Implementing the Robust Technique for Verifying the Neighbor Positions in MANET

Ms. Sejal Rana
M.E. Student
Department of Computer Science & Engineering
Narnarayan Shastri Institute of Technology, Jetalpur, India

Mr. Pragnesh Patel
Assistant Professor
Department of Computer Science & Engineering
Narnarayan Shastri Institute of Technology, Jetalpur, India

Abstract

Mobile ad-hoc network is a collection of independent mobile nodes that can communicate to each other via radio waves". After nodes are deployed, they do not have knowledge about the neighbors so, they need to discover their neighbors in order to communicate with them. Knowledge of the neighbor nodes is essential for almost all routing protocols, medium-access control protocols and other topology control algorithms. Now, neighbor node may be trustable node or adversarial node so verification of node is require. For neighbor position verification NPV protocol is used. NPV protocol deals with verifying the neighbor node location. Nowdays, location awareness has become very important in MANET because wide range of protocol and application require knowledge of the position of participating nodes. So it is require improving NPV protocol. Examples of services that build on the availability of neighbor position information are Geographic routing in spontaneous networks, data gathering in sensor networks, movement coordination among robotics nodes, location specific services for handheld devices. Existing NPV protocol has some limitation like Lower Performance and False Positive Rate and False Negative Rate are high. So The objective of our proposed system is improve the FPR and FNR means minimize the FPR and FNR.

Keywords: Mobile Ad hoc networks, Neighbor position verification, False Positive Rate, False Negative Rate

I. INTRODUCTION

"MANET means Mobile ad hoc Networks, It is a collection of independent mobile nodes that can communicate to each other via radio waves" [1]. The mobile nodes which are in the same range of each other they can communicate directly and which are not in the same range or out of range they can communicate indirectly using intermediate or neighbor nodes to route their packets.When nodes are designed and deployed, they do not know about their neighbor nodes, so it requires that they must have knowledge about their neighbor nodes to communicate with them.They need to discover their neighbor nodes for communicating with them.Nowdays, The knowledge of neighbor nodes is basic requirement for almost all medium-access control protocols, routing protocols and other topology algorithms.The neighbor node may be trustable node or malicious node.So,It is require to verify the neighbor nodes.Neighbor Position Verification (NPV) protocol is used to verify the neighbor node location.Because of malicious node, nowdays location awareness has become vey important in MANET. In MANET wide range of routing protocol and application require knowledge of the position of neighbor nodes.So, it is necessary to improve NPV protocol.Example of services which build on the availability of neighbor position information are data gathering in sensor networks, location specific services for handheld devices, Geographic routing in spontaneous networks, movement coordination among robotics nodes etc.

II. RELATED WORK

A. Node Discovery

After nodes are deployed, they do not have knowledge about the neighbors so they need to discover their neighbors in order to communicate with them. Knowledge of the neighbors is essential for almost all routing protocols, medium-access control protocols and several other topology-control algorithms. Neighbor discovery is, therefore, a crucial first step in the process of self-organization of a wireless ad-hoc network [5].

The neighbors can be either physical neighbors or communication neighbor. The physical neighbors are those that are in the range of physical proximity of the discoverer. The communication neighbors are those that are reachable for communication but need not to be in the physical range of the discoverer.

1) Neighbor Discovery Algorithms

2) Randomized Neighbour Discovery

In randomized neighbour discovery, each node transmits at randomly chosen times and discovers all its neighbours by a given time with high probability.

All rights reserved by *www.ijste.org*

3) Deterministic Neighbour Discovery
In deterministic neighbour discovery, each node transmits according to a predetermined transmission schedule that allows it to discover all its neighbours by a given time with probability one.
4) Antenna Based Neighbour Discovery
The antenna models used in ad hoc networks are Omni directional antenna model or directional antenna model.
5) The Omni Directional Antenna Model
The Omni directional antenna model propagates signal in all directions. The algorithm used by Omni directional antenna is 1-way algorithm where the receiver will not send any acknowledgement after receiving the discovery message. The sender broadcasts the DISCOVER message to advertise itself. The receivers will discover one neighbor if it receive the DISCOVER message correctly in the listen state.The Omni directional antennas have drawbacks like reduced gain, increased signal distraction, high bandwidth consumption, and increased noise.
6) Directional Antennas Model Provide
Directional antennas model provide longer transmission range and higher data rate. They strongly reduce signal interferences in unnecessary directions and reduce jamming susceptibility. The directional antenna algorithms used to discover neighbors.
7) Direct Discovery Algorithm
In direct discovery algorithm the nodes discover the neighbors which communicate with it directly. The method used to discover the neighbors is recording the angle of arrival of the beacon signal, determining the location based using GPS. The direct discovery algorithm will discover only those neighbors that communicate with it directly.
8) Gossip Based Algorithms
In gossip based algorithm the neighbors are discovered indirectly through the interaction with other neighbors. Messages are exchanged to discover the neighbors. The message consists of the list of neighbors‟ IDs and their locations. The main drawbacks of gossip based algorithm are message length grows as more and more nodes are discovered and the presence of physical obstacles can cause nodes to incorrectly infer another node as its neighbor.
9) Limitation of Neighbour Discovery Algorithms
These algorithms do not provide the security architecture to identify the malicious or misbehaving nodes. These algorithms do not verify the position of the neighbor nodes.

B. Existing Methods

1) Securely Determining Own Location
In MANET, self-localization is mainly achieved through Global Navigation Satellite Systems, for example GPS, whose security can be provided by cryptographic and non-cryptographic defense mechanisms [6].
2) Secure Neighbour Discovery (SND)
It deals with the identification of nodes which a communication link can be recognized or that are within a given distance [8]. SND is only a step toward the solution that simply place, an adversarial node could be securely discovered as neighbour and be indeed a neighbour (within some SND range), but it could still cheat about its position within the same range. In other words, SND is a subset of the NPV problem, since it lets a node assess whether another node is an actual neighbour but it does not verify the location. In short SND just finds neighbour node but it does not verify the position of that node.
3) Neighbour Position Verification
In [7], an NPN protocol is proposed that first lets nodes calculate distances to all neighbours, and then commends that all triplets of nodes encircling a pair of other nodes act as verifiers of the pair's positions. This scheme does not rely on trustworthy nodes, but it is designed for static sensor networks, and requires lengthy multi-round computations involving several nodes that seek consensus on a common neighbour verification.

In [9], an NPV protocol that allows nodes to validate the position of their neighbours through local observations only. This is performed by checking whether subsequent positions announced by one neighbour draw a movement over time that is physically possible. The approach in [9] forces a node to collect several data on its neighbour movements before a decision can be taken, making the solution unfit to situations where the location information is to be obtained and verified in a short time span. Moreover, an adversary can fool the protocol by simply announcing false positions that follow a realistic mobility pattern.

C. NPV Algorithm

This algorithm basically used to discover and verify the position of its communication neighbors [10]. The below steps are used to explain the NPV algorithm.

1) Step 1: Discover Nodes In Range.
2) Step 2: Send Request To Nodes
3) Step 3: Wait For Connection
4) Step 4: Get Location From Peers With Time.
5) Step 5: Maintain Location Table
6) Step 6: Broadcast The Location To Other Nodes

All rights reserved by *www.ijste.org*

7) Step 7: Get Response From Other
8) Step 8: Verify The Destination Location And Response From Other Nodes
9) Step 9: Check For Location Data At Every Request Or Operation
10) Step 10: If The Location Of Peer Is Invalid Mark It As Spam (By Its Mac Id)
11) Step 11: Broadcast The Spammed Peer Mac Id To All Other Nodes.

1) NPV Protocol

NPV means Neighbor position Verification Protocol. This Protocol exchanges messages and using verification test verify the position of communicating nodes [11].

Let a node S is called as a verifier, which discovers and verifies the position of its communicating neighbors. A verifier, S, can initiate the protocol at any time instant, by triggering the 4-step message exchange. The aim of the message exchange is to let S collect information it can use to compute distances between any pair of its communication neighbors. After the distances are calculated the nodes are classified as:

- Verified: Node is in the claimed position.
- Faulty: Node has announced an incorrect position.
- Unverifiable: Insufficient information.

The verification tests aim at avoiding false negatives (i.e., adversaries announcing fake positions that are deemed verified) and false positives (i.e., correct nodes whose positions are deemed faulty), as well as at minimizing the number of unverifiable nodes. Here four set of messages are exchanged they are:

- POLL message
- REPLY message
- REVEAL message
- REPORT message

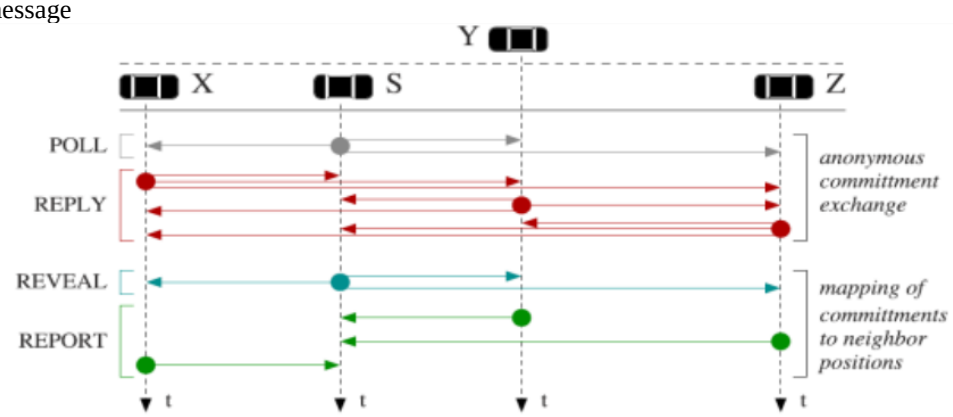

Fig. 1: Message exchange

2) POLL Message

A verifier S initiates this message. This message is anonymous. The identity of the verifier is kept hidden. Here software generated MAC address is used. This carries a public key K'S chosen from a pool of onetime use keys of S'.

3) REPLY Message

A communication neighbour X receiving the POLL message will broadcast REPLY message after a time interval with a freshly generated MAC address. This also internally saves the transmission time. This also contains some encrypted message with S public key (K'S). This message is called as commitment of X CX.

4) REVEAL Message

The REVEAL message is broadcasted using Verifier's real MAC address. It contains A map MS, a proof that S is the author of the original POLL and the verifier identity, i.e., its certified public key and signature.

5) REPORT Message

The REPORT carries X's position, the transmission time of X's REPLY, and the list of pairs of reception times and temporary identifiers referring to the REPLY broadcasts X received. The identifiers are obtained from the map MS included in the REVEAL message. Also, X discloses its own identity by including in the message its digital signature and certified public key.

6) Position Verification Test

To verify the position of a node following three tests is done they are:

- Direct symmetry test
- Cross symmetry test
- The Multilateration Test

All rights reserved by *www.ijste.org*

7) Direct Symmetry Test
In the Direct Symmetry Test, S verifies the direct links with its communication neighbors. To this end, it checks whether reciprocal Time of Flight-derived distances are consistent with each other, with the position advertised by the neighbor, and with a proximity range R.
8) Cross Symmetry Test
In Cross symmetry test information mutually gathered by each pair of communication neighbors are checked. This ignores nodes already declared as faulty by the DST and only considers nodes that proved to be communication neighbors between each other, i.e., for which ToF-derived mutual distances are available.
9) The Multilateration Test
In Multilateration test, the unnotified links are tested. For each neighbor X that did not notify about a link reported by another node Y, with X, Y € WS range. Once all couples of nodes have been checked, each node X for which two or more unnotified links exist is considered as suspect.

III. PROPOSED SYSTEM

There are various methods for verifying the neighbor position but there is not an efficient or robust technique which minimizes the False Positive Rate and False Negative Rate. So we proposed a system which will minimize the FPR and FNR. For minimizing the FPR and FNR we included parameter in the proposed system. This parameter is Threshold Value. After that we will make efficient method of Message Exchange for verifier, Message Exchange for any neighbor, Algorithm of DST, Algorithm of CST and Algorithm of MLT.

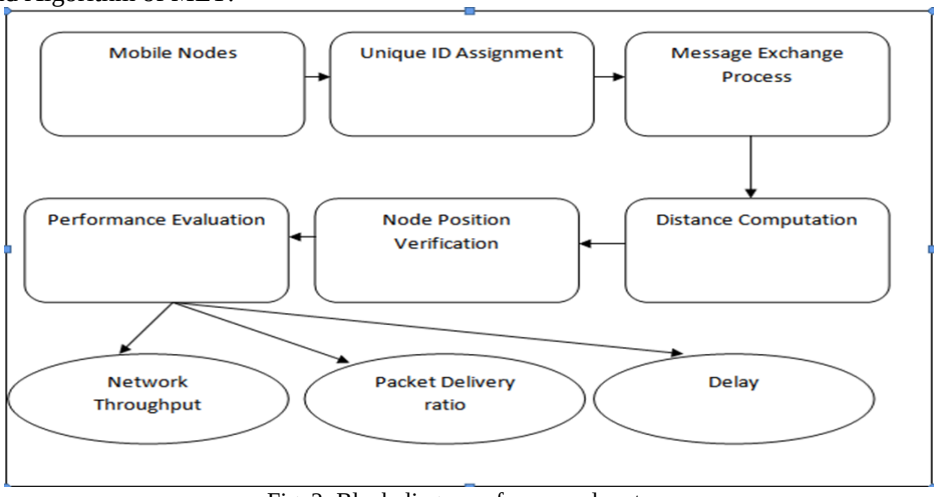

Fig. 2: Block diagram of proposed system

IV. IMPLEMENTATION OF PROPOSED SYSTEM

A. Modules

- Node configuration setting
- Nodes unique identity
- Message Exchange process for route discovery
- Distance computation
- Node position verification
- Node verification process
- Graph Examination

B. Module Description

1) Node Configuration Setting:
The mobile nodes are designed and configured dynamically, designed to employ across the network, the nodes are set according to the X, Y, Z dimension, which the nodes have the direct transmission range to all other nodes.

All rights reserved by *www.ijste.org*

2) Nodes Unique Identity:
All the mobile nodes tend to have a unique id for its identification process, since the mobile nodes communicates with other nodes through its own network id. If any mobile node opted out of the network then the particular node should surrender its network id to the head node.
3) Message Exchange Process for Route Discovery:
This module states a 4 step message exchange process i,e POLL, REPLY, REVEAL, REPORT. As soon the protocol executed the, POLL and REPLY messages are first broadcasted by Source and its neighbours, respectively. These messages are anonymous and take advantage of the broadcast nature of the wireless medium, allowing nodes to record reciprocal timing information without disclosing their identities.
4) Distance Computation:
In order to compute the distance range, after a POLL and REPLY message a REVEAL message broadcast by the source nodes disclose to S, through secure and authenticated REPORT messages, their identities as well as the anonymous timing information they collected. The source S uses such data to match timings and identities; then, it uses the timings to perform ToF-based ranging and compute distances between all pairs of communicating nodes in its neighbourhood.
5) Node Position Verification:
Once Verifier node has calculated such distances, it runs some position verification tests in order to classify each candidate neighbour as either: Verified Node: This node is in the right or exact position. Faulty Node: This node has declared fake position. Unverifiable Node: this node has insufficient information. The position verification are performed by direct symmetric test, cross symmetry test and multilateration test.
6) Node Verification Process:
In this module a proposed work of node verification technique is introduced to detect the adversary nodes in the network. The node verification is done by hash function technique the public key and id of source node generates hash id. In the same way the neighbor nodes generate the hash id, if the source node hash id and neighbor node hash id are same then the nodes are authenticated for data transmission through the minimum distance range discovered path to destination.
7) Graph Examination:
The performance analysis of the proposed work is examined through graphical analysis.

C. Implementation

We implement the proposed system in NS2 and for that the parameter setting is shown as below. Here Implementation is done under this scenario of networking conditions.

- set val(prop) Propagation/TwoRayGround # radio-propagation model
- set val(netif) Phy/WirelessPhy # network interface type
- set val(mac) Mac/802_11 # MAC type
- set val(ifq) Queue/DropTail/PriQueue # interface queue type
- set val(ll) LL # link layer type
- set val(ant) Antenna/OmniAntenna # antenna model
- set val(ifqlen) 50000 # max packet in ifq
- set val(nn) 30 # number of mobilenodes
- set val(rp) NPV # routing protocol
- set val(x) 1500 # X dimension of topography
- set val(y) 1500 # Y dimension of topography
- set val(stop) 10.0 # time of simulation end
- set val(threshold1) 80
- set val(energy) 10

V. RESULTS

The below figure shows the verification of the neighbor nodes is done and malicious nodes are found by the proposed system.

All rights reserved by *www.ijste.org*

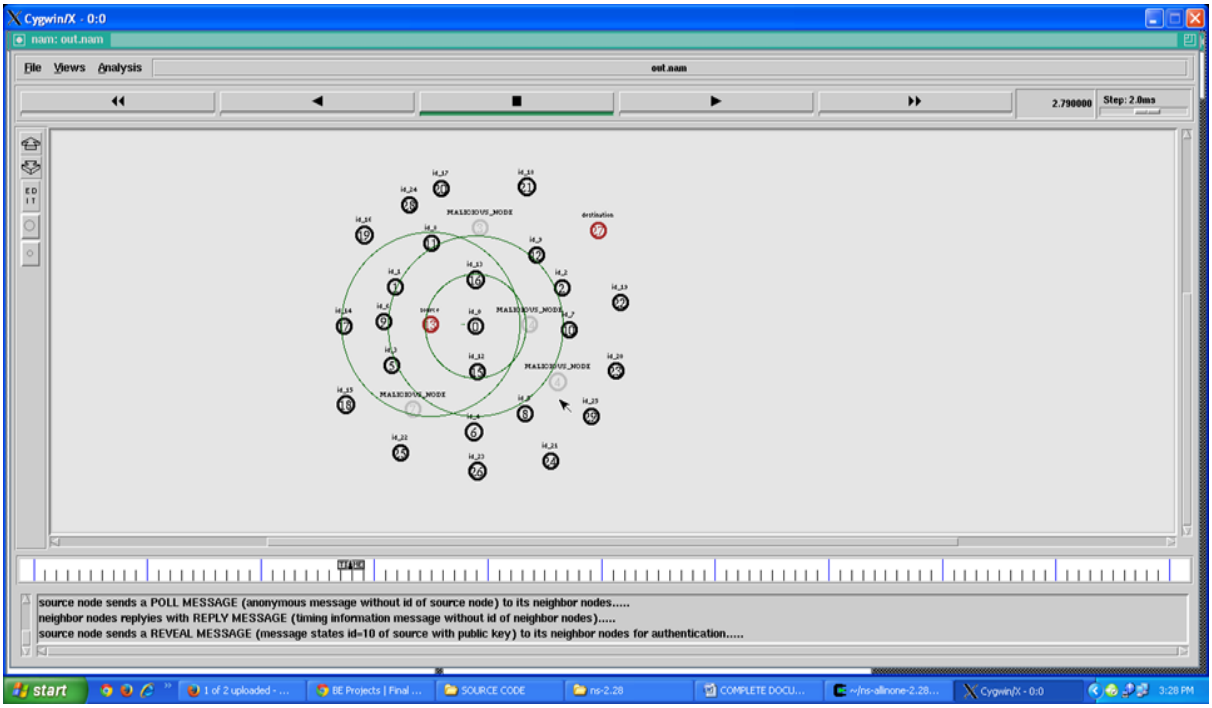

Fig. 3: Malicious nodes are found by NPV

Here this graph is showing results of Packet delivery ration Vs Node mobility for Different scenarios. As the graph shows that the PDR remains constant for all three scenarios.

Fig. 4: Packet delivery ration Vs Node mobility for Different scenarios

Here this graph is showing summarized results of Packet delivery ratio, Throughput & Delay. We can analyze that the performance of the proposed system is improved in terms of Delay. Also network throughput is not so much improved but the PDR has been improved better.

All rights reserved by *www.ijste.org*

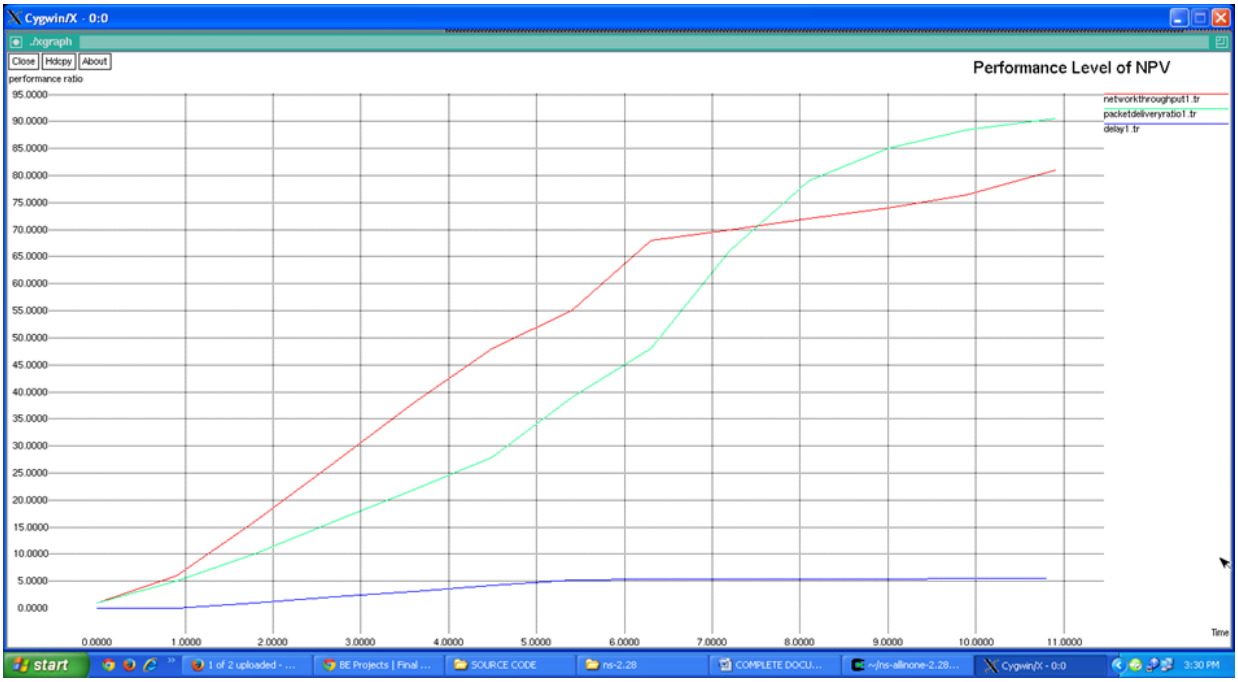

Fig. 5: Summarized results of Packet delivery ratio, Throughput & Delay

VI. CONCLUSION

In MANET a growing number of ad hoc networking protocols and location-aware services require that mobile nodes learn the position of their neighbors. So we require to verify the position of the neighbor node for secure communication. There are various methods for verifying the neighbor position but there are some limitation of Existing methods like lower performance and FPR & FNR are not minimize. So we proposed a robust technique which minimizes the FPR & FNR using Threshold parameter.

REFERENCES

[1] Study of Manet:Characteristics, Challenges,Application and Security Attacks. Tyagi, Dr.S.S. May 2013, International journal of Advance Reserach in Computer Science and Software Engineering, p. 7.
[2] Secure Data Transmission in MANET Routing protocol. Srivastava, Kartik Kumar. ISSN, Gorakhpur : s.n., Vols. 3(6),1915-1921. 2229-6093.
[3] A Study on the Behaviour of MANET Routing Protocols with varying Densities and Dyanamic Mobility Patterns. Nawaz, Dr.D.M Kadhar. Mobile Ad-hoc Networks, Salem : IJCA, 2010.
[4] Neighbor node Discovery and Trust Prediction in MANETs. Dr.D.Thilagavathy, Ms.Suganya Devi.S. 1, Tamilnadu : IJSETR, January , 2013, Vol. 2. ISSN: 2278-7798.
[5] GNSS - based Positioning:Attack and Countersmeasures. P.Papadimitratos, A.Jovanovic. San Diego : IEEE Milcom, 2008.
[6] Secure positionig in Wireless Networks. S.Capkun, K, J-P.Hubaux. s.l. : IEEE JSAC, 2006, Vol. 24.
[7] Effective Neighbor Identification with False Report verification Using Manets. M. Abinaya, Mrs. K. Thamaraiselvi. 1, Tamilnadu : IJIRCCE, March,2014, Vol. 2. ISSN 2320-9801.
[8] Improved Security in Geographic Ad Hoc Routing through autonomous Position verification. T.Leinmuller, C.Maihofer.Schoch,F.Kargal. Los Angeles : s.n., Sept.2006.
[9] Neighbor Position Verification in Mobile Ad Hoc Network. RAJA, C.LOURDU. 1, Tamilnadu : IJIRCCE, March 2014, Vol. 2. ISSN 2320-9798.
[10] Dyanamic Neighbor Positioning In Manet with Protection against Adversarial Attack. K.Priyadharshini, V.Kathiravan,S.Karthiga,A.Christopher Paul. 4, s.l. : IJCER, Vol. 3.
[11] Discovery and Verification of Neighbor Positions in Mobile Ad Hoc Networks. Fiore, Macro. Carala-Fabiana : IEEE, february 2013, Vol. 12. 2.
[12] Secure Location verification for Vehicular Ad-hoc Networks. J.H Song, V.Wong and V.Leung. s.l. : IEEE Globecom, December 2008.
[13] Secure Neighborhood Discovery:A Fundamental Element for Mobile Ad-hoc Networks. P.Papadimitratos, M.Poturalski, P.Lafourcade, D.Basin,S.Capkum. 2, s.l. : IEEE comm.Magazine, February 2008, Vol. 46.
[14] A Practical Secure Neighbor Verification Protocol for Wireless Sensor Networks. R.Shokri, M.Poturalski ,G.Ravot, P.Papadimitratos, J-P.Hubaux. Zurich Switzerland : ACM WiSec, March 2009.

All rights reserved by *www.ijste.org*