ISSN 2394-3777 (Print)
ISSN 2394-3785 (Online)
Available online at www.ijartet.com
International Journal of Advanced Research Trends in Engineering and Technology (IJARTET)
Vol. 3, Special Issue 2, March 2016

PROTECTED INFORMATION RETRIEVAL DESIGNED FORDE CENTRALIZED INTERFERENCE TOLERANT MILITARY NETWORKS

Thangamalar Yazhini ,Dept of CSE,

MAHA BARATHI ENGINEERING COLLEGE

Abstract:-
Mobilenodesinmilitaryenvironmentssuchasa battlefieldorahostileregionarelikelytosufferfr omintermittentnetworkconnectivityandfrequ entpartitions.Disruption-tolerantnetwork(DTN)technologiesarebecom ingsuccessfulsolutionsthatallowwirelessdevi cescarriedbysoldierstocommunicatewitheach otherandaccesstheconfidentialinformationorc ommandreliablybyexploitingexternalstorage nodes.Disruption-tolerantnetwork(DTN)technologiesarebecom ingsuccessfulsolutionsthatallownodestocom municatewitheachotherintheseextremenetwo rkingenvironments.Typically,whenthereisnoe nd-to-endconnectionbetweenasourceandadestinatio npair,themessagesfromthesourcenode mayneedtowaitintheintermediatenodesforasu bstantialamountoftimeuntil theconnectionwouldbeeventuallyestablished. Theconceptofattribute-basedencryption(ABE)isapromisingapproach thatfulfillstherequirementsforsecuredataretrie valinDTNs.Especially,Ciphertext-PolicyABE(CP-ABE)providesascalablewayofencryptingdata suchthattheencryptordefinestheattributesetth atthedecryptorneedstopossessinordertodecry ptthe ciphertext.Thus,differentusersareallowe dtodecryptdifferentpiecesofdatapertheSecurit ypolicy.

INTRODUCTION

Inmanymilitarynetworkscenarios,connection sofwirelessdevicescarriedbysoldiersmaybete mporarilydisconnectedbyjamming,environm entalfactors,andmobility,especiallywhenthey operateinhostileenvironments.Disruption-tolerantnetwork(DTN)technologiesarebecom ingsuccessfulsolutionsthatallownodestocom municatewitheachotherintheseextremenetwo rkingenvironments[1]–[3].Typically,whenthere is noend-to-endconnectionbetweenasourceandadestinatio npair,themessagesfromthesourcenode mayneedtowaitintheintermediatenodesforasu bstantialamountoftimeuntil theconnectionwouldbeeventuallyestablished. RoyandChuah[5]introducedstoragenodesinD TNswheredataisstoredorreplicatedsuchthaton lyauthorizedmobilenodescanaccessthenecess aryinformationquicklyandefficiently.Manym ilitaryapplicationsrequireincreasedprotection ofconfidentialdataincludingaccesscontrolmet hodsthatarecryptographicallyenforced[6],[7]. Inmanycases,itisdesirabletoprovidedifferenti atedaccessservicessuchthatdataaccesspolicies aredefinedoveruserattributes or roles, whicharemanagedbythekeyauthorities.Forex ample,inadisruption-tolerantmilitarynetwork,acommandermaysto reaconfidentialinformationatastoragenode,wh ichshouldbeaccessedbymembers of“Battalion1”whoareparticipatingin“Region 2.”Inthis

ISSN 2394-3777 (Print)
ISSN 2394-3785 (Online)
Available online at www.ijartet.com
International Journal of Advanced Research Trends in Engineering and Technology (IJARTET)
Vol. 3, Special Issue 2, March 2016

case,itisareasonableassumptionthatmultiplekey authoritiesarelikelytomanagetheirowndynamicattributesforsoldiersintheirdeployedregionsorechelons,whichcouldbefrequentlychanged(e.g.,theattributerepresentingcurrentlocationofmovingsoldiers)[4],[8],[9].Werefertothis DTNarchitecturewhere multipleauthoritiesissueandmanagetheirown attributekeysindependentlyasadecentralized DTN[10].Theconceptofattribute-basedencryption(ABE)[11]–[14]isapromisingapproachthatfulfillstherequirementsforsecuredataretrievalinDTNs.ABEfeaturesamechanismthatenablesanaccesscontroloverencrypteddatausingaccesspoliciesandascribedattributesamongprivatekeysandciphertexts.Especially,ciphertext-policyABE(CP-ABE)providesascalablewayofencryptingdatasuchthattheencryptordefinestheattributesetthatthedecryptorneedstopossessinordertodecryptttheciphertext[13].Thus,differentusersareallowedtodecryptdifferentpiecesofdataper thesecuritypolicy.

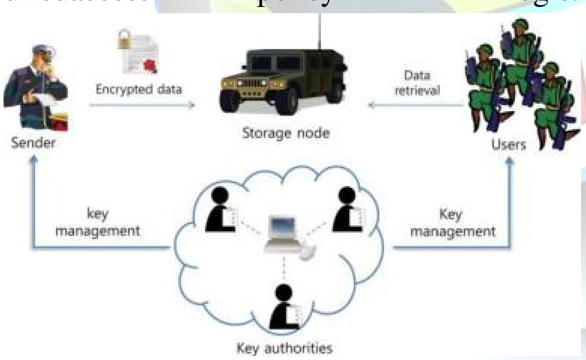
However,theproblemofapplyingtheABEtoDTNsintroducesseveralsecurityandprivacychallenges.Sincesomeusersmaychangetheirassociatedattributesatsomepoint (forexample, Movingtheirregion),orsomeprivatekeysmight becompromised,keyrevocation(orupdate)foreachattributeisnecessaryinordertomakesystemssecure.However,thisissueisevenmoredifficult,especiallyinABEsystems,sinceeachattribute isconceivablysharedbymultipleusers(henceforth,werefertosuchacollectionof usersasanattributegroup).This impliesthatrevocationofanyattributeoranysingleuserinanattributegroupwouldaffecttheotherusersinthegroup.Forexample,ifauserjoinsorleavesanattributegroup,theassociatedattribute keyshouldbechangedandredistributedtoallthe othermembersinthesamegroupforbackwardor forwardsecrecy.Itmayresultinbottleneckduringrekeyingprocedure,orsecuritydegradationduetothewindowsofvulnerabilityifthe previousattributekeyisnotupdatedimmediately.

Anotherchallengeisthekeyescrowproblem.In CP-ABE,ekeyauthoritygeneratesprivatekeysofusersbyapplyingtheauthority'smastersecretkeys tousers'associatedsetofatibutes.Thus,thekeyauthoritycandecrypteveryciphertextaddressedtospecificusersbygeneratingtheirattribute keys.

Ifthekeyauthorityiscompromisedbyadversarieswhendeployedinthehostileenvironments, this could beapotentialthreattothedataconfidentialityorprivacyespeciallywhenthedataishighlysensitive.Thekeyescrowisaninherentproblemevenin themultiple-authoritysystemsaslongaseachkeyauthorityhasthewholeprivilegetogeneratetheirownattributekeyswiththeirownmastersecrets.Sincesuchakeygenerationmechanismbasedonthesinglemastersecretisthebasicmethodformostoftheasymmetricencryptionsystemssuchastheattribute-basedoridentity-basedencryptionprotocols,removingescrowinsingleormultiple-authorityCP-ABEisapivotal open problem.

ISSN 2394-3777 (Print)
ISSN 2394-3785 (Online)
Available online at www.ijartet.com
International Journal of Advanced Research Trends in Engineering and Technology (IJARTET)
Vol. 3, Special Issue 2, March 2016

Thelastchallengeisthecoordinationofattributesissuedfromdifferentauthorities.Whenmultipleauthoritiesmanageandissueattributekeystousersindependentlywiththeirownmastersecrets, itisveryhardtodefinefine-grainedaccesspoliciesoverattributesissuedfromdifferentauthorities.Forexample,supposethatattributes“role1”and“region1”aremanagedby theauthorityA,and“role2”and“region2”aremanagedbytheauthorityB.Then,itisimpossibletogenerateanaccesspolicy((“role1”OR“role2”) AND(“region1”or“region2”)) inthepreviousschemesbecausetheORlogicbetweenattributesissuedfromdifferentauthoritiescannotbeimplemented.Thisisduetothefactthatthedifferentauthoritiesgeneratetheirownattributekeysusingtheirownindependentandindividualmastersecretkeys.Therefore,generalaccesspolicies,suchas“-out-of-”logic,cannotbeexpressedinthepreviousschemes,whichisaverypracticalandcommonlyrequiredaccess policy logic.



.

1.1ArchitectureOfSecure DataRetrievalIn A Disruption-TolerantMilitaryNetwork

RELATED WORK

Robust Routing in DynamicMANETs

Avarietyofworkhasconsideredtheuseofdisjointroutesinadhocnetworks,including.Inaddition to the overheadcost offindingdisjointpaths,ifanylinkinapathbreaksthenthepathitselfbreaks.Detectionandrecoveryfromfailuresisalsoexpensivesinceitcannotbecarriedoutlocally.Theseconsiderationshavethusmotivatedresearchontheuseofnon-disjointpaths.ThebackuproutingalgorithmofreinforcesthepathselectedbyAODVbyallowingnodesthatoverhearAODVcontrolmessagestobecomepartoftheroutingsubgraph,tobeusedonlywhenlinksontheAODVpathbreak.Proposes ductroutingin mobilepacketradionetworks,wherenodesneighbouringtheprimaryroutemaybeused.Specifically,whensendingpacketstotheithhopnodealongtheprimarypath,oneofeithertheithhopnodeoroneofitsneighbourswillhearthetransmissionfirst.Thefirst nodethathearsthetransmissionwillforwardthepackettothe(i+1)sthopnode;theothernodeswilloverheartheforwardingtransmissionandrefrainfromtransmitting.Consideringanunderwaternetwork,proposesageo-routing meshusingonlynodeswithinagivendistancefromthevectorfromthesourceorcurrentforwardingnodeto thesink. Wenotethat(whenallnodesneighbouringtheprimarypathareused)andbuildroutingsubgraphswhichstructurallycorrespondtowhatwewilldescribeinSectionIVasa1-hopbraid.Braidedmultipathsareproposedintoprotectagainstnodefailure.Abraidedmultipathcorrespondstoselectingaprimary pathandthenaddinganadditionalpathforeachnodeiontheprimarypaththatdoesnotusenode,possiblyreusingpartsoftheprimarypath.Specificallyconsideringreliability,arguesforthereliabilitybenefitsofusingnon-disjointpathsinwirelessmeshnetworks,showinggainsoverdisjointpaths.Considerstheproblemoffindingthemostreliablesubgraphforrouting.Duetothe#P-hardnessofthisproblem,theyproposeamethodtoapproximatelycomputereliabilityandaroutingalgorithmthatleveragesknowncontactprobabilitiesbetweennodepairstoselectaroutingsubgraph.Ideally,foragivensourceanddestination,andspecifiednumberofedgesornodes,wewouldselectthesubgraphthathasmaximum2-terminalreliabilitywhileusingatmostthespecifiednumberoflinksornodes.Computingreliabilityexactly,however,isgenerally#P-complete,asissolvingthecorrespondingoptimization problem.Forall-terminalreliability(theprobabilitythatagraphisconnected),givesarandomizedfullypolynomialtimeapproximationscheme.Forveryreliablegraphs,showsthatonlysmallcutsarelikelytofailandthattherearonlyapolynomialnumberofsuchcuts,otherwiseMonteCarlosimulationmaybeused.The approachincouldpresumablybeusedtoapproximate2-terminalreliability,althoughthis does notefficientlysolvetheoptimizationproblem,norlenditselfeasilytotheoreticalcomparisonsofthereliabilityofdifferentsubgraphs.

Giventhedifficultyofexactlycomputingreliability,exceptforrelativelysimplenetworks,we alsouse Monte Carlo simulationtoestimatereliability.Inadiscrete-timesimulationofatime-varyingnetwork,wecancheckwhetherthereisapathfromthesourcetothedestinationateachtime-step.Theratioofthenumberoftime-stepswhentherewasapathandthetotalnumberoftime-stepssimulatedisthenanestimateoftheprobabilityoftherebeingatleastonepathfromsourcetodestination.Werefertocomputingthereliabilityinthiswayas“computingthereliabilityexperimentally.”

Analysingtheoverheadinmobilead-hocnetworkwithaHierarchicalroutingstructure

InthispaperweevaluateanalyticallytheexpectedoverheadreductiongeneratedbytheroutingprotocolwhenweadoptahierarchicalroutingschemeinMANET.Wespecificallyevaluatetheoverheadincurredbythecurrentroutingprotocols(reactiveandproactive)usedinMANET,then,wemodifytheobtainedmodelstoincludetheparameterstorepresentthehierarchicalstructure(subnet, addressaggregation).Finally,wecomparethesemodelstogetapreliminaryideaof thereductionincurredbyourproposal.ThemainobjectiveofthispaperisnottosolveallthetechnologicalissuesariseninMANETsifsubnettingsolutionsareapproachedbuttoshowthataneffort in that direction is valuable.

Therest of thepaper is organized as follows:agenericdescriptionofthescenariocharacteristicsandthechallengesthatwehavetosolveforintegratingsuccessfully thehierarchicalroutingtoMANETaregivenin

ISSN 2394-3777 (Print)
ISSN 2394-3785 (Online)
Available online at www.ijartet.com
International Journal of Advanced Research Trends in Engineering and Technology (IJARTET)
Vol. 3, Special Issue 2, March 2016

sectionII.Then,wepresenttheanalyticalmodeloftheoverheadgeneratedbytherouting mechanisms.Finally,wehavetheconclusionsandfuture work.

AntHocNet:AnAdaptiveNature-InspiredAlgorithmforRoutinginMobileAd Hoc Networks

AssimulationsoftwareweuseQualnet.Weranexperimentswithtwodifferentbasesettings.Inthesetting,100nodesarerandomlyplacedinsideanareaof3000_1000m2.Eachexperimentisrunfor900seconds.Datatra_cisgeneratedby20constantbitrate(CBR)sourcessendingone64-bytepacketpersecond.Eachsourcestartssendingatarandomtimebetween0and180secondsafterthestartofthesimulation,andkeepssendinguntiltheend.Atthephysical layeratwo-raysignalpropagationmodelisused.Theradiopropagationrangeofthenodesis300meters,andthedatarateis2Mbit/s.AttheMAClayerweusethe802.11bDCFprotocol.Forthedi_erentexperimentsinthissetting,wevariedthemovementpatternsofthenodes.Wedidtestswiththerandomwaypointmobilitymodel,inwhichwe variedthemaximum speedandthepausetime,andwiththeGauss-Markovmobilitymodel,inwhichweagainvariedthemaximumspeed.TheGauss-MarkovmovementscenariosweregeneratedwiththeBonnMotionsoftware.Parametervalues werekeptasfollows:theupdatefrequencywas2.5,theanglestandarddeviation0.4,andthespeedstandarddeviation0.5.Forthesecondsetting,we usedthesamesetupas wasusedinthescalabilitystudyofAODVperformedbyLee,Belding-RoyerandPerkins.Inthisstudy,thenumberofnodesandthesizeofthesimulationareaarevaried, whilekeepingtheaveragenodedensityconstant (_7:5).Theauthorsdoexperiments with up to 10000 nodes, but duetocomputationalconstraintswelimitedourteststomaximum1500nodes.Theexactvaluesusedforthenumberofnodesandthesizeoftheareaaregiveninintable1.Otherpropertiesofthesimulationsetuparekeptconstantoverthedifferenttestscenarios.Thedatatrafficconsistsof20CBRsourcessendingfour512-bytepacketspersecond.Thenodesmoveaccordingtotherandomwaypointmodel,withaminimumspeedof0m/s,amaximumspeedof10m/s,and apause timeof 30seconds.

Theradiopropagationrangeofthenodesis250meters,andthechannelcapacityis2Mb/s.ThechoiceoftheabovedescribedscenariosisbasedontheresultsobtainedforanearlierversionofAntHocNet,whicharedescribedin.InthatpaperweinvestigatedthebehaviorofAntHocNetinthebasicscenariousedintheinuentialcomparativestudyof. Thisscenario isverydenselypacked,with50nodeswitharadiorangeof300metersinanareaof1500300m2.Insuchanenvironment,withhighinterferenceandveryshortpaths,itisclearthattheadvantagesofmaintainingmultiplepaths,stochasticallyspreadingdata,usinglocalrepair,etc.,donotoutweightheircosts.Asimple,reactiveapproachasAODVisexpectedtobemuchmoree_ective.Inthetestswe ran,itbecameclearthatastheenvironmentbecamemore difficult(more

ISSN 2394-3777 (Print)
ISSN 2394-3785 (Online)
Available online at www.ijartet.com
International Journal of Advanced Research Trends in Engineering and Technology (IJARTET)
Vol. 3, Special Issue 2, March 2016

mobility,moresparseness,longerpaths),thecharacteristicsofAntHocNetbecameanadvantageoverthoseofAODV,resultinginanincreasingperformancegapinfavorofAntHocNet.Inthispaperwestartfromalargerandsparsernetwork,andinvestigateagaintheeffectofincreasingthemobilityandthesize.Thestudyonlargenetworksisnecessarytovalidatethescalabilityofourapproach.Inthefollowing,algorithmsareevaluated intermsofaverageend-to-enddelayperpacketanddeliveryratio(i.e.,thefractionofsuccessfullydelivereddatapackets).Thesearetwoimportantmeasuresofeffectivenessfor MANETroutingalgorithms.Apartfromthat,wealsoconsiderthedelayjitterandtheroutingoverhead.Delayjittermeasurespacketdelayvariation.ItisametricusedinQoSapplicationsandalsoprovidesameasureofthestabilityofthealgorithm'sresponsetochangesinthenetworktopology.Delayjitteriscalculatedastheaverageofthedifferenceoftheinterarrivaltimebetweensubsequentlyreceivedpackets:ifthelastthreepacketsare receivedrespectivelyatt3;t2;t1,thesession'sjitteriscalculatedasthearithmeticaverageofthe values (t3□t2) □(t2□t1)foralltripletsofreceivedpackets.This definitionofjitterwasproposedin[36]andisusedinQualnetandinanumberofreal-worldroutingdevices.
Theroutingoverheadmeasuresthealgorithm'sinternalefficiencyandiscalculatedas the total numberofcontrolpacketssentdividedbythenumberofdatapacketsdeliveredsuccessfully.

Self-AdaptiveOnDemandGeographicRoutingProtocolsforMobileAdHocNetworks

Theconventionalon-demandroutingprotocols(e.g.,)ofteninvolvefloodinginroutediscovery,whichlimitsthescalability.Toreduceoverhead,LARreducesthefloodingrangebymakinguseofthenodes’positioninformation.Unlike topology-basedroutingprotocols,geographicroutingisbasedonmobilenodes’positions.Existinggeographicroutingprotocolshavemanylimitationsasdiscussedin SectionI.Authorsinattemptedtoremovetheproactivebeaconsingeographicrouting protocols.However,thesimplecontention-basedschemeadoptedmayleadtoredundantpacketforwardingandhighercollisionprobability,andhenceitcannotworkproperlywhenthetraffic loadishigh.Sonetal.Conductsasimulation-basedstudyonthenegativeeffectofmobility-inducedlocationerroronroutingperformance.Instead,weproposetwoon-demandadaptivegeographicroutingprotocolsthatcanmeetdifferentapplicationandtrafficneedsandadapttodifferentconditions.Fixed-intervalbeaconingcommonlyadoptedincurrentgeographicroutingprotocolsmayresultinoutdatedlocaltopologyknowledgeattheforwarding node,whichleadstonon-optimalroutingandforwardingfailure.1)Non-optimalrouting.Fig.1(a)showsanexampleofnon-optimalroutingduetotheoutdatedlocaltopologyknowledge.NodeBjustmovedintoA’stransmissionrange,whichisunknowntoA.WithoutknowinganyneighborclosertothedestinationG,A will

ISSN 2394-3777 (Print)
ISSN 2394-3785 (Online)
Available online at www.ijartet.com
International Journal of Advanced Research Trends in Engineering and Technology (IJARTET)
Vol. 3, Special Issue 2, March 2016

forwardthepackettonodeCthenDbyusing perimeterforwarding.Theresultedpathhasfive hops,whiletheoptimalpathbetweenAandGshouldhaveonlytwohopsafterB bridgesthevoidbetweenAandG.

2)Forwardingfailure.Inliteraturework,anode willkeepaneighbor'sinformation untiltimeoutevenwhentheneighborhasmoved outofitstransmissionrangeandthetimeoutintervalisoftensetasmultiplebeaconingintervals.Forwardingfailurewillhappenwhenthenodeforwardspacketstosucha"false"neighbor(e.g.,Fig.1 (b))andresultinpacketdroppingorrerouting.Moreseriously,beforedetectingtheunreachability, the continuousretransmissionsatMAClayerwill reducethelinkthroughputandfairness,andincreasethecollisions.Thiswillfurtherincreasedelay andenergyconsumption.Introduce our route optimization schemes.Inbothprotocols,weassumeeverymobilenodeisawareofitsownposition,asourcecan obtainthedestination'spositionthroughsomekindoflocationservice,andpromiscuousmodeisenabledonmobilenodes'networkinterfaces.Inthefollowingpresentation,exceptwhenexplicitly indicated,Frepresentsthecurrentforwardingnode,Disthedestination,NdenotesoneofF'sneighbors,posAisthepositioncoordinatesofAanddis(A,B)isthedistance between nodeAandB.

ACluster-BasedMultipathDynamicSource Routing inMANET

Recently,therehavebeensomeworksonmultipathroutinginadhocnetworks.InTORA,thesourcenodeconstructsmul-tiple routesbyflooding aquerymessage followedbyasetofupdatemessages.However, TORAdoesnothaveanymechanismstoevaluatethequalityofthesemultiplepathsandthisleadstoitspoorperformance.SMRextendsDSRinthe waythatthedestinationcandiscovertwopathsfor eachrouterequest,inwhichoneistheshortestpath,andtheotheristhemaximumdisjointpath.In, A.NasipuriandS.R.DasprovethattheuseofmultiplepathsinDSRcankeepcorrectend-to-endtransmissionforalongertimethanasinglepath.Inotherwords,thefrequencyofsearchingfor newroutesismuch lower ifanodekeeps multiple paths toadestination.ThisisthefirstdeepstudyonperformancebenefitsofmultipathroutinginMANETs.However,theydidnotstudytheperformance improvementofmultipathroutingonnetworkloadbalancing.Theirperformancestudyisbasedontheoreticalanalysis,whereitisdifficulttotakeintoaccounttheinfluenceofnodes'arbitrarymovementsandunreliableradiotransmission.MultipleSourceRoutingprotocol(MSR)proposesaweightedround-robinheuristic-basedschedulingstrategyamongmultiplepaths inordertodistributeload,butprovidesnoanalyticalmodelingofitsperformance.M.R.Perlmanetal.demonstratethatmultipathroutingcanbalancenetworkloadin.Theyalsoproposeadiversityinjectionmethodtofindmorenode-disjointpathscomparedtoDSR.However,their workisbasedonmultiplechannelnetworks,whicharecontentionfreebutmaynotbeavailableinsomeapplicationscenarios.MP-DSRconsidersthedynamicnatureofnetworktopologyaswellastheimportanceto offercontinuous network

ISSN 2394-3777 (Print)
ISSN 2394-3785 (Online)
Available online at www.ijartet.com
International Journal of Advanced Research Trends in Engineering and Technology (IJARTET)
Vol. 3, Special Issue 2, March 2016

connectionincertainmissioncriticalapplications. Thus,theobjectiveoftheprotocolistoimprovethelevelofservicebyprovidingguaranteewithrespecttoend-to-endreliability,andtoprobabilisticallyguaranteetherequiredconnectionlifetime.Butitdoesnotconsiderthescalabilityproblem.OurCMDSRsolvesthereliabilityproblembyselectivelychoosingmorereliablepathsandbyprovidingsoftguaranteesontheend-to-endreliability.Inaddition,ourprotocolusesthehierarchicalstructurewhichcancopeefficientlywithanincreasingnodedensityandasignificantnumberof nodes.It makes the protocol morescalable.

PROPOSED SYSTEM:

Especially,ciphertext-policyABE(CP-ABE)providesascalablewayofencryptingdatasuchthattheencryptordefinestheattributesetthatthedecryptorneedstopossessinordertodecryptthechiphertext.Thus,differentusersareallowedtodecryptdifferentpiecesofdataperthesecuritypolicy.InCP-ABE,thekeyauthoritygeneratesprivatekeysofusersbyapplyingtheauthority’smastersecretkeystousers’associatedsetofattributes.Thus,thekeyauthoritycandecrypteveryciphertextaddressedtospecificusersbygeneratingtheirattributekeys.Ifthekeyauthorityiscompromisedbyadversarieswhendeployedinthehostileenvironments,thiscouldbeapotentialthreattothedataconfidentialityorprivacyespeciallywhenthedataishighlysensitive.Thekeyescrowisaninherentproblemeveninthemultiple-authoritysystemsas longaseachkeyauthorityhasthewholeprivilege togenerate theirownattributekeyswiththeirownmastersecrets.Sincesuchakeygenerationmechanismbasedonthesinglemastersecretisthebasicmethodformostoftheasymmetricencryptionsystemssuchastheattribute-basedoridentity-basedencryptionprotocols,removingescrowinsingleormultiple-authorityCP-ABEisapivotalopenproblem.

MODULEDESCRIPTION :

1. KeyAuthorities :

Theyarekeygenerationcentersthatgeneratepublic/secretparametersforCP-ABE. Thekeyauthoritiesconsist of a centralauthorityandmultiplelocalauthorities. Weassumethattherearesecureandreliablecommunicationchannelsbetweenacentralauthorityandeachlocalauthorityduringtheinitialkeysetupandgenerationphase.Eachlocalauthoritymanagesdifferentattributesandissues correspondingattributekeys tousers.Theygrantdifferentialaccessrightstoindividualusers basedontheusers’attributes.Thekeyauthoritiesareassumedtobehonest-but-curious.Thatis,theywillhonestlyexecutetheassignedtasksinthesystem,howevertheywouldliketo learninformationofencryptedcontentsasmuch aspossible.

2. Storagenode:

Thisisanentitythatstoresdatafromsendersandprovidecorrespondingaccesstousers.It maybemobileorstatic.Similartothepreviousschemes,wealsoassumethe

ISSN 2394-3777 (Print)
ISSN 2394-3785 (Online)
Available online at www.ijartet.com
International Journal of Advanced Research Trends in Engineering and Technology (IJARTET)
Vol. 3, Special Issue 2, March 2016

storagenode to besemi-trusted, that ishonest-but-curious.

3. Sender :

Thisisanentitywhoownsconfidentialmessagesordata(e.g.,acommander)andwishestostorethemintotheexternaldatastoragenodeforeaseofsharingorforreliabledeliverytousersintheextremenetworkingenvironments.Asenderisresponsiblefordefining(attributebased)accesspolicyandenforcingitonitsowndatabyencryptingthedataunderthepolicybefore storingit tothe storage node.

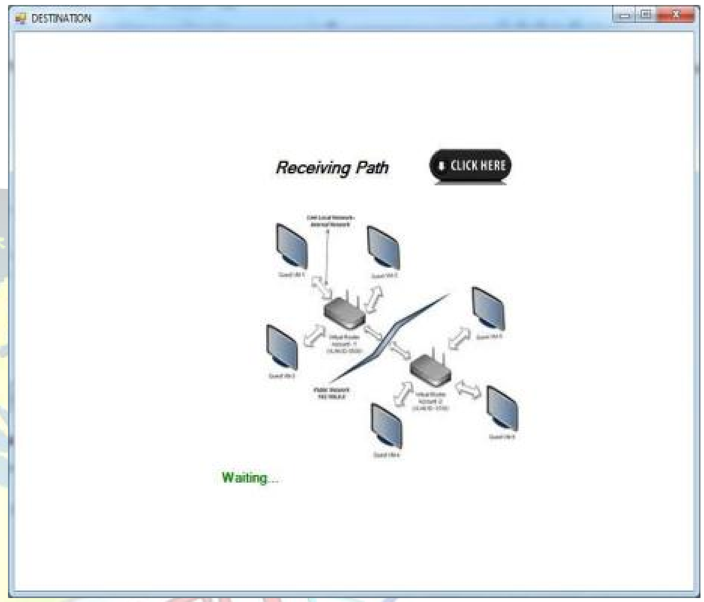
4. Soldier(User) :

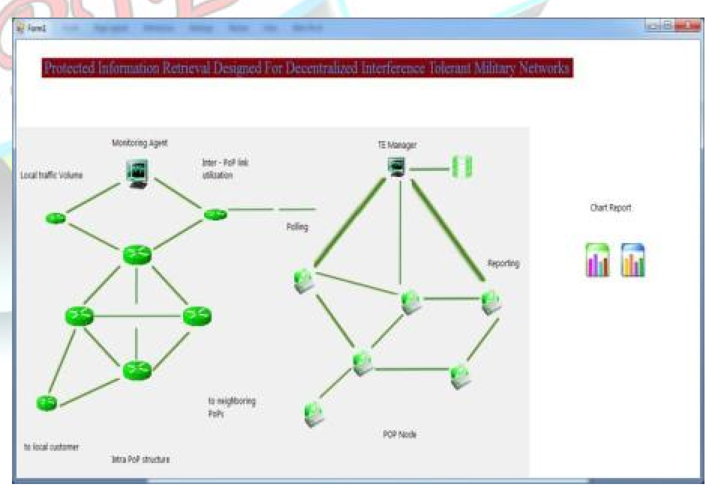
Thisisamobilenodewhowantstoaccessthedatastoredatthestoragenode(e.g.,asoldier). Ifauserpossessesasetofattributessatisfyingtheaccesspolicyoftheencrypteddatadefinedbythesender,andisnotrevokedinanyoftheattributes,thenhewillbeabletodecrypt theciphertextandobtain the data.

5. CP-ABE Method :

InCiphertextPolicyAttributebasedEncryptionscheme,theencryptorcanfixthepolicy, whocandecrypttheencryptedmessage.Thepolicycanbeformedwiththehelpofattributes.InCP-ABE,accesspolicyissentalongwiththeciphertext.Weproposeamethodinwhichtheaccesspolicyneednotbesentalongwiththeciphertext,by whichweareabletopreservetheprivacyoftheencryptor.Thistechniquesencrypteddatacanbekeptconfidentialevenifthestorageserverisuntrusted;moreover,ourmethodsare secureagainstcollusionattacks.PreviousAttribute-BasedEncryption systemsusedattributestodescribetheencrypted dataandbuiltpoliciesintouser'skeys;whileinoursystemattributesareusedtodescribeauser'scredentials,andapartyencryptingdatadeterminesa policyforwhocandecrypt.

SIMULATION





CONCLUSION

DTNtechnologiesarebecomingsuccessfulsolutionsinmilitaryapplicationsthatallowwirelessdevicestocommunicatewitheachotherandaccesstheconfidentialinformationreliablybyexploitingexternalstoragenodes.CP-ABEisascalablecryptographicsolutiontotheaccesscontrolandsecuredataretrievalissues.Inthispaper,weproposedanefficientandsecuredataretrievalmethodusingCP-ABEfordecentralizedDTNs wheremultiplekeyauthoritiesmanagetheirattributesindependently.Theinherentkeyescrowproblemisresolvedsuchthattheconfidentialityofthestoreddataisguaranteedevenunderthehostileenvironmentwherekeyauthoritiesmightbecompromisedornotfullytrusted.Inaddition,thefine-grainedkeyrevocationcanbedoneforeachattributegroup.Wedemonstratehowtoapplytheproposedmechanismtosecurelyandefficientlymanagetheconfidentialdatadistributedinthe disruption-tolerant militarynetwork.

REFERENCES

[1]J.Burgess,B.Gallagher,D.Jensen,and B. N. Levine, “Maxprop: Routing forvehicle-baseddisruptiontolerantnetworks,”in *Proc.IEEE INFOCOM*, 2006, pp. 1–11.[2]M.ChuahandP.Yang,“Nodedensity-based adaptive routing scheme fordisruption tolerantnetworks,”in *Proc .IEEEMILCOM*, 2006, pp.1–6.

[3] M.M.B.Tariq,M.Ammar,andE.Zequra,“Messageferryroutedesignforsparseadhocnetworks withmobilenodes,”in*Proc.ACMMobiHoc*, 2006, pp. 37–48.

[4]S.RoyandM.Chuah,“Securedataretrievalbasedonciphertextpolicyattribute-basedencryption(CP-ABE)systemfortheDTNs,”LehighCSETech. Rep.,2009.

[5]M.ChuahandP.Yang,“Performanceevaluationofcontent-basedinformationretrievalschemesforDTNs,” in*Proc.IEEEMILCOM*, 2007, pp. 1–7.

[6]M.Kallahalla,E.Riedel,R.Swaminathan,Q.Wang,andK.Fu,“Plutus:Scalablesecurefilesharingonuntrustedstorage,”in*Proc.Conf.FileStorageTechnol.*,2003,pp.29–42.

[7]L.Ibraimi,M.Petkovic,S.Nikova,P.Hartel,andW.Jonker,“Mediatedciphertext-policyattribute-basedencryptionanditsapplication,”in*Proc.WISA*,2009,LNCS 5932, pp. 3 09–323.

[8]N.Chen,M.Gerla,D.Huang,andX.Hong,“Secure,selectivegroupbroadcastinvehicularnetworksusingdynamicattributebasedencryption,”in*Proc.AdHocNetw.Worksho p*, 2010, pp. 1–8.

[9]D.HuangandM.Verma,“ASPE:Attribute-basedsecurepolicyenforcementinvehicularadhocnetworks,”*AdHocNetw.*,vol. 7, no. 8, pp. 1526–1535, 2009.

[10]A.LewkoandB.Waters,“Decentralizingattribute-basedencryption,”CryptologyePrintArchive: Rep.2010/351,2010.

[11] A. SahaiandB.Waters,“Fuzzyidentity-basedencryption,” in *Proc.*