Literature Review on Neighbor Position Verification in Mobile Ad Hoc Networks

Balaji P[1] Gopinathan B[2]
[1]P.G Scholar [2]Associate Professor
[1,2]Department of Computer Science & Engineering
[1,2]Adhiyamaan College of Engineering, Hosur-635 109, Krishnagiri (Dist), Tamilnadu, India

Abstract— In mobile Ad hoc networks, the adversarial nodes can easily attack the networks. These adversarial nodes affect the performance in networks. So it is more important to identify the neighbors in MANET. Neighbor discovery and position verification is an important part of mobile Ad hoc networks. The mobile nodes required to identify and verify the neighbor's position which minimizes the adversary attacks. In this survey paper, various approaches are discussed for the neighbor discovery and position verification.

Key words: Adversaries, Mobile Ad hoc networks, Neighbor position verification

I. INTRODUCTION

Mobile Ad hoc network is an infrastructure-less network and it's a self-configuring network of mobile routers connected by wireless links. In mobile Ad hoc network every device is absolve to move in any direction. This sort of network changes is links often to different devices and data should be routed via intermediate nodes. A mobile ad-hoc network is an ad-hoc network however an ad-hoc network isn't essentially a MANET. MANET is especially used in Military environments, Emergency operations, and in space application.

MANET is a continuously self-configuring, infrastructure-less network of mobile devices connected while not wires. Ad hoc is from Latin and means "for this purpose". Every device in a MANET is unengaged to move severally in any direction, and can thus amendment its links to different devices often. Every device should forward traffic unrelated to its own use, and thus be a router. The primary challenge in building a MANET is arming every device to continuously maintain the data needed to properly route traffic. Such networks could operate by themselves or could also be connected to the larger internet. They will contain one or multiple and completely different transceivers between nodes. This ends up in a extremely dynamic, autonomous topology.

The node discovery and location verification is a vital issue in mobile Ad hoc networks, and it becomes difficult within the presence of adversaries aims at harming the system. The neighbor nodes should be always trusty nodes or else the adversarial nodes will easily attack the networks. In order to discover and verify the neighbor nodes numerous techniques are proposed.

II. LITERATURE REVIEW

Neighbor discovery is a fundamental building block of networking protocols, determines that devices are within direct radio communication. It deals with the identification of nodes during which the communication link is established at intervals a given vary. Neighbor position verification is mainly used to verify the position of its communication neighbors. Verifying the location is an effective protection against attacks. Several techniques are used for secure location verification.

A. Intelligent AODV:

Mobile Ad hoc Networks (MANETs) have opened a replacement window for recent concepts and thoughts to be born-again to reality and to help in creating higher use of mobile communication enforced with mobility models. For example, vehicular Ad hoc Networks (VANETs), a subset of MANETs, is employed in vehicular connectivity like Car-to-Car and Car-to-Internet and Infrastructure. Ad hoc On-Demand Distance Vector (AODV) is one in all the Ad hoc routing protocols utilised in MANET and VANET. Ad hoc routing protocols are classified into Table- driven routing protocol and On-demand routing protocol. On-Demand routing protocols notice their destinations supported the method of flooding a request to neighbors searching for their destinations. Neighbor nodes are detected supported the neighbor discovery methodology, that broadcasts HELLO messages to observe available neighbors. Generating routing packets and neighbor discovery messages produce high overhead within the On-Demand routing protocol, like AODV and so as to overcome such problems, Intelligent-AODV (I-AODV) [1] is proposed.

Figure 1, demonstrates the overhead caused by HELLO messages with the idea that each one HELLO messages are sent at single HELLO intervals. based on the I-AODV theory, if the destination node of the HELLO message is checked among neighbors on an inventory and is found to possess active HELLO time, I-AODV doesn't send HELLO message to it destination, that means it filters the broadcasting HELLO message. The distinction in HELLO message overhead is illustrated in Figure 2, wherever a HELLO message is barely sent to a destination that's not within the neighbor list. This distinction will give less routing packets and thus, higher normalized routing load. In fact, I-AODV will deliver data to its destination by finding a shorter, new route entry with fewer routing packets.

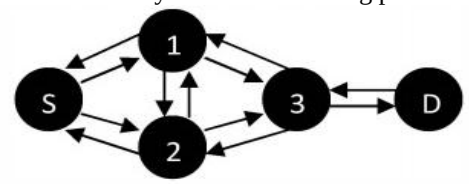

Fig. 1: Original AODV HELLO Message Overhead

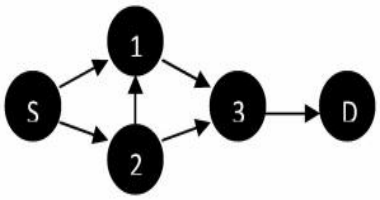

Fig. 2: I-AODV HELLO Message Overhead

Neighbors are recognized and added to the neighbor list once after sending an ACK to the hello message sender. The neighbor node's data is employed in flooding RREQ and as a place to begin for the data delivery route to destination. In I-AODV, RREQ and RREP headers are checked to match header data with the routing table. This helps determine newer shorter routes to destination. Thus, I-AODV will smartly identify neighbors whereas sending and receiving RREQ and RREP. This implementation permits the protocol to get neighbor nodes quickly and utilize neighbor node data within the route discovery method. The fact that mobile nodes are designed with mobility is a plus notably in MANET. However, I-AODV is far better behaved in such situations involving mobility.

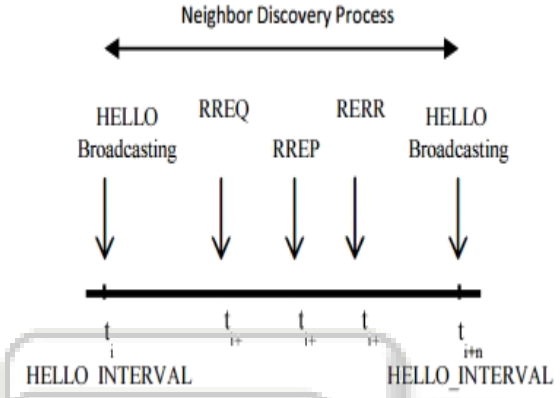

Fig. 3: I-AODV Additional Neighbor Discovery Overview

Figure 3, displays a summary of the notion that RREQ and RREP are used for neighbor discovery. I-AODV is ready to acknowledge a replacement neighbor before or after hello Timer. this suggests that I-AODV checks RREQ and RREP sequence numbers and hop counts whereas comparison them with route entries within the routing table, then checks whether or not the corresponding node is found within the neighbor list; if not, that node is considered a neighbor. By victimization I-AODV, there's still an opportunity of finding neighbors using RREQ and RREP next node's data assumptive there's no neighbor discovery functioning within the protocol.

B. Neighbor Assisted Route Discovery (NARD):

Reactive routing protocols for mobile ad-hoc networks sometimes discover routes by spreading management packets across the whole network; this system is thought as brute-force flooding. NARD stands for Neighbor Assisted Route Discovery Protocol [2] for mobile ad-hoc networks. In NARD, a source node floods just for a restricted portion of the network looking not only for the destination node, however also for the routing information that is related to different nodes that were close to the destination node recently. Destination-neighbors are often used as anchor points wherever a second restricted flooding takes place in search for the destination node. Because, only two limited parts of the network are flooded by control packets close to the source and destination nodes, nard will scale back signaling overhead due to route-discovery.

NARD operation consists by neighbor discovery part. The neighbor discovery part is performed by a node with the aim of determinative the identity of its one-hop neighbors. The identity is such that by a 2 tuple containing the ip and mac address. This data is collected by suggests that of two possible procedures. The primary one is to overhear packets from communications happening within the neighborhood. To this end, a node will set its transceiver in promiscuous mode. It's value remarking that the over-heard packets will be originated by a finish point of a connection or forwarded by relay nodes. Because of this reason, from this procedure, a node is just capable of getting the mac addresses of relay nodes in its neighborhood. However, their corresponding ip addresses will be found by a mechanism just like the one utilized in the RARP protocol. The second procedure will be used, once a node has not transmitted information packets for a while. During this procedure, a node transmits a particular management packet referred to as hello, so its current neighbors will be alert to its presence and full identity. The signal overhead because of hello packets is negligible as a result of they're little and aren't retransmitted by alternative nodes. HELLO packets might not be continually necessary. The speed of hello packets transmitted by every node is also constant and independent of the network size. A node also can control the speed of hello packets in step with its own wants. A node will even stop sending hello packets if it's not expecting any connection with alternative nodes within the close to future.

In this protocol, nodes collect and store neighbor information in Neighbor Tables (NTs). These tables are changed between the end points of a connection when it's created. During this work, the term connection refers to any wireless information transfer using either a connection orientated (TCP) or a connectionless (UDP) communication. Nodes store their own neighbor tables, and alternative neighbor tables acquired whereas communication with alternative nodes. Figure 4, illustrates however the neighbor-discovery part works and the diagram depicts the two finish points of affiliation, i.e., nodes A and B. This connection has been antecedently discovered using nard and it's mainly used to transfer message from A to B. These nodes exchange their corresponding neighbor tables (NTA and NTB), by attaching them to message packets.

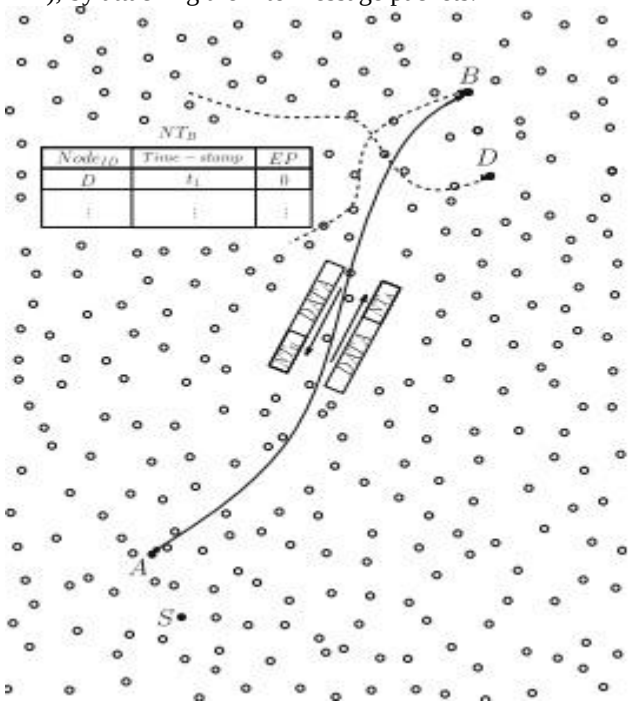

Fig. 4: Neighbor Discovery Phase

After the end points of a connection have changed their neighbor tables, these tables will be updated by coverage their changes only, e.g., entries recently created or changed. Obviously, there's a trade-off between the rate of those updates and therefore the increase on signal overhead due to this procedure. The most purpose of nard is to reduce the signal overhead due to the route discovery procedures therefore the rate of updates should be adjusted in line with specific needs.

When the end points exchange their neighbor tables, they conjointly record some extra data regarding the route accustomed transfer them. Such message considers the quantity of nodes on the route and therefore the time once the table exchange came about. This data are accustomed estimate whether or not or not the route remains valid at a later purpose in time.

C. Mobile Secure Neighbor Discovery (MSND):

Neighbor discovery could be a most significant part of several protocols for wireless Ad hoc networks. If neighbor discovery fails, communications and protocols performance decreases. The networks suffering from relay attacks also are referred to as wormholes. The wormhole by selection degrades the communications. The Mobile Secure Neighbor Discovery (MSND) [3] is employed, that offers a measure of protection against wormholes by permitting taking part mobile nodes to firmly verify if they're neighbors. To the most effective of data, this work is that the initial to secure neighbor discovery in mobile Ad hoc networks. MSND leverages ideas of graph rigidity for wormhole detection. It proves security properties of protocol, and demonstrates its effectiveness through intensive simulations and a true system analysis using Epic motes and iRobot robots.

The MSND protocol is predicated on the intuition that once nodes vary whereas moving, the length of ensuing vary is expounded to the distance traveled between consecutive ranges. Since the wormhole is unable to understand the distance traveled by node.

When two nodes travel along expressible ways, it's possible to outline one node's line of travel relative to the other. The lines of travel might converge, diverge or be parallel. When two ranges, there's a time of doable relationships between the 2 ways. Three ranges limit the quantity of relative ways to a number of distinct eventualities whereas four or a lot of produce a rigid graph. During this rigid graph, it's possible to accurately estimate the expected lengths of following ranges and compare them to the particular ranged worth.

In this same movement situation, a wormhole induces distortion due to its position relative to the lines of travel of every node. Once no wormhole is present, a ranging signal travels directly from the sender to the receiver. However, within the presence of a wormhole, the ranging signal should travel from the sender to the close to side of the wormhole, transit the wormhole, then travel from the distant side of the wormhole to the second node. If ranging nodes were static, this distortion would be not possible to discover with solely 2 nodes. However, quality causes the distance between every node and its associated end of the wormhole to vary. this transformation in distance ($r_i = r'_i + r''_i$), and interprets to ranges that are longer than expected, and to pairs of consecutive ranges whose lengths vary by over expected within the rigid graph made by the nodes movements.

D. Verifiable Multilateration (VM):

The verifiable multilateration (VM) [4] mechanism is employed to secure positioning. This mechanism relies on the measurements of the time of radio wave propagation. VM mechanism is principally employed in device network positioning. Multilateration could be a technique for deciding the position of a mobile device from a collection of reference points whose positions are identified, supported the ranges measured between the reference points and therefore the device. The position of the device in two dimensions may be computed, if the device measured, its distance to three reference points. The distance estimation techniques are prone to attacks from internal and external attacks, which may modify the measured distances. Multilateration is equally prone to a similar set of attacks as a result of it depends on distance estimations. The VM algorithmic rule is executed by the verifiers, and therefore the steps in VM algorithmic rule are,

- In step one of the algorithm the verifiers that are within the power vary of the applier perform distance bounding to the applier and procure distance bounds. These distance bounds, additionally because the positions of the verifiers are then reportable to the central authority.
- In step two, the authority computes an estimate of the claimant's position; this position is computed by using distance bounds from all verifiers in neighbourhood, generally by the minimum mean square estimate (MMSE).
- In step three, the authority runs the following 2 tests: 1) delta test- for all verifier, will find the space between x, y and verifier disagree from the measured distance certain by less than the expected distance measure error and 2) point within the triangle test- will x, y fall at intervals a minimum of one physical tri-angle shaped by a triplet of verifiers. Note additionally that they call Triangulum shaped by the verifiers the verification triangle. If each the delta take a look at and therefore the purpose within the triangle tests the distance positive, the authority accepts the calculable position x, y of the applicant as correct; else, the position are going to be rejected.

Secure Positioning In sensor Networks (SPINE) theme is employed during this mechanism. It secures from 2 kinds of attackers 1. Internal attackers and 2. External attackers. Internal attackers report the false position and external attackers modifies the calculated position. The positioning is completed by 2 sorts a) node-centric and b) Infrastructure-centric. In node-centric positioning system, node computes its positions by observant radio signals with well-known locations. In infrastructure-centric positioning system, infrastructure computes its positions of nodes supported their mutual communications. SPINE secures the positioning in networks supported VM.

E. Trusted Neighbor Table (TNT):

One of the security problems in vehicular ad-hoc network (VANETs) routing: position-spoofing attack. The trusted

neighbor table (TNT) [5] is employed that is predicated on location verification theme to find and prevent position-spoofing attack. The essential plan of this theme is to ascertain TNT for every node to record the most recent location of its neighbors, and every neighbor has a trust value. Since the TNT is trusty, by selecting a next hop from it and considering its trust value will mitigate the influence of falsified position data in geographic routing protocols. Analysis shows that this theme is secure and economical.

The TNT primarily based location verification theme needs every node to keep up TNT to record the newest location of its neighbors. TNT is totally different from this neighbor table. Data in neighbor table is unauthenticated, thus it's not reliable and selecting a next hop from it brings the risk of position spoofing attack. But in TNT, neighbor location data is trusty. And this trust isn't absolute trust; it suggests that the situation data in TNT will make sure the traditional routing method. They quantize this "trust" into trust worth, that is indicated by the sector "r", and $r \in [0,1]$. $r = 0$ is equivalent that this neighbor location data is neutral trust and therefore the larger r suggests that additional trust.

As shown in table 1, TNT contains 6 fields, "No." suggests that the sequence variety of a record, "name" implies a neighbor's name, and therefore the example record one suggests that "neighbor A is in p1 at t1, whereas its driving speed is v, and its trust value is 0.3.

No.	Name	Position	Velocity	Time	R
1	A	p_1	v1	t_1	0.3
…	…	…	…	…	…

Table 1: Trust Neighbor Table

F. Secure Neighbor Position Discovery (SNPD):

For neighbor position verification, SNPD protocol [6] is proposed which is lightweight and it does not rely on presence of trustworthy nodes. Here each node acts as a verifier. Every node does the message exchange protocol and position verification with the neighbor nodes.

1) Message Exchange Protocol:

Every node does message exchange protocol with the neighbor nodes. Message exchange protocol [7] contains various types of messages like Poll, Reply, Reveal and Report messages. The poll message will be sent by the verifier to all neighbor nodes and the nodes will reply to the verifier for that poll message. Now, the reveal message is sent to the neighbor nodes in this message the verifier tells about its identity and the nodes will sent the report message to the verifier which contains some information about its location. The verifier notes the transmission time and reception time of poll message, so that it calculates the distance between the nodes.

2) Position Verification:

After calculating the distance between nodes, the verifier does some of the tests to verify whether the node is verified, faulty, or unverifiable. Verified means the node is in current position, faulty means the node is in incorrect position so it may be an adversarial node and unverifiable means the node may be correct or unverifiable. The tests are direct symmetry test, Cross symmetry test and Multilateration test. In Direct symmetry test, the both side distances between the verifier and nodes should not exceed twice the ranging error. If the value exceeds, it is noted as faulty. In Cross symmetry test, the verifier will cross check the information between two nodes. In Multilateration test, the faulty nodes will be avoided then verifier lists only the verified nodes and points the distances in the graph. The distance points will be drawn in the graph and it should give a hyperbolic curve.

All the nodes verify the neighbor node so it is easy to verify the verified node. By this approach the SNPD protocol is robust against the colluding adversaries it prevents more than 99 percent of the attacks from the adversaries.

III. CONCLUSION

In this paper, several approaches for neighbor discovery and position verification is explained. The approaches contain some merits and demerits, while discovering and verifying the neighbor nodes. This paper provides a comparison of the approaches and gives the opportunities for future research.

REFERENCES

[1] Mostajeran. E, Md Noor. R, and Keshavarz. H, "A novel improved neighbor discovery method for an Intelligent-AODV in Mobile Ad hoc Networks," International Conference of Information and Communication Technology (ICoICT), Mar. 2013.

[2] Gomez. J, Rangel. V, Lopez Guerrero. M, and Pascoe. M, "NARD: Neighbor-assisted route discovery in MANETs," SPRINGER Wireless Networks, Volume 17, Issue 8, pp 1745-1761, Nov. 2011.

[3] Stoleru. R, Wu. H, and Chenji. H, "Secure Neighbor Discover in Mobile Ad hoc Networks," proc. Eighth IEEE Int'l conf. Mobile Ad-Hoc and Sensor Systems, Oct. 2011.

[4] Capkun. S and Hubaux. J.-P, "Secure Positioning in Wireless Networks,"IEEE J. Selected Areas in Comm., vol. 24, no. 2, pp. 221-232, Feb. 2006.

[5] Xiaoping Xue, Nizhong Lin, Jia Ding, and Yiwen Ji, "A trusted neighbor table based location verification for VANET Routing," Wireless, Mobile and Multimedia Networks (ICWMNN 2010), IET 3rd International Conference, Sept. 2010.

[6] Fiore. M, Casetti. C, Chiasserini. C.-F, and Papadimitratos. P, "Secure Neighbor Position Discovery in Vehicular Networks," Proc. IEEE/IFIP 10th Ann. Mediterranean Ad hoc Networking Workshop (Med-Hoc-Net), June 2011.

[7] Marco Fiore, Claudio Ettore Casetti, Carla-Fabiana Chiasserini & Panagiotis Papadimitratos 2013, 'Discovery and Verification of Neighbor Positions in Mobile Ad hoc Networks', IEEE Transactions On Mobile Computing, Vol. 12, No. 2.

