ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Monthly Peer Reviewed Open Access International e-Journal

Verification of Neighbor Nodes Positions in Dynamic Ad Hoc Mobile Networks

Chada Sravanthi
M.Tech Student,
Department of CSE,
Nova College of Engineering & Technology.

K. Ravichandra
Asst. Prof,
Department of CSE,
Nova College of Engineering & Technology.

ABSTRACT:

Location perception has become a quality in mobile systems, where a wide range of set of rules and applications require data of the place of the contributing nodes. In lack of a priori trustworthy nodes the discovery and confirmation of fellow citizen positions becomes mainly challenging in the occurrence of adversaries directing at injuring the system. In this paper, we report his exposed issue by suggesting a fully spread shared solution that is strong against autonomous and colluding adversaries, and can be damaged only by avast being there of adversaries

Index Terms:

Neighbor position verification, mobile ad hoc networks, vehicular networks.

INTRODUCTION:

Mobile computing is associated with mobility of users, hardware, data and software in computer applications. Specialized class of distributed computing systems where certain nodes can travel in physical and/or logical space, ad hoc joining/removing while remaining portion of a distributed system and perhaps take part in worldwide computational activities. The increasing growth of wireless mobile network and Position verification system services requires where the nodes are present in the unstructured networks so this process easily find out where the actual nodes are to be placed in the mobile network system and also find out adversarial nodes. The challenging of this system is to find out the trusted nodes and its original position. So in this paper we need to discussed about the secure data transmission in the mobile network with verification of position by using NPV algorithm and CRT algorithm.

The NPV performs majorly three operation in mobile network 1) Securely determining own location 2) Secure neighbor discovery 3) Neighbor position verification. Its mainly focus on to performs against several different colluding attacks.

After NPV process the CRT algorithm will determine the huge data that can be divided by some given divisors. And the divided data is to be transmit to the node via the various path and then finally collecting the divided data and merge that data and submit to the destination node.

Existing System:

In this Project, we aim at discovering the number of diverse user search goals for a query and depicting each goal with some keywords automatically. We first propose a novel approach to infer user search goals for a query by clustering our proposed feedback sessions.

Then, we propose a novel optimization method to map feedback sessions to pseudo-documents which can efficiently reflect user information needs. At last, we cluster these pseudo documents to infer user search goals and depict them with some keywords.

Proposed System:

In this paper introduces the map reduce algorithm for improving the search results proposed system, the data mining domain introduce the map reduce algorithm. It is effective for cross domain environment and also can use Big data for future work.

The search results achieved through using feedback sessions and map reduce technique. This results of the cross domain have been improved using this technique. The experimented results show the efficiency.

ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Monthly Peer Reviewed Open Access International e-Journal

Securely determining own location:

In mobile environments, self-localization is mainly achieved through Global Navigation Satellite Systems, e.g., GPS, whose security can be provided by cryptographic and noncryptographic defense mechanismsAlternatively, terrestrial specialpurpose infrastructure could be used along with techniques to deal with nonhonest beacons. We remark that this problem is orthogonal to the problem of NPV. In the rest of this paper, we will assume that devices employ one of the techniques above to securely determine their own position and time reference.

Secure neighbor discovery (SND) :

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 we are after: 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. SND is most often employed to counter wormhole attacks; practical solutions to the SND problem have been proposed, while properties of SND protocols with proven secure solutions can be found.

Neighbor position verification :

was studied in the context of ad hoc and sensor networks; however, existing NPV 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, we devise a protocol that is autonomous and does not require trustworthy neighbors.

Protocol Message Exchange

The value pX is the current position of X, and INX is the current set of its communication neighbors. We denote by tX the time at which a node X starts a broad cast transmission and by tXY the time at which a node Y starts receiving it. Note that these time values refer to the actual instant at which the node starts transmitting/receiving the first bit of the message at the physical layer.

To retrieve the exact transmission and reception time instants, avoiding the unpredictable latencies introduced by interrupts triggered at the drivers level, a solution such as that implemented is required.3 Furthermore, the GPS receiver should be integrated in the 802.11 card; software defined radio solutions combining GPS and 802.11 capabilities are proposed, among others.

PERFORMANCE EVALUATION:

We evaluated the performance of our NPV protocol in a vehicular scenario. Results obtained in a pedestrian scenario are available as supplemental material, which can be found on the Computer Society Digital Library at http:// doi.ieeecomputersociety.org/ 10.1109/TMC. 2011.258.

We focus on knowledgeable adversaries whose goal is to make the verifier believe their fake positions, and we describe the best attack strategy they can adopt in Section 7.1. Such a strategy, which depends on the neighborhood of the adversary and builds on a combination of the attacks described in Sections 6.1 and 6.2, will be assumed while deriving the results shown in Section 7.2. The results, which therefore represent a worst case

analysis of the proposed NPV, are shown in terms of the probability that the tests return false positives and false negatives as well as of the probability that a (correct or adversary) node is tagged as unverifiable.

In addition, we plot the average difference between the true position of a successful adversary and the fake position it advertises, as well as the overhead introduced by our NPV scheme. The results on attacks aimed at discrediting the position of other nodes are omitted, since they are very close to those we present later in this section.

ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Monthly Peer Reviewed Open Access International e-Journal

Figure1. Sender

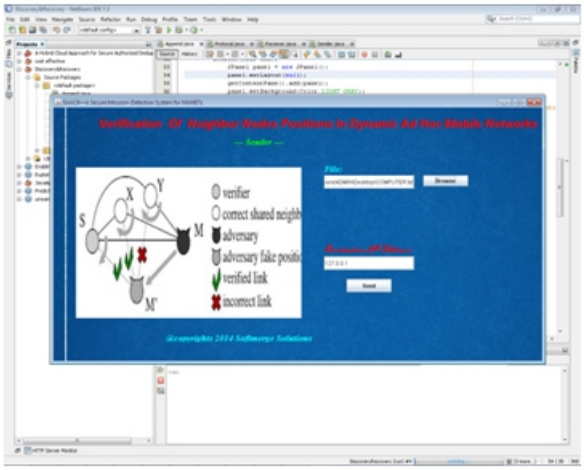


Figure2.Sending data.

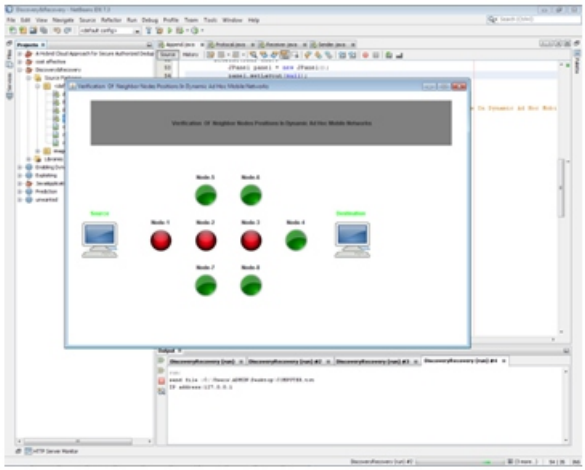


Figure3.Recieved Message

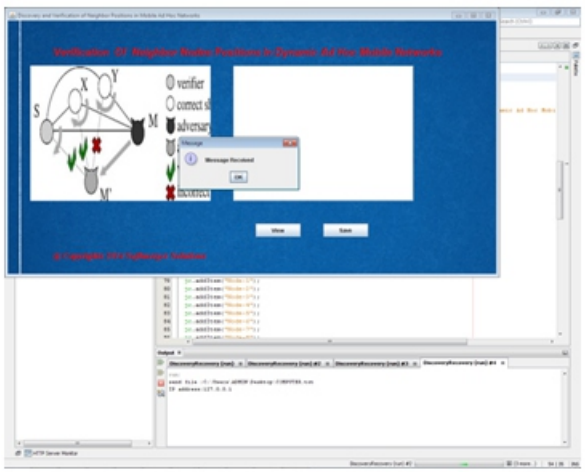


Figure4.View Message.

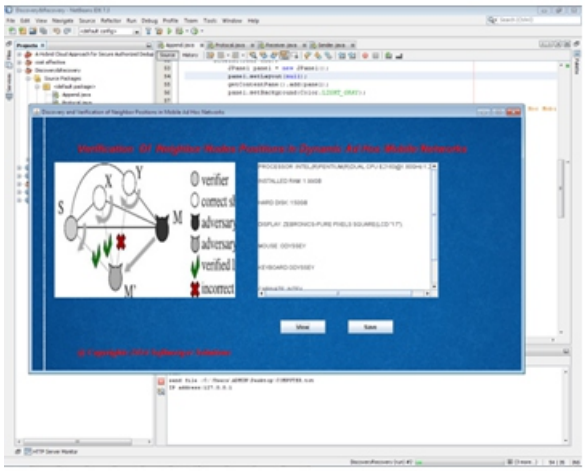


Figure5.Append

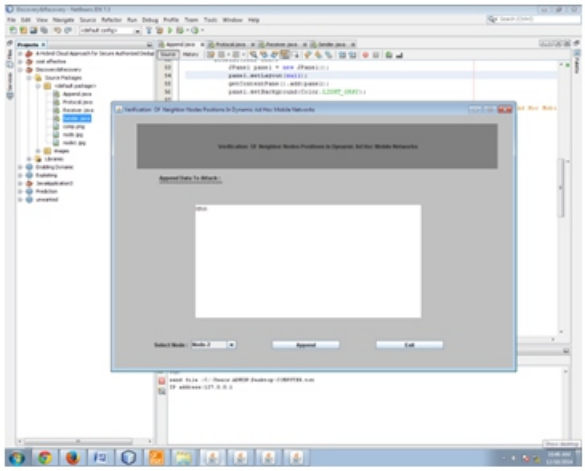
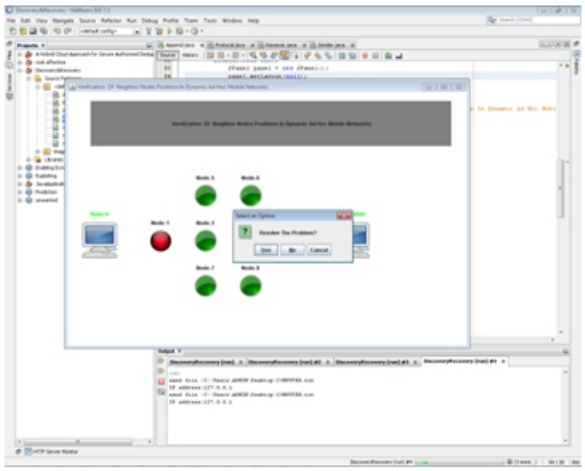


Figure6.Error



ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Monthly Peer Reviewed Open Access International e-Journal

CONCLUSION:

In this paper, an enhanced approach has been proposed. Our experiment showed that our protocol is very useful for data transmission in mobile ad-hoc network and its work against colluding attackers. Then results confirm that our solution is active in detecting nodes advertising untrue position.

The CRT algorithm will determine the huge data that can be divided by some given divisors. And the divided data is to be transmit to the node via the various path and then finally collecting the divided data and merge that data and submit to the destination node. So the experimental results can be considerably efficient and its maintains the secure transaction throughout the process.

REFERENCES:

[1] 1609.2-2006: IEEE Trial-Use Standard for Wireless Access in Vehicular Environments - Security Services for Applications and Management Messages, IEEE, 2006.

[2] P. Papadimitratos, L. Buttyan, T. Holczer, E. Schoch, J. Freudiger, M. Raya, Z. Ma, F. Kargl, A. Kung, and J.-P. Hubaux, "Secure Vehicular Communications: Design and Architecture," IEEE Comm. Magazine, vol. 46, no. 11, pp. 100-109, Nov. 2008.

[3] P. Papadimitratos and A. Jovanovic, "GNSS-Based Positioning:Attacks and Countermeasures," Proc. IEEE Military Comm. Conf.(MILCOM), Nov. 2008.

[4] L. Lazos and R. Poovendran, "HiRLoc: High-Resolution Robust Localization for Wireless Sensor Networks," IEEE J. Selected Areas in Comm., vol. 24, no. 2, pp. 233-246, Feb. 2006.

[5] R. Poovendran and L. Lazos, "A Graph Theoretic Framework for Preventing the Wormhole Attack," Wireless Networks, vol. 13, pp. 27-59, 2007.

[6] S. Zhong, M. Jadliwala, S. Upadhyaya, and C. Qiao, "Towards a Theory of Robust Localization against Malicious Beacon Nodes," Proc. IEEE INFOCOM, Apr. 2008.

[7] P. Papadimitratos, M. Poturalski, P. Schaller, P. Lafourcade, D. Basin, S. Capkun, and J.-P.Hubaux, "Secure Neighborhood Discovery:AFundamental Element for Mobile Ad Hoc Networks," IEEE Comm. Magazine, vol. 46, no. 2, pp. 132-139, Feb. 2008.

[8] Y.-C. Hu, A. Perrig, and D.B. Johnson, "Packet Leashes: A Defense against Wormhole Attacks in Wireless Networks," Proc. IEEE INFOCOM, Apr. 2003.