Communications on Applied Electronics (CAE) – ISSN : 2394-4714
Foundation of Computer Science FCS, New York, USA
Volume 4– No.4, February 2016 – www.caeaccess.org

Performance Analysis of Neighbor Discovery and Location Verification (NDLV) Scheme in Mobile Ad Hoc Networks against Adversarial Nodes

E. Gnanamanoharan
Assistant Professor
Department of Electrical Engineering
Annamalai University

R. Bensraj
Assistant Professor
Department of Electrical Engineering
Annamalai University

ABSTRACT
A mobile ad hoc network (MANET) is a continuously self-configuring, infrastructure-less network of mobile devices connected without wires. Each node supports the routing process of the communication to improve the overall throughput in entire network. Due random movement neighbor nodes comes into the coverage area of a base station and leaves at every fraction of time, which must be trusted for service handling. Adversary nodes replies with the route discovery phase using false location information with the intension to get participate in the routing process. After gets selected it simply discard the packets received, or manipulate the packets, or else it will never receive the packets because of the false location. This makes considerable amount of performance degradation. Routing algorithms for MANETs usually assume that nodes are cooperative and non-malicious. Hence a adversary or malicious node can easily become an important routing agent and disrupt network operations by disobeying the protocol specifications. The "Neighbor Discovery and Location Verification (NDLV) is a scheme utilized to protect the network from adversary nodes by verifying the location of neighbor nodes to improve performance and efficiency in MANET's. The NDLV Scheme identifies a trusted neighbor nodes by extracting timing, finding location and computing the distance between each pair of nodes. The scheme adapts quickly to location changes when node movement is frequent, yet requires little or no overhead during the periods in which hosts move less frequently. The performance analysis and simulation are carried out to compare with un trusted system based on existing AODV based on the quantitative metrics packet delivery ratio, routing overhead and end-to-end delay. The simulated result helps to understand the performance of NDLV in two different scenarios.

General Terms
Mobile AdHoc Network, Adversarial node attacks.

Keywords
Critical node, adversary node , neighbor attack, reliability, location verification, MANET's performance, Neighbor discovery.

1. INTRODUCTION
In MANET's, Nodes found within the neighborhood are neighbors and, depending on given network configuration and topology, may cooperate in the performance of various tasks including sensing ,data transfer and localization. However, due to open wireless environment attackers have the exemption to perform vicious activities ranging from simple denial of service to sophisticated deception. In the occurrence of attackers to require solutions that let nodes to properly launch their location in spite of attacks feeding false location information and validate the locations of their neighbors, so as to distinguish adversarial nodes announcing false locations. This situation is a chance for the adversarial nodes to misuse the location-based services. By advertise the forged positions, adversaries could bias data gathering processes, attracting network traffic and then discard the data. The verification of node locations is serious issue in wireless environment, and it becomes Specifically challenging in the occurrence of adversaries targeting the performance degradation in the network. An adversarial node could be distinguished efficiently with topological information [2] gathered by NDLV.

2. CLASSES AND IMPACT OF ATTACKS IN MANETs
Security is an essential requirement in the mobile ad hoc networks. Attacks on MANETs can be classified into two classes: active and passive attacks. An active attack attempts to destruct the data being exchanged in the network. Active attacks can be divided further into two types: external and internal attacks. External attacks are carried out by nodes that do not belong to the network. These attacks can be foreclose using well defined encryption techniques or firewalls. Internal attacks mainly by nodes within the network. Adversaries are already part of the network and it is considered as vigorous and difficult to detect compared to external attacks. Adversaries are giving false locations for the RREQ when it receives from a source node and disobey the routing protocol and degrade the network performance[3]. An crucial characteristic of attackers is introducing the delay when forwarding the incoming packets. This is a critical parameter where in the case of time sensitive network application and this type of attacks are further divided in to two types are slow and fast relays. The wormhole attack is a severe attack in ad hoc networks which is particularly challenging to defend against. In a wormhole attack, attacker records packets at one location, tunnel them to another location and retransmits them there into the network. The wormhole attack can form a severe threat in wireless networks, particularly against many ad hoc network routing protocols and location-based wireless security systems.

Communications on Applied Electronics (CAE) – ISSN : 2394-4714
Foundation of Computer Science FCS, New York, USA
Volume 4– No.4, February 2016 – www.caeaccess.org

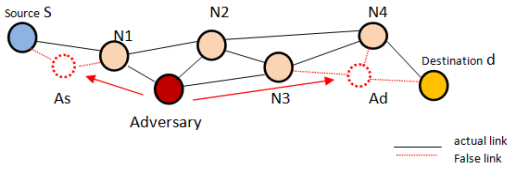

Figure 1. False appearance of adversary node A at positions Ad and As managing to snatch data traffic along the route

A typical example is shown in Figure 1, where adversary node A claims to be at a false locations near source (As) and near destination (Ad). Based on a efficient routing strategy, nodes always select the node nearest to the destination as the next neighbor node. Assuming that source S would like to send a data to node destination d, it will first send the packet to its direct neighbor N1. N1 will then forward the packet to the node nearest to the destination from which it received RREP. This seems to be Ad, so the packet ends up at node A, which can now forward, modify or discard it at will. Without node A faking its position, node N2 would have been selected. So A is able to intercept all upcoming traffic along the route. When A fakes an additional position Ad and As, thus creating a virtual clone of itself, the same argument holds for the opposite direction, so A is even able to capture all traffic in both directions using the false location As. The figure portrays the actual network topology with black edges, while the modified topology, induced by the false location announced by A, is shown with dashed red edges. It is evident that the displacement of A to false location Ad and As causes its edges with the other nodes to rotate and edge length will be modified[2]. Consequently, to prevent such attacks need to identify the false location and refrain from using these nodes as forwarders.

3. RELATED WORKS

In a mobile ad hoc network without knowing neighbor node position which make a chance to attackers to easily enter into the network.. However, such a process can be easily abused or disrupted by adversarial nodes. In absence of a priori trusted nodes, the discovery and verification of neighbor positions presents challenges that have been scarcely investigated in the literature [1]. A mechanism called packet leashes to detecting and defending against wormhole attacks is proposed in [16]. A number of trust-based protocols for mobile ad hoc networks (MANETs) and wireless sensor networks have been proposed. In [3], the authors proposed a secure routing solution to find an end-to-end route free of malicious nodes with the collaborative effort from the neighbors.

Neighbor position verification was studied in the context of ad-hoc and sensor networks; however, existing NPV schemes often rely on fixed [5], [6] or mobile [7] trustworthy nodes, which are assumed to be always available for the verification of the positions announced by third parties. In [8], an NPV protocol is proposed that first lets nodes calculate distances to all neighbors, and then commends that all triplets of nodes encircling a pair of other nodes act as verifiers of the pair's positions[2]. 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 neighbor verification[18].The approach in [9] forces a node to collect several data on its neighbor 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[2].

4. NEIGHBOR DISCOVERY AND LOCATION VERIFICATION

A Neighbor Discovery and Location Verification (NDLV) is used to discover and verify the location of the neighbors.. In a mobile ad hoc network without knowing neighbor node location which makes a chance to attackers to easily enter into the network. If neighbor discovery and location verification done in separate node, then it would be a time consuming process. The NDLV scheme is projected for dynamic ad hoc environments without presence of a trusted infrastructure. It needs cooperation but allows any node to perform location verification at any as shown in Figure 2. It is reactive, lightweight and low control overhead can be executed by any node, at any point in time and robust against independent and colluding adversaries[2]. simulation results confirm that the solutions is effective in identifying nodes claiming false location but unlikely presence of fully collinear network topologies, can degrade the effectiveness of our NDLV. Here four set of messages are exchanged given below.

POLL message: Poll message is anonymous and it is broadcasted from source (verifier) to all nearby (1 hop) neighbor nodes The identity of verifier kept covered and Poll message contains fresh software generated MAC is sent along with public key (one time use key) and transmission time as shown in Fig.4.

REPLY message: In reply message from all neighbor nodes receiving the POLL message will broadcast REPLY message after a time interval with a freshly generated MAC is. This also internally stores the transmission time. It contains some encrypted message with public key. This message is called as commitment of neighbor.

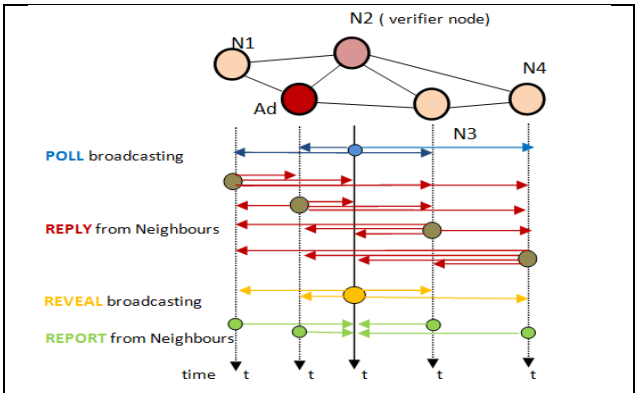

Figure 2. Message sequence chart of NDLV execution

REVEAL message: The REVEAL message broadcasting is completed by using Verifier's real MAC id and make it visible to neighbors. It contains a representation, a proof that verifier is only the generator of the original POLL and the verifier identity, i.e., its certified public key and signature. i.e., its certified public key and digital signature.

REPORT message: In this The REPORT carries neighbor's position, the transmission time of neighbor's REPLY, and the

Communications on Applied Electronics (CAE) – ISSN : 2394-4714
Foundation of Computer Science FCS, New York, USA
Volume 4– No.4, February 2016 – www.caeaccess.org

list of pairs of reception times and temporary identifiers referring to the REPLY broadcasts received. The identifiers are obtained from the map incorporated in the REVEAL message. And Also, neighbor discloses its own identity by including in the message its digital signature and certified public key.

The NDLV messages are relatively small in size that include headers with 4B sender and receiver MAC id's and 1B message type field, POLL(26B), REPLY(71B), and REVEAL(67B). The REPORT on the number of nodes data it carries.

the font named Computer Modern Roman. On a Macintosh, use the font named Times. Right margins should be justified, not ragged.

4.1 Neighbor Discovery

Neighbor discovery is started with exchange of HELLO messages periodically RREQ packets since any node has no the prior knowledge regarding total number of nearby nodes within the given transmission range in the network. The communications neighbors are discovered and validate it.

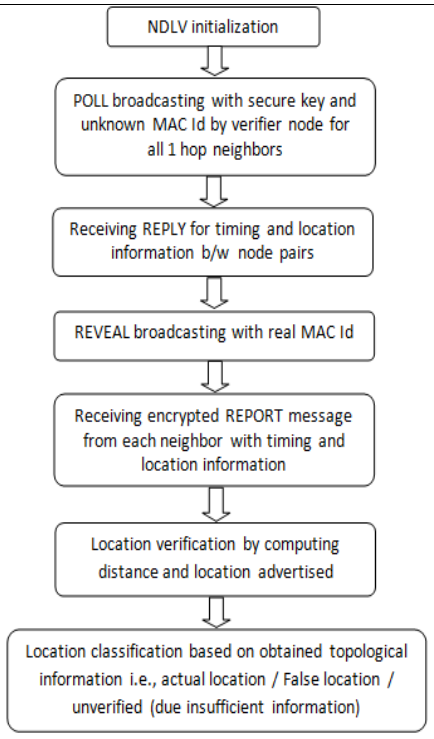

Figure 3. Computational flow Of NDLV

When a new node enters or leave the range they are updated. while updating also the same verification processes are done. The overall computation flow of the NDLV scheme can be understood by Figure 3.

```
Agent/MessagePassing/Flooding instproc send_message
{size key_id data dest} {    $self instvar HASH_KEY node_
global ns MESSAGE_PORT BROADCAST_ADDR
lappend HASH_KEY $key_id
$ns trace-annotate "[$node_ node-addr] sending PublicKey
$data $dest"  $self sendto $size "$key_id:$data"
$BROADCAST_ADDR $dest }
# Creating Public Key For Every Node
for { set i 1 } { $i<=46 } { incr i } {
set keyfile($i) [open key8($i).tr a+]
set key [expr int(rand()*5000)]
puts $keyfile($i) "$key"
puts "Public Key of Node $i $key"}
set secret1 [expr int(rand()*2000)]
set secret2 [expr int(rand()*2000)]
puts $keyfile(6) "$secret1"
puts $keyfile(6) "$secret2"
puts "Secret Key Pair $secret1"
puts "Secret Key Pair $secret2"
seek $keyfile(6) 0 start
gets $keyfile(6) line
for { set i 1 } { $i <=30 } { incr i } {if { $i==6 } { } else {puts
$keyfile($i) "$line" }  close $keyfile($i) }
```

Figure 4. High level description of the node discovery and trust initialization algorithm

4.2 Location verification and classification

Any node considered as verifier can initiate discovering neighbor nodes and verifies the location of its direct neighbors in the network. A verifier Provoke the protocol by generating the sequential message exchange within its one hop neighborhood. The target of the message exchange is that the verifier collects information to compute distances between any pair of nodes. The POLL and REPLY messages are broadcasted by the verifier and its neighbors, permitting nodes to record mutual timing information without revealing their identities. After that a REVEAL broadcast by the verifier, nodes reveal to verifier through secure and authenticated REPORT messages, their identities as well as the unknown timing information they collected[2]. The verifier utilizes the data to check timings and identities and compute distances between all pairs of one hop nodes in its neighborhood. Once the verifier computes the distances it runs location verification tests in order to classify the locations are Actual (Correct) Location: the verifier declare that the node is at the claimed location. False (Incorrect) Location: the verifier declare that the node is in an false location. Unverifiable: the verifier declare that the node is either in actual or false location due to lacking of acquired topological information.

The main objective of verification tests is avoiding false negatives (i.e., adversaries at fake location declared as actual) and false positives (i.e., Node at actual location is declared as false), as well as at reducing the number of unverifiable nodes. It also allows the verifier to independently classify its neighbors.

Communications on Applied Electronics (CAE) – ISSN : 2394-4714
Foundation of Computer Science FCS, New York, USA
Volume 4– No.4, February 2016 – www.caeaccess.org

5. ADVERSARY MODEL

We consider a adversary model which consists of adversary nodes (or compromised) nodes that are deployed after the setup phase of the network. Attackers have the ability to collude. Whereas an outsider attacker is not a legitimate user of the network, an insider attacker is an authorized node and a part of the routing mechanism on MANETs. While an insider MANET node can disrupt the network communications intentionally, there might be other reasons for its apparent misbehaviors. Specially we will focus on AODV as an exemplar protocol in this work. Since adversary nodes need to be on a routing path to drop data packets, they have little reason to drop routing protocol control packets such as RREQ, RREP, and RERR messages used in route discovery and maintenance mechanisms of AODV.

6. PERFORMANCE EVOLUTION

We describing simulation methodology and configuration as well as comparing performances through simulation and results are compared with un trusted system.

6.1 Simulation Methodologies

The performance of NPV is tested under two different scenario depends on variation in the transmission range of each node since its important parameter in the exchange of message between 1 hop neighbor (within the transmission range) also the neighborhood of the adversary in random network setup and they are located by two different connection pattern random to observe and realize their behavior. The Network setup considers the packet transfer and transmission range. We assume the adversaries are equipped with Omni directional antenna and single radio interfaces. For the evaluation of the NDLV, we fixed the transmission range of each node is 150 m and 300 m in two different scenarios respectively. The definitions and formulas for Node Coverage (Area covered by a node transmission is characterized) and Foot print (Percentage of the simulation area covered by a node's transmission range) given by eqn (1) and (2)

$$\text{Node Coverage} = \pi r^2 \quad (1)$$

$$\text{Foot print } A = (\pi r^2) / (w \times h) \times 100 \quad (2)$$

Where w = width, h = height of the topology (simulation area) , r = transmission range. The average number of neighbor nodes accounting for the edge of the simulation area reducing the node's coverage. For example, a node in the corner of the simulation area only has neighbors in 25% of its coverage area.

Scenario 1: In this scenario, The transmission range of 150 m for each node is fixed and available number of one hop neighbor are increased. Nodes are being located at random position. Nodes are moving at constant speed.

Scenario 2: In this scenario, The transmission range of 300 m for each node is fixed and available number of one hop neighbor are reduced. Nodes are being located at random position. Nodes are moving at constant speed.

6.2 Simulation Configurations

The simulation is carried out with the Network Simulator (NS) 2.34 event driven open source software on a platform with and Ubuntu 9.10. The system is running on a laptop with Intel(R) Core(TM) i5 2450 CPU and 8-GB RAM. Network Simulator (NS-2.34) which is compiled of two languages: C++ and TCL. First of all, we define the simulation in the 1,500 m×1,500 m region, random waypoint mobile model, network setup consists of 100 nodes are CBR data sources placed randomly and transmission range of 150 m and 300 m moves at constant speeds of 1 m/s.

The propagation model is two-ray ground reflection models and random waypoint model is used for the mobility model. provides other simulation parameters. The mobile node chooses a random destination in the simulation area and the adversarial nodes were uniformly distributed over the whole network. Each simulation run takes 60 simulated seconds.

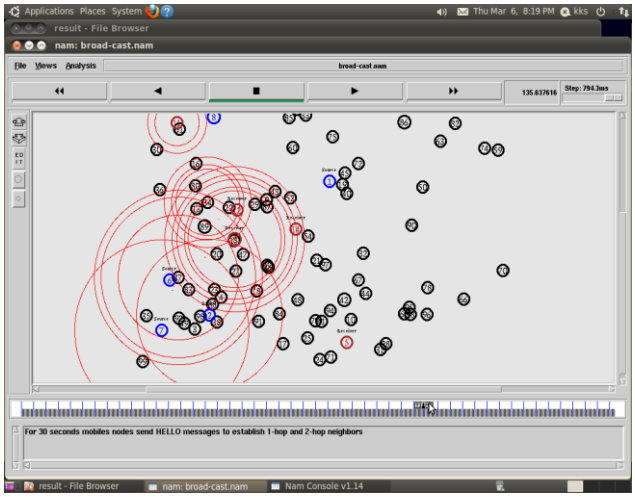

Figure 5. Simulation window

The source 6 sends the packets to node 12 and another source 2 sends the packet to node 12. So the data packets start dropping from node 7 as shown in Fig. 5. The node 15 and 20 is declared as adversary advertised from false locations. In order to compare and analyze the performances of NDLV with existing system ,we continue to acquire the following three performance metrics [13].

6.3 Performance metrics

6.3.1 Packet delivery ratio (PDR):

PDR defines the ratio of the number of packets received by the destination node to the number of packets sent by the source node.

6.3.2 Routing overhead (RO):

RO defines the ratio of the measure of routing-related control messages [Route Request (RREQ), Route Reply (RREP), Route Error (RERR),ACK, POLL,REPLY,REVEAL and REPORT]. The average number of transmitted control bytes per second, including both header of the data packets and the control packets.

6.3.3 End to End Delay:

The average time elapsed for delivering a data packet within a successful transmission from source to destination.

6.4 Experimental Results

In this section the experimental results is shown for the NPV and un trusted system. The neighbor position verification protocol is used to for the neighbor discovering and verification in the mobile ad hoc networks.

6.4.1 Packet delivery ratio

Figure 6 and 7 shows the simulation results in scenario 1 and 2 is based on PDR. The Y axis shows PDR of received packets by destination node and the X axis shows number of adversarial nodes. The red line of the graph represents the performance of NDLV.

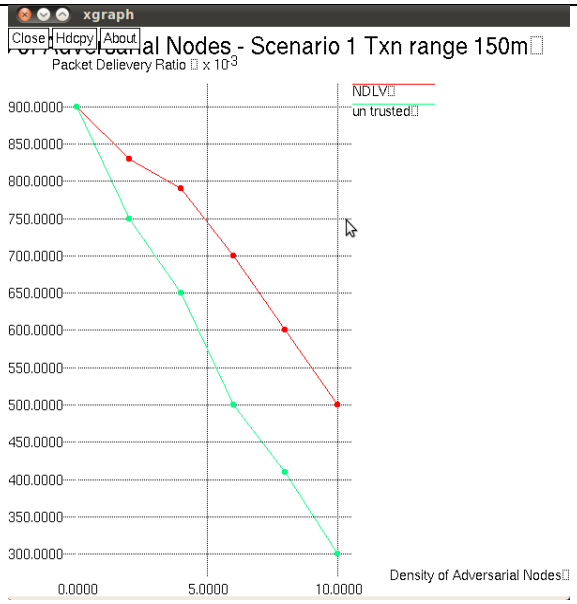

Figure 6. PDR in scenario 1

The green line of the graph shows the performance of un trusted system. Note that the PDR decreases as the number of adversarial nodes increase. The reduction in PDR is mainly due to presence of adversary along the route and more possibility to pick up packets and discard them packets received. When their numbers increase further, they will inevitably discard the packet, therefore, failing to deliver more number packets. But the packet delivery ratio in NDLV is perform better than the un trusted system presence of adversarial nodes approximately 10% in the network.

In scenario 2, By increasing transmission range from 150 m to 300 m, the number of data packets dropped and PDR is gradually decreased when the neighbor nodes are communicating with each other, the packets will move between node pairs. From the results, we conclude that the NDLV is able to detect misdeeds with number of adversarial nodes from false location.

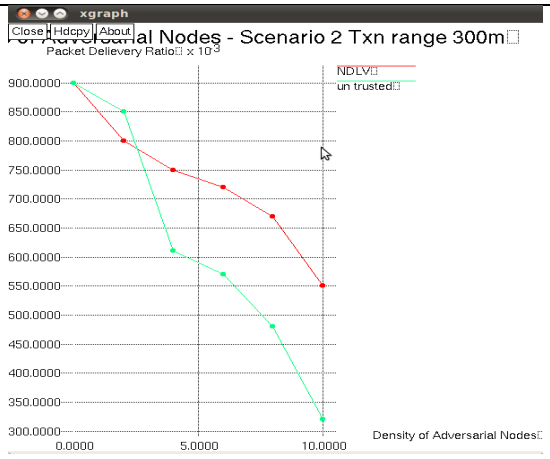

Figure 7. PDR in scenario 2

6.4.2 Routing Overhead:

The simulation results of RO in scenario 1 and 2 is shown in Figure 8 and 9.We observe that NDLV and un trusted system has very less routing overhead with presence of very few adversaries as they do not require much computation. However, RO rises suddenly with the increase of adversary. The results on attacks targeted at discrediting the location of other nodes are omitted, since they are very close verifier. The plot only accounts for number of adversary nodes variations and transmission range. The routing overhead in NDLV protocol is moderate than that of a basic un trusted system of neighbor position discovery, consisting of only one poll and associated position replies from neighbors. In scenario 2, By increasing transmission range from 150 m to 300 m, RO rises gradually more than basic un trusted system of neighbor position discovery due to large number of control packets compare with pay load. The plot only considers for transmission range differences in the simulated scenario 1 and 2. and the NDLV 's overhead is similar to that of the un trusted system for both transmission ranges.

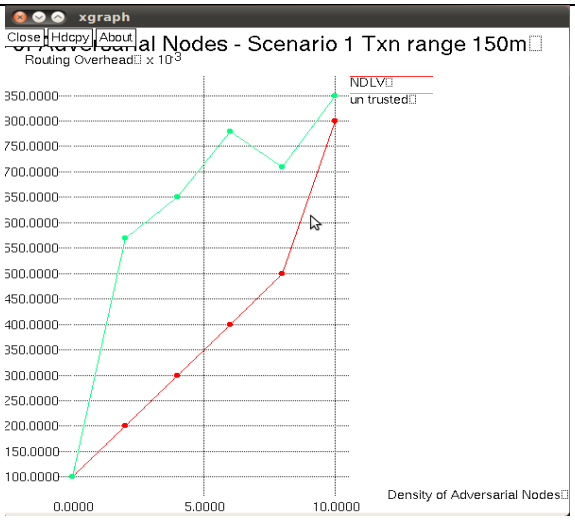

Figure 8. Routing Overhead in scenario 1

Communications on Applied Electronics (CAE) – ISSN : 2394-4714
Foundation of Computer Science FCS, New York, USA
Volume 4– No.4, February 2016 – www.caeaccess.org

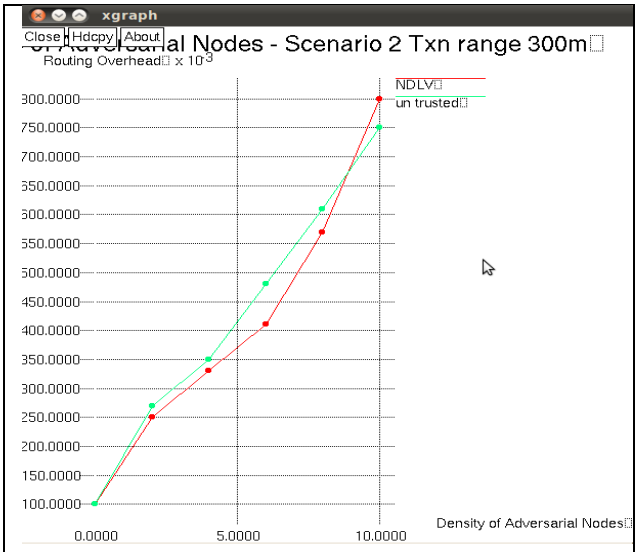

Figure 9. Routing Overhead in scenario 2

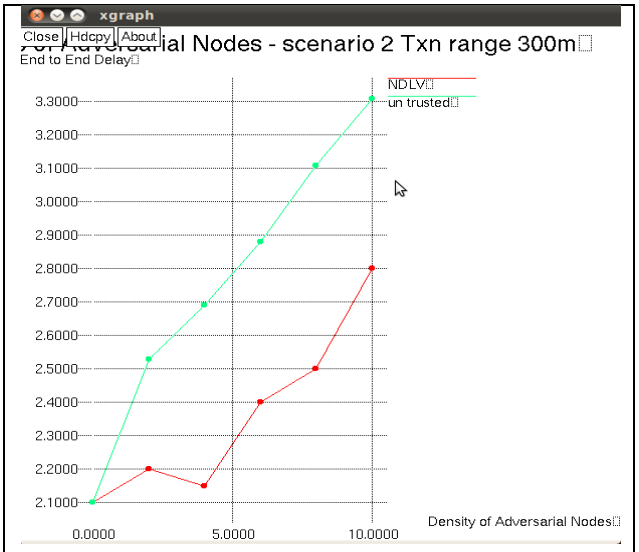

Figure 10. End to End Delay in scenario 1

6.4.3 End to End Delay:

Figure 10 and 11. Shows the simulation results that are based on end to end delay . There are possible delays caused by bandwidth, throughput, average number of node receiving delay between node pairs and presence of adversarial nodes etc. The reduction in end to end delay is the better performance in the network. We observe that NDLV very less end to end delay compare with un trusted system.

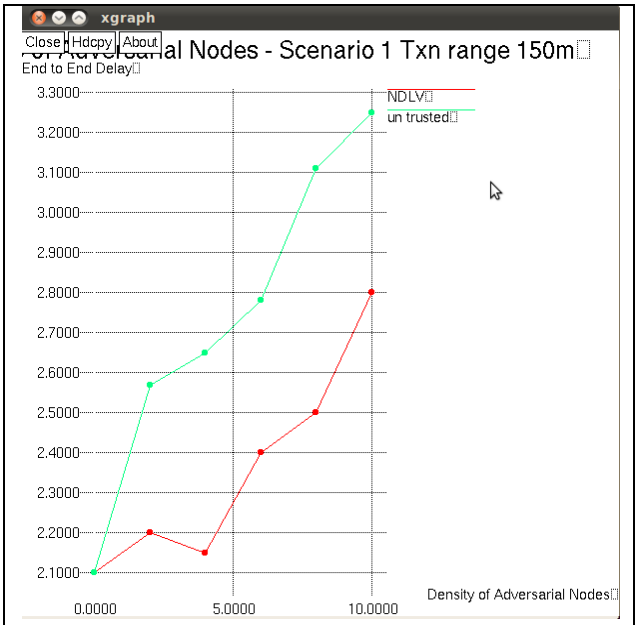

Figure 11. End to End delay in scenario 2

Since the adversarial nodes has been increased, the delay is increased gradually in the both scenarios and at the same time as the difference tends to increase for lesser transmission ranges in the scenario 1.

7. CONCLUSION

A new scheme NDLV is tested with large number of nodes with presence of adversary nodes approximately 10 % at two different scenarios for neighbor discovery and location verification. Its performance has been evaluated through simulation and the metrics computed. The graphs have been projected to realize the efficiency of the new algorithm. It has been identified from the graphs that NDLV introduces moderate routing overhead compare with un trusted system. It shows clearly that little more routing overhead when increased the frequency of location verification and classification. It allows any node and at any time instant in a network to verify the location of its neighbors without relying any additional mechanism also is less time consuming so that even if more number of adversaries present in the network. It has been constructed to extract the improved performance with increased PDR, minimum routing overhead and minimum delay. and its suitability for present day applications in real time networks. The plot only accounts for density of adversary node with two different transmission range and other parameters do not have an impact on the metrics. In future work, need to have a more extensive analysis of the protocol with different mobility speed with different scenario.

8. ACKNOWLEDGMENTS

The authors thank the authorities of Annamalai University for providing the necessary facilities in order to accomplish this piece of work.

9. REFERENCES

[1] P. Papadimitratos, M. Poturalski, P. Schaller, P. Lafourcade, D. Basin, S.Capkun, J.-P. Hubaux, " Secure Neighborhood Discovery: A Fundamental Element for Mobile Ad Hoc Networks," IEEE Comm. Mag., vol. 46, no. 2,Feb. 2008.

[2] M. Fiore, C. Casetti, C.-F. Chiasserini, P. Papadimitratos, "Secure Neighbor Position Discovery in Vehicular Networks," IEEE/IFIP Med-Hoc-Net, Favignana, Italy, June 2011.

[3] T. Ghosh, N. Pissinou, and K. Makki, "Collaborative trust-based secure routing against colluding malicious

nodes in multi-hop ad hoc networks," Annual Conference on Local Computer Networks (LCN), pp.224-231, Tampa, USA, 2004.

[4] T. Ghosh, N. Pissinou, and K. Makki, "Towards designing a trusted routing solution in Mobile Ad Hoc networks," ACM Journal, Mobile Networks and Applications (MONET), Special issue on NonCooperativeWirelessNetworking and Computing,2005.

[5] E. Ekici, S. Vural, J. McNair, D. Al-Abri, "Secure Probabilistic Location Verification in Randomly Deployed Wireless Sensor Networks," Elsevier Ad Hoc Networks, vol. 6, no. 2, pp. 195-209, 2008.

[6] J. Chiang, J. Haas, Y. Hu, "Secure and Precise Location Verification Using Distance Bounding and Simultaneous Multilateration," ACM WiSec, Zurich, Switzerland, Mar. 2009.

[7] S. Capkun, K. Rasmussen, M. Cagalj, M. Srivastava, "Secure Location Verification with Hidden and Mobile Base Stations," IEEE Trans. on Mobile Computing, vol. 7, no. 4, pp. 470–483, 2008.

[8] S. Capkun, J.-P. Hubaux, "Secure Positioning in Wireless Networks," IEEE JSAC, vol. 24, no. 2, pp. 221–232, 2006.

[9] T. Leinmuller, C. Maih¨ofer, E. Schoch, F. Kargl, "Improved Security in Geographic Ad Hoc Routing through Autonomous Position Verification," ACM VANET, Los Angeles, CA, Sept. 2006.

[10] A. A. Pirzada, and C. McDonald, "Establishing trust in pure Ad-hoc networks," The 27th Australasian Computer Science Conference, Dunedin, New Zealand, 2004.

[11] N. Pissinou, T. Ghosh, and K. Makki, "Collaborative trust-based secure routing in multihop Ad Hoc networks," The Third IFIP-TC6 Networking Conference (Networking '04), Athens, Greece, 2004.

[12] S. Yi, P. Naldurg, and R. Kravets, Security- Aware Ad hoc Routing for Wireless Networks, UIUCDCS-R-2001-2241, Aug. 2001.

[13] M. Poturalksi, P. Papadimitratos, J.-P. Hubaux, "Towards Provable Secure Neighbor Discovery in Wireless Networks," Workshop on Formal Methods in Security Engineering, Alexandria, VA, Oct. 2008.

[14] E. Ekici, S. Vural, J. McNair, D. Al-Abri, "Secure Probabilistic Location Verification in Randomly Deployed Wireless Sensor Networks," Elsevier Ad Hoc Networks, vol. 6, no. 2, pp. 195-209, 2008.

[15] J. Chiang, J. Haas, Y. Hu, "Secure and Precise Location Verification Using Distance Bounding and Simultaneous Multilateration," ACM WiSec, Zurich, Switzerland, Mar. 2009.

[16] Y.-C. Hu, A. Perrig, D. B. Johnson, "Packet Leashes: A Defense against Wormhole Attacks in Wireless Networks," IEEE Infocom, S. Francisco,CA, Apr. 2003.

[17] R. Maheshwari, J. Gao, S. Das, "Detecting Wormhole Attacks in Wireless Networks Using Connectivity Information," IEEE Infocom,Anchorage, AK, Apr. 2007.

[18] R. Shokri, M. Poturalski, G. Ravot, P. Papadimitratos, J.-P. Hubaux,"A Practical Secure Neighbor Verification Protocol for Wireless Sensor Networks," ACM WiSec, Zurich, Switzerland, Mar. 2009.