ISSN (Online) : 2278-1021
ISSN (Print) : 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 3, Issue 2, February 2014

# SECURE DATA-TRANSMISSION IN MOBILE AD-HOC NETWORK WITH VERIFICATION OF NEIGHBOR POSITIONS

**Mr.M.Premkumar[1], G.Praveenkumar[2], G.Ravindran[3], R.Sasikumar[4]**

Assistant Professor, CSE, Christ College of Engineering & Technology, Pondicherry, India[1]

Student, CSE, Christ College of Engineering & Technology, Pondicherry, India[2,3,4]

**Abstract** - Location perception has become a quality in mobile systems, where a wide range of set of rulesand applications require dataof the placeof the contributingnodes. In lackof a priori trustworthy nodes the discovery and confirmationof fellow citizen positions becomes mainly challenging in the occurrenceof adversaries directing at injuring the system. In this paper, we reportthis exposedissue by suggestinga fully spreadsharedsolution that is strong against autonomous and colluding adversaries, and can be damaged only by avastbeing there of adversaries.

**Index Terms** -Unstructured-Network, Position verification, Chinese remainder theorem, CRT-Algorithm, Back-tracking Algorithm.

## I. 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.

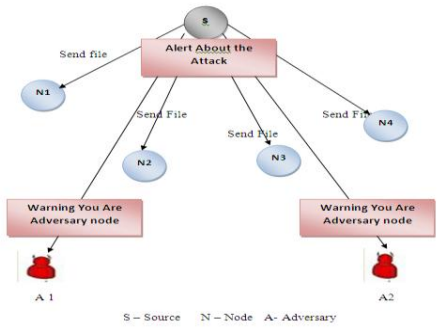
## II. EXISTING SYSTEM

An autonomous sensor is proposed in the existing system that allows nodes to authenticate the spot of their fellow citizen through local comments only. This is achieved by testing whether subsequent positions stated by one neighbor draw a movement over time that is physically probable. The approach forces a node to collect some data on its neighbor movements in the past a decision can be taken, making the solution unfit to positions where the place information is to be achieved and verified in a squat time area.

The general pseudo code for NPV Algorithm,

1. Start with initial source node.
2. Calculate distances between all neighbors nodes.
3. Check if nodes are in original position or not.
4. Apply direct symmetry test.
5. Apply cross symmetry test.
6. Check if nodes are trusted node or adversarial node.
7. Evaluate each and every node in ah-hoc network.
8. Repeat until terminating condition.

### 2.1 ARCHITECTURE DIAGRAM




### 2.3 Drawbacks in Existing System

- Adversary can fool the protocol by simply proclaiming false locations.
- This sensor can be attacked by using fake id nodes.
- Another drawback of the presented solution is that each node has only a local view that might not be enough to reliably identify all position faking node.

## III. PROPOSED SYSTEM

In this paper fully spread cooperative scheme for NPV, which allows a node, hereinafter called the verifier, to determine and validate the position of its communication fellow citizen is planned. This paper deals with a portable ad hoc network, where a ubiquitousinfrastructure is absent, and the position data must be got through node-to-node communication. Such a scenario is of certain interest since it leaves the door exposed for adversarial nodes to ill use

ISSN (Online) : 2278-1021
ISSN (Print) : 2319-5940

*International Journal of Advanced Research in Computer and Communication Engineering*
*Vol. 3, Issue 2, February 2014*

or interrupts the location-based services. The proposed approach is designed for freead hoc environs, and, as such, it does not depend ontheexistence of a trusted structure or of a priori reliable nodes and it also controls cooperation but agrees a node to achieve all verification techniquesseparately.

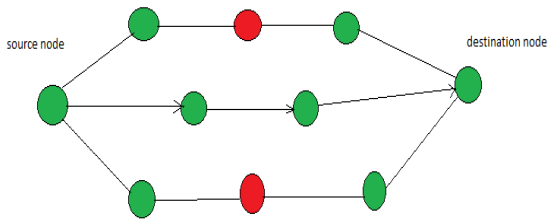



Fig 3.1 Verification and distance calculating using NPV

### 3.1 FURTHER ENHANCEMENT

In its elementary form, the Chinese remainder theorem will conclude a number *n* that when divided by some given divisors leave given remainders. In this proposed technique we enhance our work by discussing the use of the Chinese Remainder Theorem (CRT) for a novel forwarding scheme in Mobile adhoc networks aimed at combining low computational complexity and high performance. The proposed approach is characterized by a computationally simple packet splitting procedure able to reduce the energy needed for transmission.The proposed technique executes a splitting of the original messages in several packets such that each node in the network will forward only small packets. Finally, the receiver node will recombine all the packets received thus reconstructing the original message. In order to keep the computational complexity low we have chosen prime numbers as parameters for CRT Algorithm.

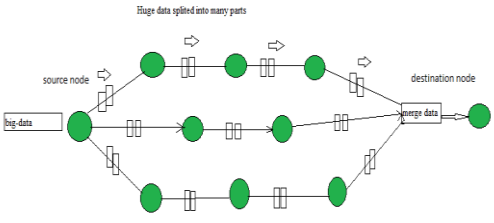



Fig 3.2 CRT method of data transmission process

**Advantages of Proposed System**

- Robust against independent and colluding adversaries Lightweight, as it generates low overhead traffic
- Does not require any infrastructure or a priori confidential neighbors
- Suitable for both low and high mobile environments
- Easily data can be transmit by using CRT Protocol

## IV. 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.