Design and Implementation of Efficient Neighbor Route Discovery Protocol [ENRDP] for Position Verification in MANET

Prachee U. Ketkar, Dr. Pradip M. Jawandhiya

P.L.I.T.M.S.,Buldhana

Abstract-Energy awareness and protocol management is becoming an important factor in the design of MANET protocols. Because of mobility, it needs the support of scalable routing strategies. These protocols try to consider the path duration in order to respect some QoS constraints and to reduce fake neighbor position for route discovery. In the existing system communication and packet delivery ratio decreases when neighbor discovery fails. The proposed ENRDP protocol selects the stable path to reduce the fake position and communication overhead. It selects the stable path, so neighbor discovery failure decreases and there by increases the packet delivery ratio and reduces energy consumption, End-to-End delay and packet lost. The effectiveness of ENRDP protocol is demonstrated through NS2 stimulation.

Keywords-*MANET, ENRDP, Neighbor discovery, Secure neighbor Discovery, Neighbor position verification.*

*****

I. INTRODUCTION

Wireless Mobile Ad Hoc Networks (MANETs) have emerged as an advanced networking concept based on collaborative efforts among numerous self-organized wireless devices. MANET is a network where no fixed infrastructure exists. Such networks are expected to play vital role in future civilian and military settings, being useful to provide communication support where no fixed infrastructure exists or the deployment of a fixed infrastructure is not economically profitable and movement of communicating parties is possible. The topology of MANETs is dynamic, because the link among the nodes may vary with time due to device mobility, new device arrivals, and the possibility of having mobile devices. Hence, any routing protocol design must consider the physical limitations and constraints imposed by the ad hoc environment so that the resulting routing protocol does not degrade system performances. Since in MANET, there is no fixed-infrastructure such as base stations, mobile devices need to operate as routers in order to maintain the information about the network connectivity, as a result the Conventional routing protocols cannot be supported easily by ad hoc networks. Several research studies have been launched to study this issue, those defined by the IETF MANET group can be classified into two categories: proactive protocols and reactive protocols. MANET's technology offers both new challenges and opportunities for many applications . The major challenges for ad hoc technology is secure and efficient routing, due essentially to MANET features (e.g., open medium, lack of centralized management, nodes mobility). Several approaches have been introduced to secure ad hoc routing. Some existing solutions in wireless networks employ mechanisms used to protect routing protocols in wired networks that are based on the presence of a centralized infrastructure. These solutions are not appropriate for a decentralized ad hoc network. In mobile ad hoc networks, neighbor discovery is the process by which a node in a network determines the total number and identity of other nodes in its vicinity .It is a fundamental building block of many protocols including localization, routing, leader election, and group management. Time-based communications and many media access control mechanisms rely on accurate neighbor information. Neighbor discovery is especially important to the proper functioning of wireless networks. In wireless networks, neighbors are usually defined as nodes that lie within radio range of each other. Thus, neighbor discovery can be considered as the exploration of the volume of space or "neighborhood" immediately surrounding a wireless node. Nodes found within the neighborhood are neighbors and, depending on network configuration and topology, may cooperate in the performance of various tasks including communications, routing and localization. However, wireless communications are vulnerable to attacks. Attackers have the freedom to perform malicious The verification of node locations is an important issues in mobile networks, and it becomes particularly challenging in the presence of adversaries aiming at harming the system.

A. Finding the position of a neighbour

Neighbour discovery deals with the identification of nodes with which a communication link can established or that are within a given distance. An adversarial node could be securely discovered as neighbour and be indeed a neighbour (with in some range),but it could still cheat about its position within the same range. In other words, SND lets a node assess whether another node is an actual neighbour but it does not verify the location it claims to be at. This is most often employed to counter wormhole attacks.

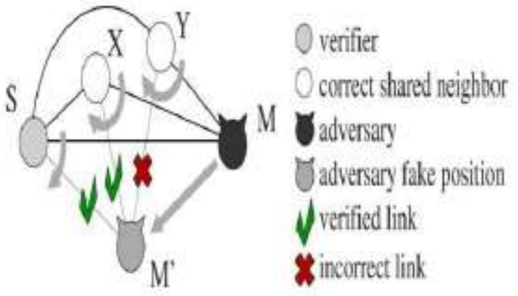

Figure 1. Neighbor discovery in adversarial environment

B. Confirmation of claimed position.

Neighbor verification schemes often rely on fixed or mobile trustworthy nodes, which are assumed to be always available for the verification of the positions announced by third parties. In ad hoc environments, however the pervasive presence of either infrastructure or neighbor nodes that can be aprioristically trusted is quite unrealistic. Thus, a protocol is devised that is autonomous and does not require trustworthy neighbours.

C. Importance Of Neighbor Position Update

An ad hoc network is the collection of wireless mobile hosts forming a temporary without the aid of any established infrastructure or centralized administration. In such an environment , it is necessary for one mobile host to enlist the aid of other hosts in forwarding packet to its destination, due to the limited range of each mobile host's wireless transmissions. In order to procure the position of other nodes while moving, an approach is proposed such a way that it helps in obtaining the position of dynamic mobile node. This paper presents a protocol for updating the position of node in dynamic ad hoc networks. The protocol adapts quickly to position changes when host movement is frequent, yet requires little or no overhead during periods in which hosts move less frequently.

II. RELATED WORK

A large portion of the directing calculations proposed for MANETs depend on receptive steering procedure, in which course is set up just when there is a need to transmit a bundle. In these conventions course recuperation and upkeep methodology are started when a course break. This strategy expends additional data transfer capacity and force at preparing hubs furthermore builds the deferral. It is imperative to discover courses that last more, to decrease the course breakage and utilization of assets. T-Cabrera, A., N-Perez, proposed Link strength is characterized as a measure of how stable the connection is and to what extent the correspondence will persevere. Signal Strength is one of the parameter used to evaluate the dependability of connections. C-K. Toh, proposed the course revelation depends on sign quality and area soundness of hubs . SSA, a versatile hub decides the normal sign quality at which the parcels are traded in the middle of Nodes and area soundness is utilized to pick longer-lived course. Sulabh Agarwal and Pal Singh proposed RABR, in which the course choice is done taking into account the smart remaining lifetime appraisal of the competitor courses. This significant test with this convention is, to pick the ideal edge values. Hwee Xian et.al the creators evaluated the connection soundness in light of the sign quality . In the event that the got signal quality is more noteworthy than a specific limit, the connection is thought to be steady.

Min-Gu and Sunggulee proposed a course determination in view of Differentiated sign quality [DSS]. DSS shows whether the hubs are getting closer or getting more remote separated. In the event that the sign quality is getting more grounded, the connection is thought to be steady. On the off chance that the sign quality is getting weaker if there should be an occurrence of hub moving without end is thought to be precarious connection. N.Sharma and S.Nandi proposed RSQR in which the connection steadiness and course security are figured utilizing got signal quality. In view of the limit values the connections are delegated steady or shaky connection. Join solidness and connection vulnerability qualities are utilized for stable course determination among all the attainable courses. Weapon Woo and Lee proposed EBL, in which the creators offer significance to both connection dependability and the remaining Battery limit. The EBL enhance the vitality proficiency as well as diminish system parcel.

Floriano and Guerriero proposed LAER, in which they consider joint metric of connection solidness and vitality channel rate into course disclosure, which brings about decreased control overhead and adjusted activity load. The normal course lifetime is basically anticipated with the parameters hub battery vitality and connection solidness. It is desirable over select stable connections i.e. joins having longer anticipated lifetime, rather than selecting feeble connections which break soon and present steering overhead. Guerriero proposed PERRA, a receptive steering convention, which accounts both connection security and force productivity . Middle of the road hubs in PERRA engenders course ask for, just in the event that it meet the vitality prerequisite indicated by the source hub. In this manner, the way settled is a steady way that brings about leftover vitality, way steadiness and evaluated vitality for information transmission. It likewise keep up substitute way, which can be utilized before connection break jumps out at lessen the way breakage. Ahamed nabet et.al is proposed a proficient secure directing convention (ASRP) to guarantee the steering security in impromptu systems. ASRP gives intense security augmentations to the responsive AODV convention, taking into account changed secure remote secret word convention and Diffie-Hellman (DH) calculations.

III. EXISTING SYSTEM

Neighbor disclosure is the procedure by which a hub in a system decides the aggregate number and character of different hubs in its region. It is a basic building piece of numerous conventions including limitation, directing, pioneer decision, and gathering administration. Time-based interchanges and numerous media access control systems depend on exact neighbor data. Neighbor revelation is particularly imperative to the best possible working of remote systems. In remote systems, neighbors are normally characterized as hubs that exist in radio scope of one another. In this manner, neighbor revelation can be considered as the investigation of the volume of space or "neighborhood" quickly encompassing a remote hub . Hubs found inside of the area are neighbors and, contingent upon system design and topology, might participate in the execution of different assignments including interchanges, detecting and limitation. Be that as it may, remote correspondences are defenseless to mishandle. Assailants have the flexibility to perform pernicious exercises going from basic refusal of administration to complex duplicity.

A. Location-based Technique

It offer neighbor discovery protocols to ensure that nodes claiming to be neighbors share the same neighborhood. It uses localized beacons to detect wormholes while executing a localization protocol for statically deployed nodes . A mechanism for geographically assigning local broadcast keys was used to limit the range of communications. However, location-based protocols assume the availability of localization information, at least for a subset of participating nodes, making them unsuitable for scenarios without this information .

B. Secure neighbor discovery (SND) Technique

It deals with the identification of nodes with which a communication link can be established or that are within a given distance. SND is only a step toward the solution, so simply put, an adversarial node could be securely discovered as neighbor and be indeed a neighbor (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 neighbor but it does not verify the location it claims to be at.

C. Neighbor position verification (NPV) Technique

It was studied in the context of ad hoc and sensor networks; however, existing NPV schemes often rely on or mobile trustworthy nodes, which are assumed to be always available for the verification of the positions announced by third parties. In ad hoc environments, however, the pervasive presence of either infrastructure or neighbor nodes that can be aprioristically trusted is quite unrealistic . This protocol is autonomous and does not require trustworthy neighbors.

D. NPV routing protocol

NPV convention is first gives hubs a chance to calculate separations to all neighbors, and afterward lauds that all triplets of hubs surrounding a couple of different hubs go about as verifiers of the pair's positions. This plan does not depend on reliable hubs, but rather it is intended for static sensor arranges, and requires extensive multi round calculations including a few hubs that look for agreement on basic neighbor confirmation . In addition, it goes for evaluating not the position but rather whether the hub is inside of a given area or not.NPV arrangement, rather, permits any hub to approve the position of the majority of its neighbors through a quick, one-time message trade, which makes it suitable to both static and portable situations.

IV. PROPOSED WORK

To guarantee the unwavering quality and soundness of the directing procedure here Efficient Neighbor Route Discovery Protocol (ENRDP). Initially it is give a conveyed, lightweight answer for the neighbor position confirmation issue that need not require foundation or from the earlier trusted neighbors and is hearty against a few distinct assaults, including composed assaults by autonomous and conniving foes. Next, it gives best determination of neighbor in light of the strength of the connection.

Partitioning the ENDRP convention into two errands.

1) Distributed agreeable NPV

2) Path security expectation procedure

A. Distributed cooperative scheme for NPV

A completely disseminated helpful plan for NPV, which empowers a source hub, to find and check the position of its correspondence neighbors.

Step 1: find hubs in reach.
Step 2: send solicitation to hubs
Step 3: sit tight for association
Step 4: get area from companions with time.
Step 5: keep up area table
Step 6: telecast the area to different hubs
Step 7: get reaction from other
Step 8: confirm the destination area and reaction from different hubs
Step 9: check for area information at each solicitation or operation
Step 10: if the area of companion is invalid imprint it as spam (by its macintosh id)
Step 11: show the spammed peer macintosh id to every other hub.

a) Discover own location and neighbor location:

Discovering own location and neighbor location is tedious task in mobile ad hoc network. In this stage of process it’s used to find the own location and Neighbor location through the wifi integrated service. These findings are used to involve in the neighbor position verification.

b) Connection between neighbor nodes

Connection establishment with neighbor and accept connection by their neighbors made a connection more secure. In this stage it’s used to follow initial security mechanism through the cryptography techniques. Connections with their neighbors are established here using AES cryptography technique. Connection need to be accepted in both ends then only source can sent secure message transaction. Neighbor position verification algorithm used to check all with their neighbor through above mentioned steps to verify their neighbors.

c) Secure content transaction

A completely appropriated agreeable plan for NPV, which empowers a source hub, to find and confirm the position of its correspondence neighbors. For clarity, here we abridge the standards of course revelation and position check process. A source hub, S can start the convention whenever moment, by setting off the 4-stage message trade process [POLL, REPLY,REVEAL and REPORT], subsequent to finishing the message trade process, source hub S has determines separation scope of neighbor hubs to find the most brief way to achieve destination, after course revelation S runs a few position check tests with a specific end goal to order every competitor neighbor as either VERIFIED, FAULTY, UNVERFIABLE. Unmistakably , the check tests go for maintaining a strategic distance from false negatives(i.e..adversaries declaring fake positions that are considered confirmed) and false positives (i.e., right hubs whose positions are regarded faulty),as well as at minimizing the quantity of unverifiable hubs. we comment that our NPV plan does not focus on the formation of a predictable "guide" of neighborhood relations all through a vaporous system: rather, it permits the verifier to autonomously order its neighbors.

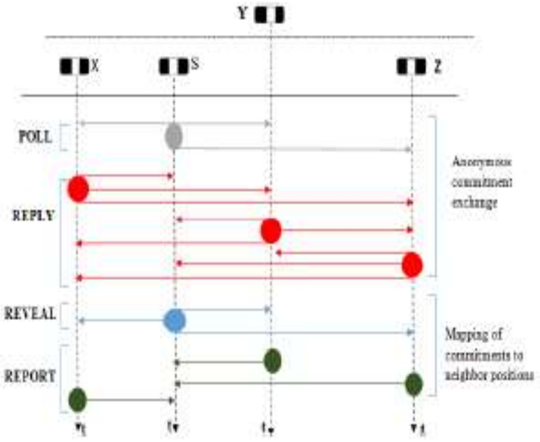
Y
X
S
Z
POLL
REPLY
REVEAL
REPORT
Anonymous commitment exchange
Mapping of commitments to neighbor positions
t
t
t
t

Figure 2. Messages Exchange Process

Survey message A verifier S starts this message. This message is unknown. The character of the verifier is kept covered up. Here programming produced MAC location is utilized. This conveys an open key K'S browsed a pool of onetime use keys of S'.

Answer message A correspondence neighbor X getting the POLL message will telecast REPLY message after a period interim with a crisply produced MAC address. This additionally inside recoveries the transmission time. This additionally contains some encoded message with S open key (K'S).

This message is called as responsibility of XCX.

Uncover message The REVEAL message is shown utilizing verifier's genuine MAC address. It contains A guide MS, a proof that S is the creator of the first POLL and the verifier personality, i.e., its affirmed open key and mark.

REPORT message The REPORT conveys X's position, the transmission time of X's REPLY, and the rundown of sets of gathering times and impermanent identifiers alluding to REPLY shows X got. The identifiers are acquired from the guide MS incorporated into the REVEAL message. Likewise, X reveals its own personality by incorporating into the message its advanced signature and ensured open key. The hub position check is not suitable for element environment, since portable hubs are in element in nature, so every last calendar the versatile hubs experiences position confirmation test, in this manner results in postponement time of bundle conveyance proportion.

B. Path stability prediction technique

A fundamental issue arising in mobile ad hoc networks (MANETs) is the selection of the optimal path between two nodes. Ensuring a path to be valid for adequately longer period of time is a very difficult problem in MANET due to its high mobility nature. A method that has been advocated to improve routing efficiency is to select the most stable path so as to reduce the latency and the overhead due to route reconstruction. As per Distributed cooperative scheme for NPV technique, solves the neighbor verification and this scheme does not concentrate on link failures which is more often in MANET network so neighbor position verification is not get optimized results thus provide solution to link breakages through path quality technique and enhance neighbor position verification technique as per path quality technique which delivers results in efficient manner. Route maintenance and route discovery procedures are similar to the DSR protocol, but with the route selection based on the three aforementioned metrics. Delivery probabilities are synthesized locally from context information's like value describes the above metrics. A delivery probability of each node is used to select link stability path over dynamic route discovery.

V. ENRDP ROUTING PROTOCOL

Efficient Neighbor Route Discovery Protocol (ENRDP) is very evident that two major factors neighbor position verification, mobility and energy efficiency need to be considered to assure better network performance. Especially while assuring QoS in MANET environment nodes should not die due to power constraint or the links should not expire due to mobility in the middle of the transmission. So the target is to choose a more stable path considering higher link stability and less cost along predicted higher life path. It combines the idea of link stability calculation based on mobility prediction and best neighbor selection in terms of cost and lifetime along with QoS support. The working procedure of ENRDP protocol is described in the Fig.5.

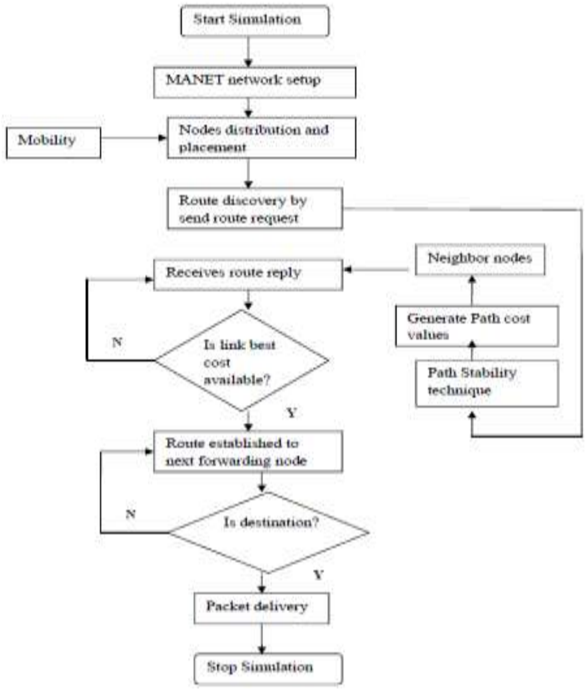
Start Simulation
MANET network setup
Mobility
Nodes distribution and placement
Route discovery by send route request
Receives route reply
Neighbor nodes
N
Is link best cost available?
Generate Path cost values
Path Stability technique
Y
Route established to next forwarding node
N
Is destination?
Y
Packet delivery
Stop Simulation

Figure 3. ENRDP Protocol

VI. PERFORMANCE EVALUATION

The metrics used in evaluating the performance are:

Packet Delivery Ratio: The ratio between the, number of received data packets to the number of total data packets sent by the source.

Packet delivery ratio = Number of packet received / Number of packet send * 100

Average End-to-End delay: The average time elapsed for delivering a data packet within a successful transmission from source to destination.

End to end delay = Inter arrival of 1st packet time& 2nd packet time / Total packet data delivery time.

Packet Lost: The discarding of data packets in a network when a router, is overloaded and cannot accept any incoming data at a given moment.

Packet lost = total number of packet received - Send

Energy consumption: The energy consumption for the entire network, including transmission and processing energy consumption for both the data and control packets.

Energy consumption = Energy consumed on IDL sleep, transmit and receive / Total energy consumed

VII. CONCLUSION

Mobile ad hoc networks, knowledge of neighbor positions are important task. Distributed techniques to perform secure neighbor position discovery, suitable for highly mobile ad hoc environments, ENRDP system under discovery of neighbor by avoiding false positions neighbors and also addressed the selection of stable path among the neighbors which not only describes the selection of correct position neighbors but also best link stability neighbors. Thus overcome the adversary and also link failures. both the availability and the duration probability of a routing path that is subject to link failures caused by node mobility in terms of malicious activities. Then ENRDP protocol is simulated the in NS-2. The parameters like throughput, delay, packet lost and packet delivery ratio of the proposed protocol are compared with that of existing and ENRDP. This performance has reduced the packet lost, delay and increases the delivery ratio, throughput of the network.

REFERENCES

[1] Ahmed Nabet, RidaKhatoun, LyesKhoukhi, Juliette Dromard and Dominique Gaïti "Towards Secure Route Discovery Protocol in MANET," IEEE 2011.

[2] C. LOURDU RAJA "Neighbor Position Verification in Mobile Ad Hoc Network", ISSN (Online): 2320-9801,Vol.2, Special Issue 1, and March 2014.

[3] C-K. Toh, "Associativity-Based Routing for Adhoc Mobile Networks," IEEE Personal Communications, Vol.4,No.2, pp.103 – 139, March 1997.

[4] F.D. Rango, F. Guerriero, "Link Stability and Energy Aware Routing Protocol in Distributed Wireless Networks", IEEE Transactions on Parallel and Distributed systems, vol.23, no. 4, April 2012.

[5] F.Guerriero "ABiojective Optimization Model for Routing in Mobile Ad-hoc Networks", IEICE Trans. Comm. Pp 4588- 4597.

[6] G.W. Park, S.Lee, "A routing protocol for Extent Network Lifetime through the Residual Battery and Link Stability in MANET", ACC '08, Istanbul, Turkey, May 27-30, 2008.

[7] Hwee Xian, Winston Seah, "Limiting Control Overheads Based on Link Stability for Improved performance in Mobile Adhoc Networks", Springer, UNCS3510, pp.258-268. WWIC 2005.

[8] Lee, M.-G., & Lee, S. "A link stability model and stable routing for mobile ad-hoc networks", LNCS4096, Seoul,