SECURE DATA FORWARDING AND POSITIONING IN MOBILE AD HOC NETWORK USING DV-HOP PROPAGATION METHOD

B.Lourdu Ruby,
M.Phil Research Scholar,
P.G & Research Department of Computer Science,
Senguthar Arts and Science College,
Tiruchengode,Tamilnadu,India.

P.Balamurugan,
Assistant Professor,
P.G & Research Department of Computer Science,
Senguthar Arts and Science College,
Tiruchengode,Tamilnadu,India.

Abstract: A Mobile Ad-hoc Network (MANET) is an autonomous collection of mobile users that communicate over relatively bandwidth constrained wireless links. One of the main issues in such networks is performance- in a dynamically changing topology; the nodes are expected to be power-aware due to the bandwidth constrained network. Another issue in such networks is security - since every node participates in the operation of the network equally, malicious nodes are difficult to detect. There are several applications of mobile ad hoc networks such as disaster recovery operations, battle field communications, etc. The paper is discussed introductory background on ad hoc wireless networks and reviews existing work in routing and positioning; presents the APS family of positioning algorithms, and examines their performance analysis analytical, and through simulation.

Keywords: Mobile Ad Hoc Network, Routing, Positioning, forwarding and Security

I.INTRODUCTION

Mobile Ad hoc networks or MANETs are the category of wireless networks which do not require any fixed infrastructure or base stations. They can be easily deployed in places where it is difficult to setup any wired infrastructure. As shown in Figure.1, there are no base stations and every node must co-operate in forwarding packets in the network.

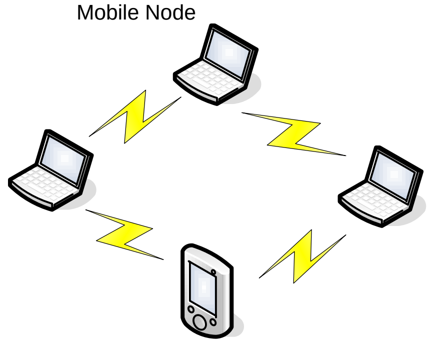


Figure 1: A Mobile ad hoc

Thus, each node acts as a router which makes routing complex when compared to Wireless LANs, where the central access point acts as the router between the nodes. A sensor network is a special category of ad hoc wireless networks which consists of several sensors deployed without any fixed infrastructure. The difference between sensor networks and ordinary ad hoc wireless is that the sensor nodes may not be necessarily mobile. Further, the number of nodes is much higher than in ordinary ad hoc networks. The nodes have more stringent power requirements since they operate in harsh environmental conditions. An example of a sensor network is a set of nodes monitoring the temperature of boilers in a thermal plant. Other application domains include military, homeland security and medical care [1][2].

Advantages of Mobile Ad hoc Networks

Having discussed the general issues in MANETs, the reason behind their popularity and their benefits will now be discussed.

(a) Low cost of deployment: As the name suggests, ad hoc networks can be deployed on the fly, thus requiring no expensive infrastructure such as copper wires, data cables, etc.
(b) Fast deployment: When compared to WLANs, ad hoc networks are very convenient and easy to deploy requiring less manual intervention since there are no cables involved.
(c) Dynamic Configuration: Ad hoc network configuration can change dynamically with time. For the many scenarios such as data sharing in classrooms, etc., this is a useful feature. When compared to configurability of LANs, it is very easy to change the network topology [3].

II. LITERATURE REVIEW

M. Tamer Refaei, *et al.* [4] proposed reputation-based mechanism as a means of building trust among nodes. Here a node autonomously evaluates its neighbouring nodes based on completion of the requested service(s). The neighbours need not be monitored in promiscuous mode as in other reputation based methods. There is no need of exchanging of reputation information among nodes. Thus involves less overhead, and this approach does not rely on any routing protocol. This approach provides a distributed reputation evaluation scheme implemented autonomously at every node in an ad hoc network with the objective of identifying and isolating selfish neighbours. A reputation table is maintained by each node, where a reputation index is stored for each of the node's immediate neighbours. A node calculates reputation index of its neighbour based on successful delivery of packets forwarded through that neighbour. For each successfully delivered packet, each node along the route increases the reputation index of its next-hop neighbour that forwarded the packet and packet delivery failures result in a penalty applied to such neighbours by decreasing their reputation index.

Pietro Michiard, *et al.* [5] proposed a Collaborative Reputation (CORE) mechanism that also has a watchdog component for monitoring. Here the reputation value is used to make decisions about cooperation or gradual isolation of a node. Reputation gives values are obtained by regarding nodes as requesters and provider and compare results. In this system the reputation value ranges from positive (+) through null (0) to negative (-). The advantage of this method is that having a positive to negative range allows good behaviour to be rewarded and bad behaviour to be punished. This method gives more importance to the past behaviour and hence tolerable to sporadically bad behaviour, e.g. battery failure. But the assumption that past behaviour to be indicative of the future behaviour may make the nodes to build up credit and then start behaving selfishly.

Buchegger, *et al.* [6] Here evidence from direct experiences and recommendations is collected. Trust relationships are established between nodes based on collected evidence and trust decisions are made based on these relationships. There are four interdependent modules, monitor, reputation system, path manager and trust manager. Monitor collects proof by monitoring the transmission of a neighbour after forwarding a packet to the neighbour. It then reports to the reputation system only if the collected evidence represents a malicious behaviour. Reputation system changes the rating for a node if the evidence collected for malicious behaviour exceeds the predefined threshold value. Then, path manager makes a decision to delete the malicious node from the path. Trust manager is responsible for forwarding and receiving recommendations to and from trustworthy nodes. But this approach does not talk much about isolating the misbehaving nodes from the network.

Tiranuch Anantvalee, *et al.* [7] in their paper, introduces, a new type of node called as suspicious node besides cooperative nodes and selfish nodes, Some actions will be taken to encourage the suspicious nodes to cooperate properly after further investigation. They introduce the use of a state model to decide what to do or respond to nodes in each state. In addition to a timing period for controlling when the reputation should be updated, a timeout for each state is introduced.

III. AD HOC POSITIONING SYSTEM

It is a given that in many of these networks, due to considerations of cost, size, and power requirements, individual nodes will not have full position and orientation capabilities. A more general question is how to export capabilities to various nodes in the network so that the overall capability can be increased in the network. Finding position without the aid of GPS in each node of an ad hoc network is important in cases where the GPS service is either not accessible, or not practical to use due to power, form factor or line of sight conditions such as indoor sensors, sensors hidden under foliage, etc. A similar argument holds for orientation as compasses face erratically behavior in the vicinity of large metal objects or electrical fields. Orientation, or heading, is used in remote navigation, or remote control of specialized sensors, such as directional microphones or cameras. I address the problems of self positioning and orientation of the nodes in the field, which may provide a general framework for exporting capabilities in a network where more capable nodes cooperate in dispersing information to less capable nodes.

What is necessary for ad hoc deployment of temporary networks is a method similar in capability to GPS and magnetic compasses, without requiring extra infrastructure, or extensive processing capabilities. Here, propose a method by which nodes in an ad hoc network collaborate in finding their position and orientation under the assumptions that a small fraction of the network has only the positioning capability. The orientation and positioning problems have been extensively studied in the context of mobile robot navigation, however, many methods proposed by the robotics community make extensive use of image processing and preset infrastructure, such as \recognizable" landmarks. The aim for the ad hoc networks is to find a positioning method that is robust, but relies on less computational resources and on fewer infrastructures.

IV. DV-HOP PROPAGATION METHOD

This range free method is the most basic scheme, and it comprises of three non-overlapping stages.

(1) First, it employs a classical distance vector exchange so that all nodes in the network get shortest paths, in hops, to the landmarks. Each node maintains a table $\{X_i, Y_i, h_i\}$ and exchanges updates only with its neighbors.

(2) In the second stage, after it cumulates distances to other landmarks, a landmark estimates an average size for one hop, which is then deployed as a correction to the nodes in its neighborhood.

(3) When receiving the correction, an arbitrary node may then have estimate distances to landmarks, in meters, which can be

used to perform the trilateration, which constitutes the third phase of the method. The correction a landmark (X_i , Y_i) computes is

$$c_i = \frac{\sum \sqrt{(X_i - X_j)^2 + (Y_i - Y_j)^2}}{\sum h_i}, \; i \neq j, \; all\, landmarks\, j$$

The drawbacks of DV-hop are that it will only work for isotropic networks, that is, when the properties of the graph are the same in all directions, so that the corrections that are deployed reasonably estimate the distances between hops. The DV-hop idea was independently explored in the context of amorphous computing by Nagpal [8], who has also given an upper bound on the accuracy.

CRLB for trilateration:

The Cramer-Rao lower bound is a method that sets a lower bound on the variance of any unbiased estimator. Its main merit is that it provides a benchmark against which to evaluate the performance of an estimator. The trilateration problem is cast as an estimation problem by considering the true position x as the parameter to be estimated. The distribution of errors of distances to landmarks is assumed to be known at this point in the presentation. Using the same notations the error in the obtained position can be estimated, given the range to landmark estimation error. This approach is applicable to all the algorithms that use trilateration as a final phase (DV-hop, DV-distance, and Euclidean). The hop by hop nature of multi hop algorithms always produces normal range errors for a sufficiently large number of hops - this was confirmed by simulation for all algorithms mentioned here. The CRLB of the variance in the estimated parameter x is:

$$CRLB(Cov[\mathrm{x}]) \;=\; (J_0^{\top} W J_0)^{-1}$$

DV-hop range error:

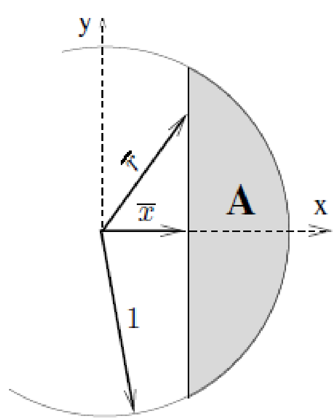


Figure 2: Progress

In DV-hop, the main source of range error stems from the fact that a node translates the length of shortest path to a landmark into a Euclidean distance by assuming that every hop produces progress ci - equation. Geographic forwarding has been shown in [9] to produce paths with low dilation, that is, good shortest path approximates.

Density,

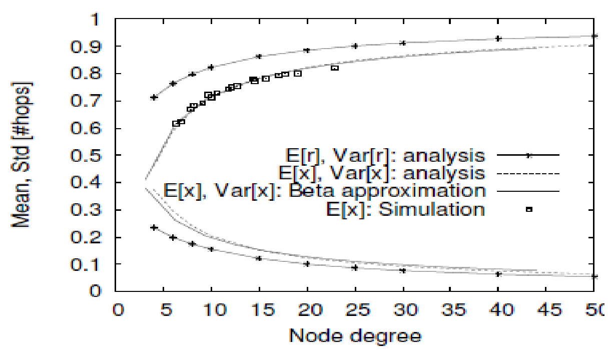
$$\hat{c}_i \;=\; r\left(1 + e^{-N_i} - \int_{-1}^{1} e^{-\frac{N_i}{\pi}(\arccos t - t\sqrt{1-t^2}}dt\right)$$

Where N_i is the number of neighbors for node i, and r is the maximum wireless radius. For DV-hop, this implies that in uniform networks, nodes may locally estimate the correction based on their local perception of density, and thus eliminate the need for the second stage of the algorithm. Assuming a Poisson spatial distribution of nodes with rate λ , and a wireless range of radius 1, the expected number of neighbors of a node will be λ . throughout the chapter both the average number of neighbors, and the rate λ are used when referring to density. A node chooses a next hop that produces most progress x towards a destination on the horizontal axis (Figure 4.1). There are no nodes in area A, which allows for the following derivation of the distribution of x.

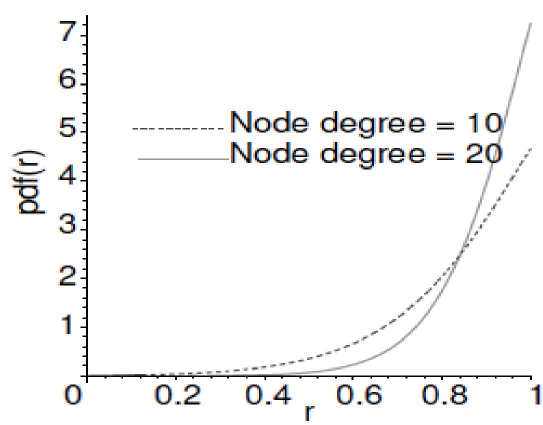
$$A(\overline{x}) \;=\; 2\int_{\overline{x}}^{1} \sqrt{1-t^2}dt = \arccos(\overline{x}) - \overline{x}\sqrt{1-\overline{x}^2}$$

$$F_{\overline{X}}(\overline{x}) \;=\; \{\overline{X} \leq \overline{x}\} = e^{-\lambda A(\overline{x})}$$

$$f_{\overline{X}}(\overline{x}) \;=\; \{\overline{X} = \overline{x}\} = -\lambda A'(\overline{x})e^{-\lambda A(\overline{x})} = 2\sqrt{1-\overline{x}^2}e^{-\lambda(\arccos(\overline{x}) - \overline{x}\sqrt{1-\overline{x}^2})}$$



(a) Mean and stddev of $\overline{x}, \overline{r}$



(b) Density of $\overline{r}$ for two densities

Figure 3: Behavior of x; r

$$V[\overline{x}] = \int_{-1}^{1} \overline{x}^2 f(\overline{x}) d\overline{x} - (\int_{-1}^{1} \overline{x} f(\overline{x}) d\overline{x})^2$$

Unfortunately, there are no closed forms for the first moments E[x] and V [x] of this distribution, but it can be approximated as a Beta distribution. In Figure 3, numerically evaluated variance V [x] and expectation E[x] as functions of density λ are shown together with the approximation to beta distribution, and with values of c_i obtained from simulation using in a network with 1000 nodes with increasing densities. Since these values only depend on the density of the network, pre computed a table with all the values necessary for the experiments in this chapter, namely for densities up to 20 neighbors. In DV-hop, range estimates are obtained as $p_i = h_i c_i$, where hi is the number of hops to landmark i, and ci is approximated by E[x]. If geographic forwarding model is used to approximate shortest path to the landmark, after jumping hi times (assumed independent). Figure 4 shows the behavior of r, the actual distance traveled in one hop by the MFR policy. Its distribution is actually needed for the analysis of DV-position, but its characterization is based on the pdf of x. The pdf of r is obtained as a sum of probabilities of a next hop, integrated over the entire circle of radius r.

$$f_{\overline{R}}(\overline{r}) = \int_0^{2\pi} \frac{f_{\overline{X}}(\overline{r}\cos t)}{2\sqrt{1-\overline{r}^2\cos^2 t}} dt$$

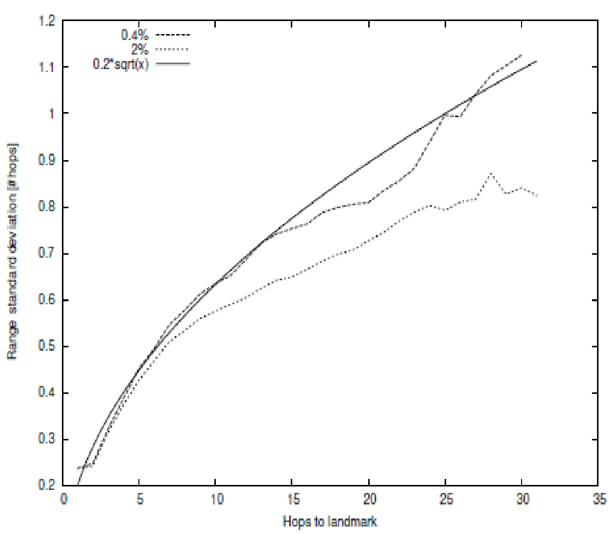


Figure 4: Range deviation (DV-hop)

r is not available in closed form, but in Figure 3b, its behavior can be seen through numerical evaluation, for two different densities. As expected, larger jumps are much more likely than short jumps, which means larger errors if r is to be used as a measure of distance. In Figure 3, the mean and standard deviation of r are shown as a function of density. Ran DV-hop in 100 networks of 1000 nodes, with an average degree of 10.48 and landmark ratios of 0.4% and respectively 2%. From Figure 3a, for this node degree, V [x] = 0.2^2, and the range deviation as a function of distance is showed in Figure 4. The behavior is similar whether corrections are produced using the second stage of DV-hop c_i based on, or the same E[x] for all nodes. The independence assumption between successive jumps in the geographic forwarding procedure fails to account for holes in the network, assuming each new jump starts on the horizontal axis. This is especially visible for longer paths, when the shortest path nature of DV-hop has the chance of optimizing routes around holes, in reality using a different x than the analysis. Higher fractions of landmarks have a beneficial effect, since each landmark generates a specific correction for its area, which gets distributed around it.

V.CONCLUSIONS

This paper explores various aspects of positioning in ad hoc networks. The main contributions are in providing several algorithms for positioning of ad hoc nodes, and a forwarding scheme that makes use of node positions. These contributions mainly address the problems of scalability with respect to node mobility, node size, and network size. Ad hoc positioning system (APS) is a family of positioning algorithms that uses a distance vector scheme and exports the positioning capability from a low fraction of landmarks to the entire network. The closest competitor in solving this problem is currently AhLOS. When compared to it, APS is simpler, requires a lower fraction of landmarks, and supports a wide range of node capabilities.

VI.REFERENCE

[1]. C. Siva Ram Murthy, B.S. Manoj, "*Ad Hoc Wireless Networks : Architectures and Protocols*", Prentice Hall Publishers, May 2004, ISBN 013147023X

[2]. C.-K. Toh, "*Ad Hoc Mobile Wireless Networks: Protocols and Systems*", Prentice Hall publishers, December 2001, ISBN 0130078174

[3]. C. Perkins and P. Bhagwat, *Highly Dynamic Destination-Sequenced Distance-Vector Routing* (*DSDV*) for Mobile Computers. In Proc. of the ACM SIGCOMM, October 1994. http://www.cs.umass.edu/~mcorner/courses/691M/papers/perkins.pdf

[4]. J. Luo, D. Ye, X. Liu, and M. Fan, "A Survey of Multicast Routing Protocols for Mobile Ad-Hoc Networks," "IEEE Communications Surveys & Tutorials", vol. 11, no. 1, First Quarter 2009

[5]. M. Tamer Refaei, VivekSrivastava, LuizDaSilva, Mohamed Eltoweissy, " A Reputation-based Mechanism for Isolating Selfish Nodes in Ad Hoc Networks", Proceedings of the Second Annual International Conference on Mobile and Ubiquitous Systems: Networking and Services (MobiQuitous'05) , 2005

[6]. Buchegger, Sonja ; Le Boudec, Jean-Yves, "Performance A nalysis of CONFIDANT Protocol:

Cooperation ofnNodes - Fairness in Dynamic Ad- Hoc Networks," Proceedings of IEEE/ACM Workshop on Mobile Ad Hoc Networking and Computing (MobiHOC). IEEE, June 2002.

[7]. Hongmei Deng, Wei Li, and Dharma P. Agrawal, "*Routing Security in Wireless Ad Hoc Network*," IEEE Communications Magzine, vol. 40, no. 10, October 2002.

[8]. The Secan Lab, University of Luxembourg, Luxembourg. http://wiki.uni.lu/secan-lab/Distributed+Bellman-Ford.html

[9]. T. Imielinski and J. C. Navas, ―GPS-based Geographic Addressing, Routing, and Resource Discovery,‖ Commun. ACM, vol. 42, no. 4, Apr. 1999, pp. 86–92.

[10]. G. Finn. Routing and addressing problems in large metropolitan-scale internetworks. Technical Report ISI Research Report ISI/RR-87-180, University of Southern California, March 1987.

[11]. Martin Mauve, J • org Widmer, and Hannes Hartenstein. A survey on position-based routing in mobile ad hoc networks. IEEE Network, pages 30{39, November/December 2001.

[12]. Ivan Stojmenovi_c. Position-based routing in ad hoc networks. IEEE Communication Magazine, 40(7):128{134, July 2002.

[13]. Y.-B. Ko and N. H. Vaidya. Location-aided routing (LAR) in mobile ad hoc networks. In ACM MOBICOM, October 1998.