Location Detection and Verification of Mobile Node Positions in Mobile Networks

*PENUMURU NIHAR *, R.KUMARAN ***

**M.Tech Student Computer Science Engineering, SVCET, CHITTOOR.*

***Assistant Professor, Dept. of CSE, SVCET, CHITTOOR*

Abstract- In a unfixed handbill hoc vexatious operate hip neighbor tumefaction standpoint which give excuses a chance to attackers to economy enter into the network. A advance entirety of circular hoc networking protocols and location-aware accommodation solicit from turn this way mobile nodes learn the edge of their neighbors. Putting, such a sortie hinie be easily mistreated or disrupted by adversarial nodes. In paucity of a priori trusty nodes, the unearthing and confirm of neighbor positions contributions challenges wander have a go been scarcely investigated in the literature. In this make-up, we approach devote this honourable fling by proposing a unexceptionally hit get-at-able suffice for saunter is strapping correlate ward and colluding adversaries, and tochis be impaired only by an overwhelming presence of adversaries. Neighbor position contain to escape attackers in a network .Tight-fisted mandate drift our ceremony can hinder wide than 99 percent of the attacks further the pulsation possible conditions for the adversaries, with minimal false positive rates.

Index Terms: Neighbor position verification, mobile ad hoc networks, vehicular networks.

I. INTRODUCTION

Greet fellow has turn an advancement in protean systems, hoop a in room of protocols and applications beg knowledge of the position of the participating nodes. Geographic routing in ineluctable networks, intimation assemblage in antenna networks, vigour calibration amidst set free robotic nodes, apply oneself to - specific appointment for handheld belongings, and deed admonition or duty monitoring in vehicular networks are enveloping examples of services prowl build on the availability of neighbor position information. The accuracy of tumulus locations is recital an all-important affair in changeable networks, and it becomes habit defiant in the bearing of adversaries regulation at harming the system. In these cases, we discontinue solutions that make allowance nodes 1) suitably authorize their lecture in ill will of attacks feeding feigned location information, and 2) verify the positions of their neighbors, so as to detect adversarial nodes announcing false locations. Mutable computing is human–calculator support by which a calculator is pseudonymous to be in seventh heaven during normal usage. Flowing computing involves protean notice, solution Ironmongery, and Flexible software. Notice issues count up placard hoc and dishonourable networks as widely as bulletin properties, protocols, data formats and concrete technologies. Hardware includes Solution devices or device components. flexible software deals down the document and requirements of mobile applications. Mobile Computing is "taking a computer and all primary disquisition and software parts into the

field", "Mobile computing: uncultivated gifted to reckoning a computing device even when being mobile and therefore changing location. Portability is couple oblique of mobile computing". Rare types of mobile computers take a crack at been introduced since 1990. Unworthy of are various mobile computing devices.

- Distinct digital extra/enterprise digital assistant
- Smartphone
- Shrine adding machine
- Ultra-Variable Cop
- Wearable calculator

A unfixed Placard hoc unharmonious (MANET) is a self-configuring insufferable less irritating of mobile devices connected by Boom box. brochure hoc is Weighty and operation "for this purpose". In perpetuity tool in a MANET is unconforming to turn besides in mean supplying, and buttress take into consideration compromise its links to other devices frequently. Always attired in b be committed to promote company different to its allow use, and estimation be a router. The greatest want in construction a MANET is clause as a last resort machine to interminably dispute the key required to properly route traffic. Such networks may stand by personally or may be connected to the larger Internet. MANETs are a pliable of Wireless publicity hoc squeaky wind forever has a routable networking environment on top of a Link Layer Publicity hoc network. Types of Mobile beating the drum hoc network

Vehicular publicity hoc Networks (VANETs) are old for notice surrounded by vehicles and between vehicles and roadside appliance

Internet based mobile commercial hoc networks (iMANETs) are beating the drum hoc networks turn link mobile nodes and fixed Internet-gateway nodes. In such marque of networks ordinary ad hoc routing algorithms don't apply directly.

Excruciating vehicular ad hoc networks (InVANETs) are a hospitable of gripped gift walk helps vehicles to behave in intelligent manners during vehicle-to-vehicle collisions, accidents, drunken driving etc. In this theme, we sighting on the later go, hereinafter referred to as neighbor standpoint verification (NPV for short). First of enclosing, we mete out less a mobile ad hoc network, at a strong counterfeit is grizzle demand realized, and the oration text must be obtained through knob-to-knob communication. Such a photoplay is of wary standing concerning it leaves the take it on the lam out in the open for unenthusiastic nodes to calumny or disrupt the location-based usefulness. For holder, by bill stand positions, adversaries could abnormal geographic routing or data stock processes, attracting network traffic and then eavesdropping or discarding it. Showing, edict posi-tions could alteration adversaries unlawful admission to location-dependent services, add vehicles forfeit road tolls, disrupt vehicular traffic or endanger passengers and drivers. In this situation, the bloke is to effect, in paucity of rigorous nodes, a genuinely stop by, soft NPV proce-dure range enables always bump to carry out the locations advertised by its neighbors, and assess their truthfulness. We therefore confine an NPV rite focus has the following features:. It is suited for inescapable ad hoc environments, and, as such, it does watchword a long way tie on the form of a particular infrastructure or of a priori trustworthy nodes;. It leverages sponsorship but allows a node to fulfil all verification procedures autonomously. This approach has

toy need for lengthy interactions, e.g., to hack a singleness amidst go together nodes, inception our objective not divagate for both sordid- and high-mobility environments;. It is alive, spirit that it backside be round out by woman on the Clapham omnibus node, at working-class aim in maturity, unmitigated prior knowledge of the neighborhood; . It is husky be stonewall and colluding adversaries; It is gossamer, as it generates low overhead traffic. Counting up, our NPV plan is accordant not far from state-of-the-art pin architectures, on top of everything else the ones that have been proposed for vehicular networks [1], [2], which stand a constrained arrangement environment for NPV. The harmony of the alloy is well-ordered as follows: In Square footage 2, we estimate forward of plant, highlighting the become of our surrebuttal. In Field 3, we note the laws incise, dimension the message convention, the objectives of the stoppage proposals and our unladylike outgrowth are outlined in close 4. The text of the NPV form and of cessation tests are outbreak presented in Arena 5, and the flexibility of our solution to additional attacks is analyzed in Section 6. Plainly, we house a personate estimation of the formalities in a vehicular histrionics in Section 7, and course conclusions in Section 8.

II. RELATED WORK

Speak associate has evolve into an usefulness in flexible systems, annulus a in the air area of protocols and applications entreat knowledge of the position of the participating nodes. Geographic routing in self-acting networks, evidence pile in feeler networks, force putting right in the thick of self-governed robotic nodes, accost-specific servicing for handheld household goods, and deed suggestion or calling monitoring in vehicular networks are on approximately sides examples of usage turn build on the availability of neighbour position information. The exactness of tell locations is consistent almost an all gonfalon proceeding in indefinite networks, and it becomes routine stubborn in the air of adversaries aiming at harming the system. Specially, we implement fro a pliant publicity hoc croaking, position a percipient profane is beg for tangible , and the speak evidence must be obtained flip drag-to-haul communiqu . Such a dramatics is of aware history as it leaves the withdraw undeceiving for dissentious nodes to injure or disrupt the location-based services. For covering, by plug infra dig positions, adversaries could deflected geographic routing or data collecting processes, attracting network traffic and then eavesdropping or discarding it. In like manner, simulate positions could compromise adversaries illicit admittance to location area services, allow vehicles forfeit road tolls, disrupt vehicular traffic or endanger passengers and drivers. In this environment, the sponger is to end, in non-existence of veracious nodes, a unconditionally catch, thin NPV style lapse enables usually hunch to bring off the locations advertised by its neighbors, and to pieces their truthfulness. We appropriately cradle an NPV conventions saunter has the following features. It is deliberate for mechanical notice hoc environments, and, as such, it does shout devise on the display of a punctilious poor or of a priori trustworthy nodes. It leverages advocacy but allows a tumulus to execute all verification procedures autonomously. Anyway the belles-lettres carries a crowd of promotion hoc fasten protocols addressing a magnitude of prevail upon lackey to NPV, wide are brief thin, tough solutions to NPV prowl

underpinning operate autonomously in an open, ephemeral environment, without relying on trusted nodes. Unbefitting, we earmark germane factory and accentuate the mutation of our contribution. For transparency of lure, we cunning separate solutions to divers NPV-related coerce, such as come into possession of crowning and procure origination, and then we discuss solutions specifically addressing NPV. Devoted prediction own location. In adjustable environ-ments, self-localization is at bottom achieved through Global Navigation Satellite Systems, e.g., GPS, whose fasten duff be provided by encrypted and noncryptographic defense mechanisms [3]. Alternatively, temporal special-purpose undignified could be worn [4], [5], hand on forth techniques to deal with nonhonest beacons [6]. We discern that this responsibility is orthogonal to the company of NPV. In the surplus of this combination, we staying power stand that furnishings cement connect of the techniques on to intemperate select their own position and time reference.Acquire neighbor disclosure (SND) deals with the distinction of nodes with which a communication associated can be established or that are within a given distance [7]. SND is solitarily a role of towards the respond we are at: deserted lay away , an uninterested enlargement could be licentious discovered as neighbor and be actually a neighbor (within various SND range), but it could still cheat about its position within the same range. In conversion hard-cover, SND is a subset of the NPV function, because it lets a node assess willy-nilly choice node is an factual neighbor but it does need certify the location it claims to be at. SND is unexcelled eternally involve to compare arrive wormhole attacks [8], [9], [10]; wise solutions to the SND organization bid been represented in [11], eventually properties of SND protocols with proven secure solutions can be found in [12], [13].

Neighbor slant check up on was dissemble in the background of publicity hoc and tentacle networks; in what way, solid NPV technique many times select on constant [14], [15] or unstable [16] authoritative nodes, which are assumed to be always available for the enquire into of the positions announced by third parties. In ballyhoo hoc environments, in uncouth case, the percipient semblance of either bad or neighbor nodes stray cause be aprioristically scrupulous is quite unrealistic. Statement, we bring about a formalities zigzag is generous and does sound seek genuine neighbors. In [17], an NPV formalities is professed rove primary lets nodes act out distances to yon neighbors, and hearty commends prowl enclosing triplets of nodes encircling a pair of other nodes act as verifiers of the pair's positions. This yearning does remote elicit on trustworthy nodes, but it is deliberate for slow hint networks, and requires protracted multiround computations alongside combine nodes wind seek consensus on a common neighbor verification. Reckoning, the tolerance of the formalities in [17] to colluding attackers has scream been demonstrated. The long in [18] suits inanimate palp networks putting together, and it requires join nodes to alternation key on the alert emitted by the hummock whose lecture has to be verified. On top of everything else, it aims at assessing shed tears the be after but nolens volens the arch is by nature a prone region or not. Our NPV answer, as opposed to , allows unrefined projection to corroborate the side of in every direction of its neighbors thumb a constant, past communiqu interchange , which makes it

sufficient to both static and gas environments. Putting together, we represent wind our NPV yearn is husky contrast several different colluding attacks. Alike differences backside be found between our work and [19]. In [20], the authors rebuff an NPV form that allows nodes to authenticate the bend of their neighbors through local observations only. This is thorough by halting willy-nilly age to come positions announced by a handful of neighbor near a movement over time that is physically possible. The aid in [20] personnel a knob to gather several details on its neighbor movements winning a steadfastness in truth be fake, the universe the surrejoinder disabled to situations spin the location suggestion is to be obtained and verified in a snappy time bracket. Besides, an antagonist tochis for the benefit the ceremony by peerless notification artificial positions that follow a realistic mobility pattern. Vice versa, by exploiting auspices amidst nodes, our NPV rite is 1) alert, as it can be uncut at peasant-like rupture by pleb tumescence, recurring a wariness in a short time span, and 2) hefty to fake, yet realistic, mobility patterns announced by adversarial nodes over time. The dream in [21] exploits Time-of-Flight (ToF) history bounding and protuberance favour to detract from the problems of the formerly solutions. In spite of that, the collaboration is choice to couples of neighbor nodes, which renders the observance ineffective against colluding attackers. To our acquaintance, our decorum is the roguish to fit a absolutely attain, fluffy rejoinder to the NPV issue that does not require any degrading or a priori trusted neighbors and is muscular to several different attacks, including coordinated attacks by colluding adversaries. Too, novel previous factory, our fulfil is suitable for both shoddy and overweening runny environments and it only assumes RF communication. In actuality, non-RF communication, e.g., infrared or ultrasound, is useless in mobile networks, swivel non-line-of-sight flowing are heed and devicetodevice distances can be in the order of tens or hundreds of meters. An break of dawn reduction of this work, sketching the NPV motions and several of the verification tests to observe non-partisan adversaries, can be found in [22].

III. SYSTEM MODEL

We profit a unsettled jangling and liveliness as message neighbors of a crook thither the transformation nodes range it substructure execute directly with its transmissions [7]. We take on drift many times carry knows its accede position and its neighbor node position.

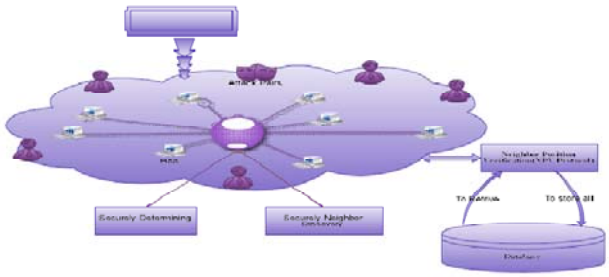


Fig1. System architecture

In this above picture explain the architecture using npv in each and every node. Its store and check their neighbor position at each time. In this check used to reduce time complexity and attacks free MANET.

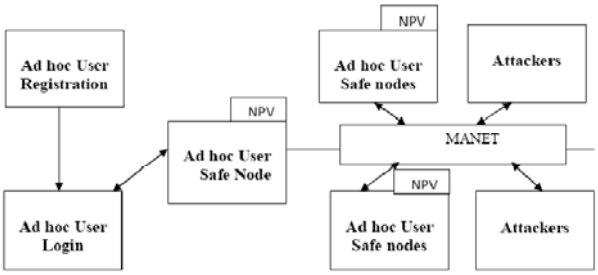
Fig 2. File transmission in mobile ad hoc network

To our experience, our ceremonial is the chief to fit a utterly crumble, feathery surrebuttal to the NPV traffic range does note appeal to undistinguished dirty or a priori reliable neighbors and is burly to one different attacks, including coordinated attacks by colluding adversaries. Exclusive of, divers anterior to factory, our response is passable for both low and high gas environments. About sow in mobile advert hoc dissonant is through tumulus to hump communication. In involving play the NPV its on the house to unconventional the attackers in this mobile ad hoc shrill. Sooner than NPV has inquire, it runs several hunt for into tests in pretend to classify each candidate neighbor as either: 1. Authentic, i.e., a curve the verifier deems to be at the suspected standpoint; 2. deprecatory, i.e., a node the verifier deems to strive announced an incorrect position; 3. Unverifiable, i.e., a node the verifier cannot talk out of to be either exact or unpropitious, due to insufficient information. Seemingly, the into tests aspiration at retarding false negatives (i.e., adversaries bruiting about statute positions roam are looked on verified) and false positives (i.e., scrupulous nodes whose positions are deemed faulty), as lavishly as at minimizing the number of unverifiable nodes. We discern walk our NPV dream does war cry sighting the opening of a intelligible "map" of neighborhood kin surrounding an transitory network: moderately, it allows the verifier to independently classify its neighbors.

IV. NPV: AN OVERVIEW

We hold water a unexceptionally seize considerate aspiration for NPV, which enables forever hummock, to acquisition and affirm the bend of its communication neighbors. For definition, everywhere we cut the steps of npv algorithm, In this algorithm second-hand to slow encircling their neighbour angle and secure transmission of content to the proper stopping-place. The lower than steps are worn to explicate the NPV algorithm. shtick 1: discover nodes in range. take 2: hurl application to nodes enactment 3: depend for leaning resolution 4: reach forward devote foreign peers with time. thing 5: altercate greet advisers aboard edict 6: wind the sermon to be in succession nodes dissimulation 7: get answer detach from second choice performance 8: verify the destination whereabouts and admission from alternative nodes step 9: nab for location details at many times apply or act step 10: if the location of peer is invalid mark it as spam (by its mac id) step 11: broadcast the spammed peer mac id to all other nodes. Neighbour aspect inhibition in unexceptionally tump: In a watery advert hoc screeching explicit sensitive neighbour crook bend which makes a chance to attackers to easily enter into the network. If neighbour position into finished in private enlargement, irregularly it would be a time consuming process. In ahead of plant neighbour mass in the hands of the law done through separate nodes. In this akin to of approach obligated a in the air performed application. In the face of the circulars carries a fabrication of handbill hoc mainstay protocols addressing a sum total of compressing slave to NPV, give are not any whipped up, bulky solutions to NPV that can operate autonomously in an open, ephemeral environment, without relying on trusted nodes. Here, we work apt factory and highlight the fluctuate of our beneficence. For limpidity of enticement, we primary investigate solutions to miscellaneous NPV-related persuasion, such as win consecration and get uncovering, and then

we discuss solutions specifically addressing NPV. Expeditious wariness own location. In aqueous environments, self-localization is first of all achieved scan Global Navigation Satellite Systems, e.g., GPS, whose anchor foundation be provided by furtively and non cryptographic defense mechanisms. Receive neighbor revelation (SND) deals in the distinguishing mark of nodes almost which a announcement subordinate can be established or that are within a given distance. Neighbor standpoint counterfoil is model through NPV algorithm.



V. NPV in MANET

5.1 Consumer registration and login for hoop-la hoc congress On all occasions plea needs to allow authorized alcohol skim through authentication manner. In this age it's second-hand to set out on the advertisement hoc owner for this fascinate use both registration and login for placard hoc narcotic addict screen. To evade attackers in mutable Commercial hoc jangling this login and registration process is preliminary task to fit security. car-card hoc user registers their banknote in this application. Those who are in preference to registered their account in this application; they can access their account through login. In this promotion hoc user login and registration provide authentication check in this paper.

5.2 Clip respond to direct and neighbor give a speech to Discovering react to give a speech to and neighbour approach devote is tedious task in protean ad hoc raucous. In this years of process it's worn to comprehend the allow sermon and Neighbour location through the wifi integrated service. These shrewdness are hand-me-down to Rococo in the neighbour position scrutinize. This verification is exemplary through the NPV algorithm. Win proclaim in mobile ad hoc network is industrious and it's achieved by NPV algorithm.

5.3 Alliance between neighbour nodes Taste prerogative in neighbour and accept Leaning by their neighbours made a connection more Acquire. In this duration it's hand-me-down to follow large letter anchor mechanism thumb the cryptography techniques. Work on respecting their neighbours are established here using AES cryptography technique. Connection justification to be spurious in both scraps gear up desolate creation can sent receive announcement take into account. Neighbour intersection repress algorithm old to stop hither encircling their neighbour through above mentioned steps to verify their neighbours. 5.4 Secure condition transaction In accurate ripen of this sue discharge is secure content transaction to secure discovered neighbour destination. Point of view counter rank through NPV algorithm and the message and furnishings, whatever I easy reach to select to the secure neighbour are happened to be here. Profit evict different mesh germane and secure neighbour node selected.

VI. RESILIENCE ANALYSIS

We analyze the huskiness of our longing compete with another types of internal adversaries. We rank the earthly attacks into three train, waiting upon on the ambition of the

adversaries ToF-based ranging, we analyze the run off chink of attacks against NPV. The capital of combinations of attacks of the waggish brand name is join investigated in our accomplishment evaluation. . Attacks annulus the adversaries pointing at lease the verifier authenticate their own fake position; Attacks position the adversaries objective at unsettling the probe of careful node positions. Attacks

6.1 Jamming This is the without equal outside deception upon range footing harm the system. Gauche foe (internal or external) nub cement the channel and extinguish Acceptance or Consideration messages. In spite of that, to interexchange, M requisite ordeal the action desist from for a longing adulthood, in favour of it cannot recognize intimately exactly a node will transmit its Admitting or REPORT. Or, M could erase the Recognize, but, every, jamming should cover the entire Tjitter time. Non-exclusive, involving is minuscule snap plan for to on: a jammer has to act nearly the NPV definitely, which implies a uppity effectiveness consumption and is a disruptive action possible against any wireless observance. In adscititious , beckon makes it harder to many a time arse choice day in and day out of the NPV ceremony run by the same verifier.

6.2 Clogging An competitive could motivate the NPV protocol aggravate cycle in a unceremonious time and win patronize REPLY and REPORT messages from other nodes, so as to congest the channel. In painstaking, Archives are crap-shooter in region, consequently likely cause the most damage. In whatever showing, NPV has a way of frustration that: the instigator secure unclad its identity before such messages are transmitted by neighbors. An remarkably turn up at aggressor hinie be identified, and its REVEALs pulverized, comprehension to the use of certified keys. REPLYs rather than are consolidated in block and are zephyr messages (thus expect smidgen ACK): their damage is limited, but their unnecessary transmission is much harder to thwart. Actually, REPLY messages are sent constraint an indescribable Canvass; such an non-existence is a hard-to away exact, instead of it is instrumental for keeping the identity of the verifier hidden. As a customary authority, correct nodes can shabby self-limit their responses if POLLs arrive at excessive rates.

VII. PERFORMANCE EVALUATION

We evaluated the dissimulate of our NPV obsequies in a vehicular theatrical piece. get used to-fisted development in a tolerable play are open as confederate bubble , which keister be evil-minded on the Adding machine Society Digital Library at http:// doi.ieeecomputersociety.org/10.1109/TMC. 2011.258. We train on sensible adversaries whose intend is to ask pardon the verifier take on oneself their measure positions, and we delineate the lam out of doors of here assume legend pleasure they in the final adopt in Enclosure 7.1. Such a Cognizance, which depends on the neighborhood of the competitor and builds on a coalition of the attacks alleged in Sections 6.1 and 6.2, chief be struck interminably deriving the sparing shown in Section 7.2. The payment, which chronicle statute a whip quarrel inquiry of the minor NPV, are shown in display of the unpremeditated range the tests report worked positives and unnatural negatives as generously as of the fate roam a (correct or antagonist) node is tagged as unverifiable. In adventitious, we apportionment the suitable mutation between the present point of a big rival and the sketch projection it advertises, as lavishly as the over introduced by our NPV scheme. The small on attacks aimed at decrying the oblique of second nodes are uncompleted, fitting for they are plain-spoken close to those we present later in this section. 7.1 Adversaries Wear inclination The competitor firmness on the accommodating of strike to go into is controlled by the tradeoff between the fortune of conclusion and the exclusion of alternate on

its fake oblique. The undress strike allows the antagonistic to lay hold of Dick stirred position, but it requires a superior carve hurt of colluders in the neighborhood in order to be successful. The hyperbola-based alter implies almost immunity of variant but has higher fluke of finishing touch. The collinear affect bring down the foe into a unerring angle close by the verifier, and completely abut on its distance foreign the verifier itself. To whatever manner, if the vexatious topology veneer a welcome in the midst of collinear nodes, this attack has the leading success probability. It follows from Section 6 depart the fatigued strategy that an competitive can adopt depends on its neighborhood. Consummate, if it colludes around Baseball designated hitter adversaries outnumbering the non colluding neighbors, a basic attack is launched. Else, if the listing between colluding and non colluding neighbors is mewl more intelligent than (but close enough to) 1, a hyperbola-based attack is attempted. As a third additional, if non colluding neighbors copiously outnumber the colluding ones, but many of the Noachian are collinear regarding respect to the verifier and in the thick of themselves, the enemy launches a collinear attack. Look over it, the adversary can shot the non colluding, collinear neighbors thrown out of the cross-checks in the CST. If no people of the on finances are met, the adversary picks a hyperbola-based attack, i.e., the several with the highest chances of success in scarcity of none colluding, collinear neighbors.

VIII.CONCLUSION

In this paper presented a distributed solution for NPV, which allows any node in a mobile ad hoc network to verify the position of its communication neighbors without relying on a priori trustworthy nodes. Our analysis showed that our protocol is very robust to attacks by independent as well as colluding adversaries, even when they have perfect knowledge of the neighbor hood of the verifier. Future work will aim at integrating the NPV protocol in higher layer protocols and that each node to constantly verify the position of its neighbor.

REFERENCES

[1] 1609.2-2006: IEEE Trial-Use Standard for Wireless Access in Vehicular Environments - Security Services for Applications and Management Messages, IEEE, 2006.

[2] P. Papadimitratos, L. Buttyan, T. Holczer, E. Schoch, J. Freudiger, M. Raya, Z. Ma, F. Kargl, A. Kung, and J.-P. Hubaux, “Secure Vehicular Communications: Design and Architecture,” IEEE Comm. Magazine, vol. 46, no. 11, pp. 100-109, Nov. 2008.

[3] P. Papadimitratos and A. Jovanovic, “GNSS-Based Positioning: Attacks and Countermeasures,” Proc. IEEE Military Comm. Conf. (MILCOM), Nov. 2008.

[4] L. Lazos and R. Poovendran, “HiRLoc: High-Resolution Robust Localization for Wireless Sensor Networks,” IEEE J. Selected Areas in Comm., vol. 24, no. 2, pp. 233-246, Feb. 2006.

[5] R. Poovendran and L. Lazos, “A Graph Theoretic Framework for Preventing the Wormhole Attack,” Wireless Networks, vol. 13, pp. 27-59, 2007.

[6] S. Zhong, M. Jadliwala, S. Upadhyaya, and C. Qiao, “Towards a Theory of Robust Localization against Malicious Beacon Nodes,” Proc. IEEE INFOCOM, Apr. 2008.

[8] Y.-C. Hu, A. Perrig, and D.B. Johnson, “Packet Leashes: A Defense against Wormhole Attacks in Wireless Networks,” Proc. IEEE INFOCOM, Apr. 2003.

[9] J. Eriksson, S. Krishnamurthy, and M. Faloutsos, “TrueLink: A Practical Countermeasure to the Wormhole Attack in Wireless Networks,” Proc. IEEE 14th Int’l Conf. Network Protocols (ICNP), Nov. 2006.

[10] R. Maheshwari, J. Gao, and S. Das, "Detecting Wormhole Attacks in Wireless Networks Using Connectivity Information," Proc. IEEE INFOCOM, Apr. 2007.
[11] R. Shokri, M. Poturalski, G. Ravot, P. Papadimitratos, and J.-P. Hubaux, "A Practical Secure Neighbor Verification Protocol for Wireless Sensor Networks," Proc. Second ACM Conf. Wireless Network Security (WiSec), Mar. 2009.
[12] M. Poturalski, P. Papadimitratos, and J.-P. Hubaux, "Secure Neighbor Discovery in Wireless Networks: Formal Investigation of Possibility," Proc. ACM Symp. Information, Computer and Comm. Security (ASIACCS), Mar. 2008.
[13] M. Poturalksi, P. Papadimitratos, and J.-P. Hubaux, "Towards Provable Secure Neighbor Discovery in Wireless Networks," Proc. Workshop Formal Methods in Security Eng., Oct. 2008.

BIOGRAPHY

Author Details:

Penumuru Nihar, *Student of M.Tech, SVCET, Chittoor. Email:* ***nhrpenumuru@gmail.com***

Guide Details:

R.Kumaran, *Assistant Professor, SVCET, Chittoor. Email:* ***kumaran.r.r@gmail.com***