuch amessage, a receiver checksits freshnessbyverifying that themessagetimestampiswithina thresholdof the receiver's currenttime. Ifso,itacceptsthemessagecreatorasa neighbour.T-basedprotocols arenotefficientinallcases. Forexample,they leadtoimpossiblyresultsifthe adversary nodehastheability torelayapacketunderthe predefinedthreshold value. Intimeandlocationbased protocols (TL-based), anode requires sending authenticatedmessagescontaining atime-stampsetatthe timeof sending,andtheirownlocation.Uponreceiptof suchamessagesentfrom anodeB,thereceiverA calculatestwoestimates;the firstestimateisbasedonthe difference ofits ownclock at reception time andthe message'stime-stamp.The secondone iscalculatedwith the helpof thelocation.If the twodistanceestimatesare equal,AacceptsBasaneighbour.

TheproposedsecureNDPprotocolconsistsof three rounds;in thefirstroundthenodebroadcastsaHELLO messagewithitslocation, thetimeofsending,andthe authenticationpartwhichindicatesthat the locationand timeofsending areauthenticatedby nodeA. Authentication process is performed using digital signature with the private key of node A. When the packetisreceivedinthe secondround,thereceiver computesthedistanceusing thelocationvaluesstoredin thepacketandtransmissiontime,then,it comparesthe resultsobtained withtherangeoftransmission.Ifthetwo distanceestimates are equal,it verifies the signature. Once the signature isverified,BacceptsA asneighbour, signsthe packetandreplieswithbeaconacknowledge. OncenodeA receivesthe beaconacknowledges,it comparestheevidence withthetransmittedone;ifthe twovaluesareequal,itverifiesthe signatureof the receivedpacket using B's public key. If verification processischeckedcorrectly,nodeA acceptsBasa neighbour,andupdatesitsentiretablebyassigning azero valueto thetrustlevelofnodeB.

The three rounds of the secure neighbour discovery are as follows

A :Signature=RSA $_{KA+}$($T_{A,}L_A$)
A–>* :<HELLO Message,$T_{A,}L_{A,}$Signature>
B :T<–(T_A+ΔT)-Tr
:D_1<– C*T
: D_2<–|L_A- L_B|
:IIF(D_1=D2&& D_1≤R)
: V<–Verify $_{KA-}$(($T_{A,}L_{A,}$Signature)
:if(v=TRUE)
:Accept A as a neighbour
:Else, Reject the packet
:<ACK, $L_{A,}$Signature>
B–>A :V<–Verify $_{KB}^{-}$(($T_{A,}L_{A,}$Signature)
A :Accept B as neighbour
:Update the neighbour table

Here,weassumedthatcorresponding nodeshave accuratetimeandlocationinformationbased on synchronized clocks and GPS. Inaccurate time and location information can be easily handled by taking into accountanacceptablesmalldifferencewhencomparing theestimatedvalues.

D. Secure Routing Packets

Oncewe achievesecureinformationexchange,wecan furthersecuretheunderlyingrouting protocolinwireless ad-hocnetworks.Securityservicesin MANETsbelongto twokindsofmessages:therouting messagesandthedata messages.Bothhaveadifferentnature anddifferent security needs. We focus here on securingrouting becausedatamessages are point-to-pointandcanbe protectedwithany point-to-pointsecuritysystem.Onthe otherhand,routing messagesaresenttointermediate neighbours,processed,possibly modified,andresent. Moreover,asaresultofprocessing ofroutingmessage,a nodemightmodifyitsrouting table.Thiscreatestheneed for boththe end-to-endandthe intermediatenodestobe able toauthenticatethe informationcontainedinthe routingmessages.

The algorithm for secure routing packets is as follows

Input: new routing packet P from source S to destination D.
{
Signature<– RSA $_{Ks}^{-}$ (p)
Select Case (P.type)
Case 1: IAPR
If (Signature=P.signature)
Update tables.

Update the packet according to ZRP procedures.
Signature <– RSA $_{KA}^{+}$ (p)

Append Signature to the packet P.
Broadcast the packet to neighbours.
Return 0
Else
Drop the packet
Detection of Malicious node(S)
Return 0

End If
Break;
Case 2: IEPR
Digest<–H[p].
Update tables.
Update the packet according to ZRP procedures.
Signature <– RSA $_{KA}^{+}$ (p)
Digest<–H[P].
Append Signature and Digest to the packet P.
Border cast the packet to peripheral nodes.
Return 0
Else
Drop the packet
Detection of Malicious node(S)
Return 0
End If
Break;
End Select
}

IfallroutingmessagesinMANETsareencryptedwith a symmetriccryptography,itmeansthateverymember wantstoparticipateinthenetworkhastoknow the common key. This is the best solution for military networksorany trusted-membersnetworkwhereevery membershouldknowthecommonkey beforejoiningthe network.However,thisis not asuitablesolutionfora conventionalMANETsuchasmeetingroomorcampus inwhichmembersarenottrusted[15].Thebestoptionis touseasymmetriccryptography sothattheoriginatorof theroutemessagessignsthemessage. It wouldnotbe neededtoencrypttheroutingmessagesbecause theyare notsecret.Theonlyrequirementisthatthe nodeswillbe abletodetectforgedroutingmessages. Toaccomplish thisgoalweusebothdigitalsignatureandone-way hash functiontoattainmessageauthentication,and message integrityasdescribed inmoredetailbelow.

Secure Intra Zone Routing Protocol

To providepacketauthenticationandmessageintegrity inIARP,digitalsignatureusingRSA isused.TheIARP packetformatisshown inFig.2.Allshaded fieldsinthe packet willbesigned using RSAalgorithmusingthe privatekey ofthesender.Thesignatureisstoredinthe packetbeforebroadcasting ittoits neighbours.This signaturewillprovide theauthenticity andintegrity ofthe senderand thepacketrespectively.

Secure IARP Scenario

Eachnodeperiodicallyadvertisesitslinkstate(current setofneighboursandcorresponding listsoflinkmetrics) throughitsrouting zone.Thescopeoflinkstateupdateis controlledby theTime-To-Live(TTL)valuethatis initializedwiththezoneradiusminusone.Thesource node signs the whole packet using its private key, appendsthesignaturetothepacket,andbroadcastittoits surrounding neighbours.Uponreceiptoflink stateupdate packet, thereceiver starts processingthepacket ifthe senderhasa hightrustedvalue.Once thisisachieved,the receivercreatesacopyofthemessageusingthepublic keyofthesourcealreadystoredinitsneighbours'table, andcomparestheresultwiththereceivedmessage.Ifthe packetpasses the verificationprocess,therouting tableis recomputedandthe packet'sTTLvalue isdecremented. The process is repeated as long as the TTL value is greater thanzero.

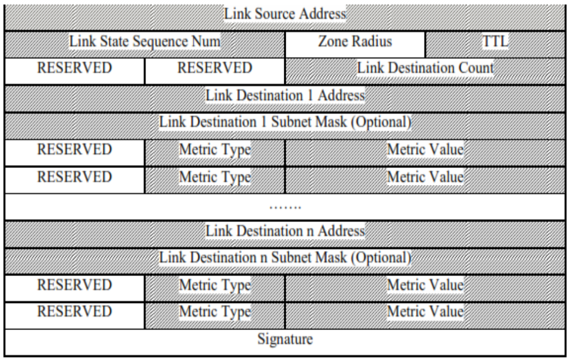

Fig2. LinkstateIARPpacketformat

Secure Inter zone Routing Protocol

To secure IERP packets, we make end-to-end authenticationusing digitalsignatureofthenon-mutable fieldsof the packets,the dashedfieldsofthe packetas illustratedinFig.3,andaone-way hashfunctionto achievetheintegrityofmutablefieldswhilethepackets are transmittedthroughintermediatenodes.The informationgeneratedbyapplying thehashfunctionand thedigitalsignatureistransmittedwithinthepacketthat werefertobysignatureanddigest.Weusetheterms IERPdigitalsignature,andIERPhashing toidentifythe twomechanismsthatare usedtosecureIERPpackets. Moredetailsaboutthefunctionality ofthesemechanisms follow.

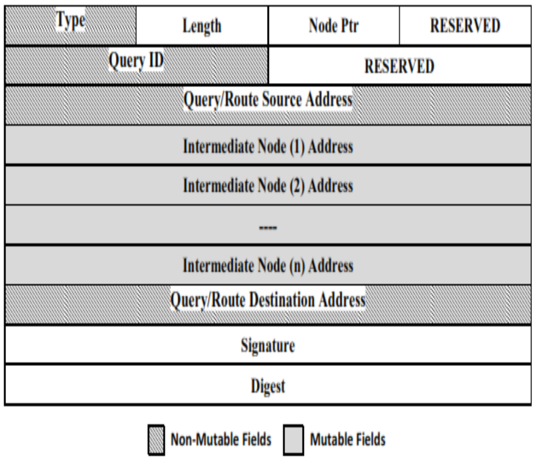

Fig3. IERPpacketformat

IERP Digital signature

Digital signatureusing RSAis usedto protectthe integrityofthenon-mutablefieldsofthepacketusing the privatekey oftheinitiator.Thesignatureisstoredinthe packetbeforeborder-casting it.Inordertodecreasethe overheadonintermediatenodes,thesigning processis carriedoutbythesourceofthepacketin the route request packetandby thedestinationfortheroutereplaypacket. Thismayleadtoaprobleminthe verificationofthe route replay. Theproblem willappeariftheRREPpacketis generatedbyanintermediatenodewhichhasthelinkto thedestination. To avoid this problem, werestrict the generation of RREP message to the destination only, while intermediate behave as they do not have routeandforward theRREQmessage.Although thismay leadtosignificantly increaseintheresponsetime,itwill decrease theoverheadoftheverificationprocess.

IERP Hashing

SZRPuseshashingtoattaintheintegrityofthepackets sinceauthenticationofdatainrouting packetsisnot sufficient,asanattackercouldremoveanodefrom the nodelist.Hashing isperformedonthemutablefieldsof IERPpackets,the digestobtainedisappendedtothe packet,and thepacketisborder-casted.Thedigestisused toallow everynodethatreceivesthemessage,eitheran intermediatenode or thefinaldestinationnode,toverify thatthese fieldsandespeciallytherouteto thedestination havenotbeenalteredby adversarynodes.

Secure IERP Scenario

Everytimeanoderequiresaroutetoadestinationbut doesnothavetheroutestored initsroutetable,itinitiates a RREQpacketwiththeformatshowninFig.3,sets the QueryIDtoanewidentifierthatithasnotrecentlyused in initiatinga routediscovery.Query/routesourceaddress and query/route destination address are set to the addressesof the sourceanddestination,respectively.The sourcethencomputesthedigital signatureofthenon-mutable fields and the hash value of its public key, appends them to the signature and digest fields, and border-caststhe packettoitsperipheralnodes.Whenany nodereceivesthepacketforwhichitisnotthetarget node,itchecksitslocaltablefrom recentrequestsithas receivedtodetermineifithasalreadyseenarequestfrom thissamesource.If ithas,thenode discardsthepacket; otherwise,thenodechecksthenodelisttobesurethat thelastnodeisalreadyanodein itszonewithahightrust level.Then,thereceivednodeperforms hashing onthe packetandcomparestheresultwiththe digestvalueto verify theintegrityofthepacket.Oncethepacketis accepted,thenodemodifiestherequestby appendingits ownaddress,A,tothenodelistandreplacing thedigest fieldwithH [A,digest],whichisthe hashvalue,thenthe nodeborder-caststhepacket.

When thedestinationnodereceivestheroute request,it checks theauthenticityofthe RREQbyverifyingthe signature using the privatekey of the source. The integrityofthepacketisverifiedby determiningthatthe digestisequalto:$H[n_n,H[n_{n-1},H[n_{n-2},\ldots H[n_1,$ signature]], wherenisthenumberofnodesin thenode, $n_i$isthenode addressatpositioniinthelist.If the destinationverifies thattherequestisvalid,itreturnsaroutereply packetto the sender; this packethas the same format of routerequestpacketexceptthe packettype field.Allfieldsare settothe correspondingvaluesinthe samemanneras describedinthe route requestphase.Thispacketisthen returnedtothesourcealong thesourcerouteobtained by reversing thesequenceofnodeliststoredinrouterequest packet.Here,thereisnoneedtoperform hashingatan intermediatenodebecauseitonlyunicaststhepacketto thenexthopaslistedinthenodelist.Whenthe source receivestheroutereplay,itverifiestheauthenticity and integrity of the packet since no changes are added through transmission. Ifallthe verifications areok, it acceptsthepacket,otherwiseitrejectsit.

E. DETECTING MALICIOUS NODES

Misbehaving nodescanaffectnetworkthroughput adverselyinworst-casescenarios.Mostexisting ad-hoc routingprotocols donot includeany mechanism to identifymisbehaving nodes.Itisnecessarytoclearly definemisbehaving nodesinordertopreventfalse positives.Itmay bepossiblethatanodeappearstobe misbehavingwhenitisactuallyencounteringatemporary problem suchasoverloadorlowbattery.Someworkhas beendonetosecuread-hocnetworksby usingonly misbehaviourdetection schemes. In thiskind of approaches,itistoohardto guaranteetheintegrityand authenticationoftherouting messages.Therefore,secure routing protocolsshouldprovidetheintegrityand authenticitytotheroutingmessagesbeforebeing ableto identifymisbehavingnodesandisolatethemduringroute discoveryorupdatesoperations.

In ourdesign,weproposeanewtechniquetodealwith malicious nodes, and prevent them from further destroying thenetwork.Thistechniqueisbasedonthe availableinformationproducedby verificationprocesses performedduring transferringroutingpackets.Itrequires thateachnodemaintainsan additionalfield, trustlevel,to itsneighbourstable;thisfieldisdynamically updatedwith thetrustvalueofthecorrespondingnode.Thetrustlevel isinitializedwith value3toindicatethatanodeisa trustedone. This levelisdecrementedin threecases:

ThenodeinitiatesaHELLOmessage with wrong evidenceor doesnotpasssecureneighbourdiscovery protocol,the packet sent by thecorrespondingnode is dropped dueto securityverificationfailures.

The algorithm for detecting malicious node is as follows

Input: node ID.
{
}
Trust-level(ID)+=1
If (Trust-level(ID)=3)
Generate Alarm packet P
Signature<–
Append Signature to P.
Broadcast P
Add node ID to black-list
Return 0
End If

}

Thenodeprovidesalistwithanon-neighbournode.Inall,casesthevalueisdecrementedby one.Thenode isconsideredasamaliciousnodeifthetrustlevelvaluereacheszero.Themaliciousnode istransferredto malicioustable,andanew authenticatedpacket,"Alarm Packet",isgeneratedthatcontainsthepackettype, the addressofthemaliciousnode,andthesignatureofboth.

Thepacketistransmittedinthe samemannerasIARP packetasdescribedbefore.Eachnode thatreceivesthe alarmpacket reassignsthetrustlevelofthemalicious nodestoredinthepackettozeroafterverifying the authenticity.Infuture,eachnodedoesnotperformanyprocessing on thereceived packets until verifying the trustlevelofthesender.

III. SIMULATION AND RESULTS

A. Simulation Environment

To evaluate our SZRP in a non-adversarial environment, we have used the Network Simulator 2 (NS-2) [18].NS-2isa discreteeventsimulatorwrittenin C++andOTcl.Itwasdevelopedby theUniversityof Californiaat Berkeley forsimulating thebehaviourof networkandtransportlayerprotocolsina complex networktopology.Ithasbeenusedextensively in evaluatingtheperformanceofad-hocroutingprotocols. It realistically models arbitrarynode mobilityas well as physicalradiopropagationeffectssuch assignalstrength, interference, capture effect, and wireless propagation delay. At thelinklayer, thesimulator implementsthe completeIEEE802.11 standardMedium AccessControl (MAC)protocol.WemodelledourSZRPbymodifying theexistingZRPin severalways:

We increasedthe packetsizetoreflectthe additional fieldsnecessary toperformsecuritymechanisms.The extendedfieldsholdthepublickey,thedigest,the unique identifier,andthe signature.One shouldnote thatnotall packetsholdthese fields.

Weincreasedthesizeoftheneighbourtableofeach nodebytwofields;thefirst fieldisusedtostorethe publickeyofitsneighboursineachentry,whiletheother isused toindicate thetrustlevelfactor ofthatneighbour.

Wecreatedanewpacketcalled"Alarm Packet"that is generatedandbroadcastedto declaremaliciousnodes when thetrustedlevelvalue reacheszero.

The parameters to study the performance of SZRP is as follows

Number of nodes	22
Simulator	Ns-2
Protocol	AODV
Simulation time	120 sec
Zone radius	2 hops
Transmission Range	200m
Type of traffic	UDP
Hash Length	160 bits
Signature length	160 bits
Public key length	160 bits

B. Performance Metrics

Weevaluate ourproposedprotocolbycomparing itwiththecurrentversionofZRP[23].Bothprotocolsrun on identical movements and communication scenarios; theprimary metrics used for evaluatingthe performanceof SZRParepacketdelivery ratio,routing overheadinbytes,routing overheadinpackets,andend- to-end latency. These metrics are obtained from enhancingthetrace files.

Packetdelivery ratio:Thisisthefractionof thedata packetsgeneratedbytheCBRsourcestothosedelivered to the destination. Thisevaluates the ability of the protocoltodiscover routes.

Routing overhead (bytes): This is the ratio of overheadbytestothe delivereddatabytes.The transmissionateachhop alongthe routeiscountedasone transmissioninthecalculationofthismetric.The routing overheadofasimulationruniscalculatedasthenumber ofroutingbytesgeneratedby theroutingagentofallthe nodesinthesimulationrun.Thismetrichasahighvalue insecureprotocolsduetothehash valueorsignature stored in thepacket.

Routing overhead (packets): This is the ratio of controlpacketoverhead to datapacketoverheadoverall hops.Itdiffersfromtheroutingoverheadinbytessince inMANETsifthemessagesaretoolarge,theywillbe splitinto severalpackets.Thismetricisalwayshigheven inunsecureroutingprotocolsduetocontrolpacketsuse d todiscoverormaintainroutessuchas IARPandIERP packets.

Average End-to-Endlatency: This isthe average delaybetweenthesendingofdatapacketby theCBR sourceanditsreceiptatthecorresponding CBRreceiver. This includes all the delays caused during routing acquisition,bufferingandprocessing atintermediate nodes.

C. Simulation Results

We simulated our SZRP over fourscenarios to evaluate itthroughdifferentmovementpatterns,network size,transmissionrate,andradiusofthezone.

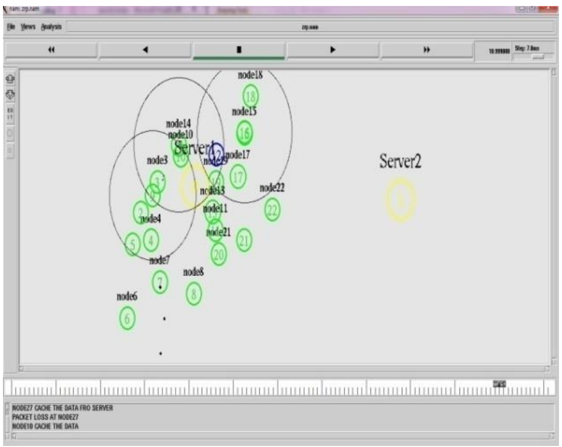

Fig4. Simulation of SZRP using NS-2

Effect of Malicious Nodes Behaviour

The experiments described before compare the performance of SZRP and ZRP when all the nodes in the network are well-behaved. In order to validate ourprotocol against malicious nodes, we conductedadditional experiments to determine the effect ofmalicious nodes behaviour that generate invalid signaturecaused by any type of attacks discussed earlier. We varied the number of malicious nodes from 0 to 5 nodes

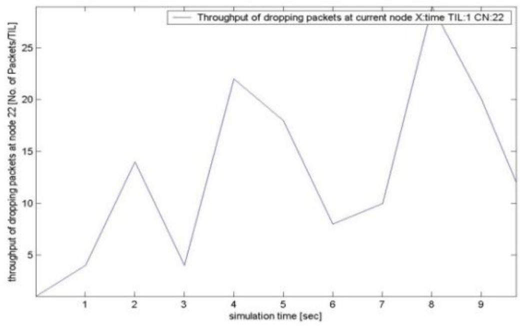

Fig5. Throughput of the dropping packet on using ZRP

On comparing the the throughput of the dropped packet obtained through SZRP and ZRP, it could be found that SZRP has high throughput of dropping packets than ZRP.

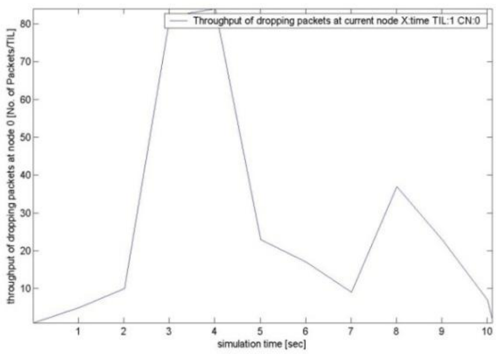

Fig6: Throughput of the dropping node on using SZRP

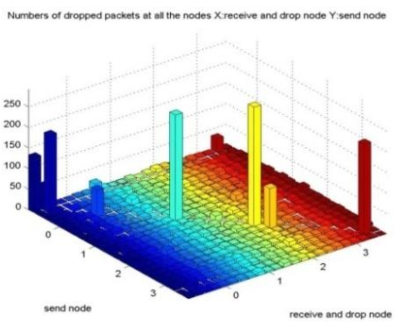

Fig7. 3D representation of Number of dropped packets at all the node on using ZRP

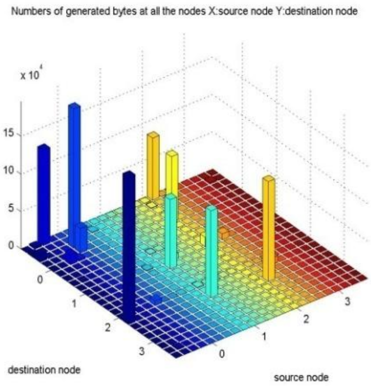

Fig8. Representation of Number of dropped packets at all the node on using SZRP

From comparing the 3D trace graph of number of dropped packets at all the nodes it is found that the packet number of packets dropped on using SZRP is very less on comparing it with ZRP.

IV. CONCLUSION

Thispaper isdedicatedtodemonstratethesecurity of zonerouting protocol;ahybridprotocolthataimsto addresstheproblemsofexcessbandwidthandlong route requestdelayofproactiveandreactiverouting protocols, respectively.Forthispurpose,wecarefully analyzedthe securedprotocolproposed withrespectto reactiveand proactiveroutingprotocols.

Fourmechanismsareproposedinorderto providea comprehensivesecurerouting thatcandefendagainstall vulnerabilitiesinad-hocnetworks.Thefirstmechanism isthe identity-based keymanagement that does not dependonany trustedkey distributioncentreor certificationauthority thatisrarelyfoundinMANETs. Thismechanism providesanidentifierthathasastrong cryptographybindingwiththepublickeyofthenode. Thesecondmechanism providesasecureneighbour discovery toassurethecorrectview ofneighbour information.Itusesa combinationof timeandlocationto verify the discovery of legal nodes and prevent a maliciousnodefromdeludingothernodesthatarewithin its radiotransmission range, and thus preventing most famousattackssuch aswormhole,rushing, andreplays attacks.Thecoreoftheproposedprotocol isrelyingon securingthecontrolpacketsgeneratedtoperform route discovery,routemaintenance,androuting tables'updates that provide through thethirdmechanism to secure routingpackets.Bothdigitalsignatureandone-way hash functionareusedtoachieveour goals.The final mechanism isbasedondetecting amaliciousnodeusing trustlevelvalue,followedby usingalarmmessagesto preventthemfrom furtherdegradingthenetwork performance.

OurfindingsarebasedonthesimulationofSZRP to evaluateitsperformancewithrespecttothe conventional ZRPusing NSsimulatorunderdistinguishablescenarios. Theselection ofparameters and assumptions foreach scenario helps in finding the optimal environment. It shows that SZRPhasaminimaladverseimpacton packet delay and total routing overhead, while the packet deliveryratio achieved is comparable to that ofZRP. Thus,our solutionispredictedtobecomeapplicablefor mostsystemswhilethelackofslow executionwouldnot be anissuebecauseof therapiddevelopmentof processors.The security analysespresentedinthispaper emphasizetheeffectivenessof our securedprotocolto providetherequiredlevelofsecurity byfulfilmentofall security servicesrequiredbyad-hocapplicationssuchas authentication,integrity,and non-repudiation,and preventing allkindsofattacksthreateningad-hoc networks.

V. FUTURE WORKS

An enhancedversionofSZRPwithminorverificationwillbe studiedto avoid newattacks thatmay be performed againstthis versionof SZRP.Inaddition,astudy ofthe effectof alternativedigitalsignaturemechanismssuchas ellipticcurvecanbe carriedouttoreducetheprocessing timerequiredtoperform signingandverification processes.For generation of unique identifier SHA-2 could be used instead of SHA-1 as the encryption hash used in SHA-2 is significantly stronger and not subject to the same vulnerabilities as SHA-1.

REFERENCES

[1] Ibrahim S. I. Abuhaiba, Hanan M. M, Abu- Thuraia “Securing Zone Routing Protocol in Ad-Hoc Networks “ in I. J. Computer Network and Information Security, October 2012.

[2] SushmaKushwaha, Prof. Vijay Lokhande “Security in Wireless Mobile Ad-Hoc Network Nodes Using Novel Intrusion Detection System
in International Journal of Engineering Science and Computing, April 2016.

[3] M. Poturalski, P. Papadimitratos, J. Hubaux, “SecureNeighbour Discovery in Wireless Networks: FormalInvestigation of Possibility,” in Proc. ACMSymposium on Information, Computer &Communication Security ASIACCS’08, Tokyo,Japan, 2008.

[4] M Poturalski, P. Papadimitratos, J. Hubaux, “Secure Neighbour Discovery in Wireless Networks,” In Proceedings of the 2008 ACM symposium on Information, computer and communications security, Tokyo, Japan, 2008.

[5] R.Pickholtz, D.Schilling, L.B. Milstein, "Theory of spread spectrum communications — a tutorial," IEEE Transactions on Communications, v.5, no. 30, pp. 855–884, 1982.

[6] Y.-C. Hu, D.B. Johnson, A. Perrig, "SEAD: Secure Efficient Distance Vector Routing in Mobile Wireless Ad Hoc Networks," Ad Hoc Networks, 2003, v. 1, pp. 175–192.

[7] Hu, Yih-Chun, Adrian Perrig, Dave Johnson, "Rushing Attacks and Defense in Wireless Ad Hoc Network Routing Protocols," In Proc. ACM Workshop on Wireless Security, San Diego, WiSe, California, September 2003.

[8] M. G. Zapata, N. Asokan, "Securing Ad Hoc Routing Protocols," in Proc. ACM Workshop on Wireless Security, Grand Hyatt, WiSe, Singapore, ACM Press, 2002, pp. 1–10.

[9] P. Papadimitratos, Z. J. Haas, "Secure Link State Routing for Mobile Ad Hoc Networks," in Proc. IEEE Workshop on Security and Assurance in Ad Hoc Networks, IEEE Press, 2003, pp. 27–31.

[10] K. Sanzgiri, B. Dahill, B. N. Levine, C. Shields, E. M. Belding- Royer, "A Secure Routing Protocol for Ad hoc Networks," in Proc. 10th Ann. Int'l Conf. Network Protocols, Paris, ICNP, France, Nov., 2002, pp. 78-87.

[11] S. Cheung and K. Levitt, "Protecting routing infrastructures from denial of service using cooperative intrusion detection," In Proceedings of the 1997 New Security Paradigms Workshop (September 1998) pp. 94–106.

[12] Y. -C. Hu, A. Perrig, D. Johnson, "Efficient Security Mechanisms for Routing Protocols," in Proc. Network and Distributed System Security Symp., California, NDPSS, Feb. 2003, pp. 57-73.

[13] Y. -C. Hu, A. Perrig, D.B. Johnson, "Packet Leashes: A Defense against Wormhole Attacks in Wireless Ad Hoc Networks," in Proc. 22nd Ann. Joint Conf. IEEE Computer and communications Societies (INFOCOM 2003), San Francisco, IEEE Press, 2003, pp. 1976–1986.

[14] G. Montenegro, C. Castelluccia, "StatisticallyUnique and Cryptographically Verifiable (SUCV) Identifiers and Addresses," presented at Network and Distributed System Security Symposium, NDPSS'02, San Diego, California, February 2002.

[15] M. G. Zapata, "Secure Ad hoc On-Demand Distance Vector (SAODV) Routing," IETF Internet Draft, August 2001, available at: http://www.potaroo.net/ietf/idref/draftguerreroMANETs-saodv/

[16] J. Schaumann, (2002),"Analysis of the Zone Routing Protocol," available at: http://www.netmeister.org/misc/zrp/zrp.htm

[17] B. Forouzan, "Introduction to cryptography and network security," McGraw-Hill, 1st ed.,2006.

[18] K. Fall, K. Varadhan, "Editors ns Notes and Documentation," The VINT Project, UC Berkeley, LBL, USC/ISI, and Xerox PARC, November 1997. Available at: http://www-mash.cs.berkeley.edu/ns

[19] Yih-Chun Hu, Adrian Perrig, David B. Johnson, "Ariadne: A Secure On-Demand Routing Protocol for Wireless Ad Hoc Networks," Wireless Networks, 2005, v. 11, pp. 21–38.

[20] B. Smith, "Securing Distance-Vector Routing Protocols," M.S. thesis, university of California, California, 1997.

[21] Sh. Rahmatizadeh, H. Shah-Hosseiniand, H.Torkaman, "The Ant-Bee Routing Algorithm: A New Agent Based Nature-Inspired Routing Algorithm," Journal of Applied Sciences, 2009, Volume 9, Issue 5, pp. 983–987.

[22] A.M.Kamal,"AdaptiveSecureRouting inAdHoc Mobile Network," M.S.Thesis,Dept.Computer and SystemsScience,RoyalInstituteof Technology, Stockholm,Sweden,2004.

[23] Z.J.Haas,M.R.Pearlman,P.Samer,"TheRouting Protocol(ZRP)forAdHocNetworks," InternetDraft,2003, availableat: http://tools.ietf.org/id/draft-ietf-MANETs-zone-zrp-04.txt.