International Journal of Emerging Technology in Computer Science & Electronics (IJETCSE)
ISSN: 0976-1353 Volume 13 Issue 3 –MARCH 2015.

# A Secure Neighbour Position Verification and Discovery in MANETS

J.KUMARAN@KUMAR,
*Assistant Professor,Department of CSE,*
*Pondicherry Engineering College.*
kumaran@pec.edu

MOHAN PRASANNA. M,
*Department of CSE,*
*Pondicherry Engineering College.*
Mohan.prasanna07@gmail.com

***Abstract*- In a mobile ad hoc network, Position aided routing protocol enhance the performance over traditional ad hoc routing protocols. To improve the performance of routing protocol in ad hoc networks, Neighbor Position Verification (NPV) routing protocol has been used. Even though NPV improves the performance of the overall network, it leads to delay, loss of security while verifying the neighbor nodes and does not suitable for dynamic environments. In the proposed work, the node verification is achieved through the hash function. In hash function, hash id was generated by the source node to verify the neighbor nodes. Hash function has been introduced to improve the security and packet delivery ratio in MANET. Hash table facilitates the neighbour's node verifications.**

***Keywords* - Routing protocol, Neighbor position verification, MANET, verification protocol, hash function.**

## I. INTRODUCTION

In a wireless sensor network, sensor nodes observe the environment, identify the interest, produce data, and collaborate in progressing the data toward a sink, which could be a gateway, base station, storage node, or querying user. A Wireless network is defined as a group of two or more wireless devices which have the capability of communicating with each other without the support of any centralized administrator [1].

A MANET is a type of ad hoc network that can change locations and configure itself on the fly. Because MANETS are mobile, they use wireless connections to connect to various networks. This can be a standard Wi-Fi connection, or another medium, such as a cellular or satellite transmission. A Mobile Adhoc Network comprises a collection of independent mobile nodes that can connect to each other through radio waves. The mobile nodes that are present in radio range can communicate directly with each other, whereas others needs the intermediate nodes to route their packets. Each of the nodes has a wireless interface to interconnect with each other. Routing approach is a very challenging problem in a wireless network because of their mobile nature and a partial amount of resources. The designing of a reliable and efficient routing strategy is a very challenging problem in MANETs because of their mobile nature and limited amount of resources. Although MANETs are valuable in providing communication support where no fixed infrastructure exists, but due to the mobility and limited resources in MANETs, various issues are there which require high research. In ad hoc networks, congestion is one of the most significant issues. MANETs sometimes show unexpected behavior due to multiple data streams which leads to congestion resulting in high overhead, packet loss and long delays [2].

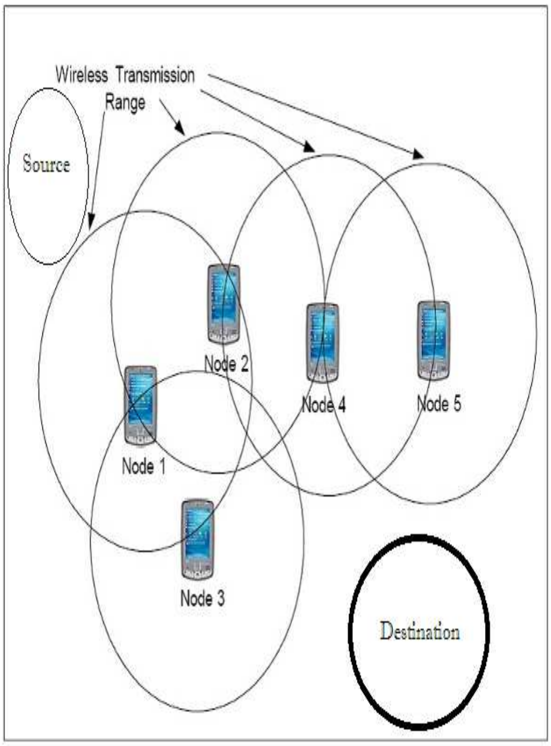


Fig. 1.Architecture of Mobile Ad hoc Networks with node transmission ranges

The rest of the paper will be organised as follows: In Fig.1, To described about the related works of the concepts. Explain about the proposed method. The implementation of our work is illustrated. Finally,draws conclusions with some remarks on future works.

## II. RELATED WORK

The authors in [3] have proposed an Asynchronous Distributed Data Collection (ADDC) algorithm with fairness, consideration for CRNs based on the PCR. Working with this PCR, an Secondary Users (SUs) can successfully conduct data transmission without troubling the activities of PUs and other SUs. ADDC collects data of a snapshot to the base station in a distributed manner without any time synchronization condition. The algorithm is scalable and more practical compared with centralized and synchronized algorithms. Through inclusive theoretical analysis, we show that ADDC is order-optimal in terms of delay and capacity, as long as an SU has a positive possibility to access the spectrum. Simulation results indicate that ADDC can effectually finish a data collection task and significantly moderate data collection delay.

In [4] the authors have presented an energy-efficient aggregation algorithm for WSNs that is secure and strong against malicious insider attack by any cooperated or faulty node in the network. The users require only certain aggregate functions of this distributed data. Computation of this collective data under the end-to-end information flow paradigm by communicating all the relevant data to a central collector node is a highly inefficient solution for this purpose. An alternative proposition is to perform in-network computation. The purpose of a wireless mobile network (WSN) is to deliver the users with access to the information of interest from data collected by spatially distributed mobiles. In contrast to the traditional snapshot aggregation approach in WSNs, a node in the proposed algorithm instead of unicasting its sensed information to its parent node, broadcasts its evaluation to all its neighbors. This makes the system more fault-tolerant and increase the information obtainability in the network. The simulations conducted on the proposed algorithm have produced result is used to validate its effectiveness.

In [5], the authors have proposed an energy efficient method for clustering the nodes in the network. Initially, mobiles identifying the same type of data are positioned within a different cluster. The remaining unclustered mobiles evaluate their divergence with respect to the clustered neighbors and ultimately join the least-divergent cluster. The overall performance of our proposed methods is evaluated using NS-2 simulators in terms of convergence rate, aggregation cycles, average packet drops, transmission cost and network lifetime. Finally, the simulation results establish the validity and efficiency of our approach. Periodic data sampling leads to enormous collection of raw facts, the transmission of which would rapidly deplete the mobile power. In their work they have performed data aggregation on the basis of entropy of the mobiles. The entropy is computed from the proposed local and global probability models. The models provide support in extracting high precision data from the mobile nodes.

In [6], the authors have presented the wormhole attack, a severe attack in ad hoc networks that is particularly interesting to defend against. The wormhole attack is potential, even if the attacker has not compromised any hosts and even if all communication provides authenticity and confidentiality. In the wormhole attack, an attacker records packets at one location in the network, tunnels them to another location, and retransmits them there into the another network. The wormhole attack can form a serious threat in wireless networks, especially against many ad hoc network routing protocols and location-based wireless security systems. They present a new, general mechanism, called packet leashes, for detecting and thus defending against wormhole attacks, and we present a specific protocol, called TIK, that implements leashes.

The authors in [8] have developed “Neighbor Position Verification” (NPV), a routing protocol designed to safe guard the network from adversary nodes by verifying the position of neighbor nodes to improve security, efficiency and performance in MANET routing. In a mobile ad hoc network, Position aided routing protocols can offer a significant performance increase over traditional ad hoc routing protocols. As position information is broadcasted to the enemy node to receive information. Routes may be disconnected due to dynamic movement of nodes. Such networks are more vulnerable to both internal and external attacks due to presence of adversarial nodes. These nodes affect the performance of routing protocol in ad hoc networks. So it is essential to identify the neighbours in MANET.

## III. PROPOSED SYSTEM

In an existing system, a wireless network that integrate a mobile wireless ad hoc network (MANET) and a wireless communications network has been confirmed to be a better unusual for the next generation wireless networks. The link between the nodes changes frequently in the highly dynamic environment. So, in the network the routing failure will occur which leads to packet loss during transmission.

To propose, a discovery and verification of neighbour’s position information in MANET routing protocols, and ways to use the position information to enhance performance and security of MANET routing protocols. We introduce, a hash function to protect the network from adversary nodes by verifying the position of neighbor nodes. To improve security, efficiency, and performance in MANET routing the link between the nodes modifies regularly.

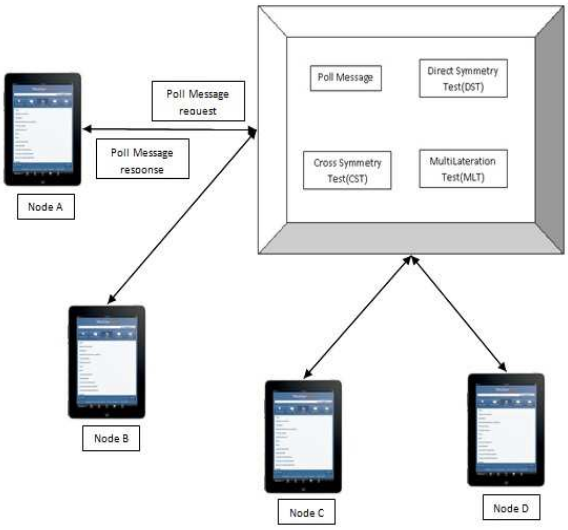


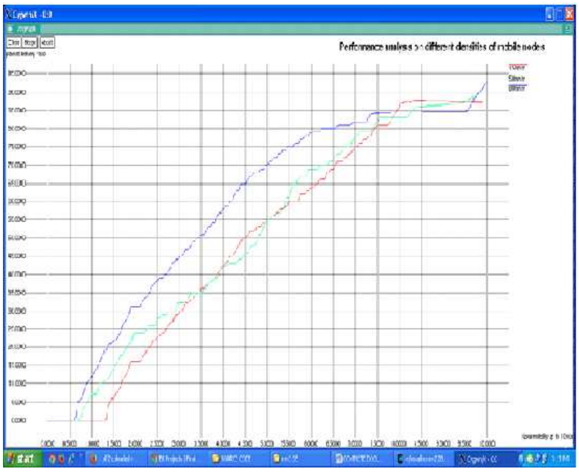
Figure 2 : Architecture diagram for node configuration

In hash function , the node verification is achieved through hash table. If the source node wants to verify the neighbor nodes, it will generate a hash id through the public key and source node id. In this source node wants to verify the neighbor nodes the source S generates a hash id through hash function H (n) = PUB_KEY/IDENTITY, the public key and id of source node generates hash id. The hash function includes the Advantages such as, verifications of neighbour’s node using hash table and High QoS performance in terms of overhead transmission delay, mobility-resilience, and scalability.

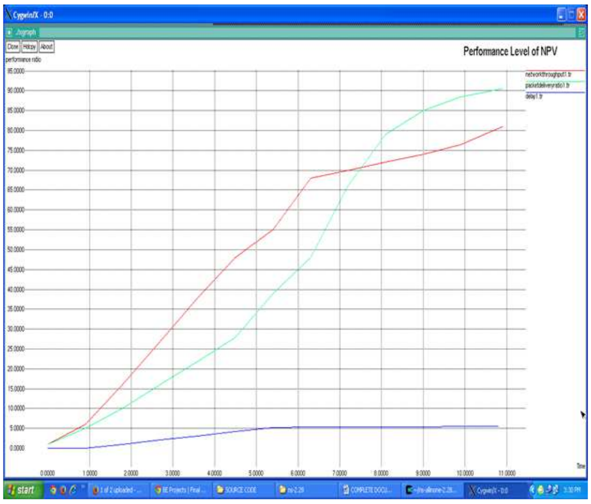
## IV. EXPERIMENTAL RESULT

In this section, To describe the simulations that have been performed on the proposed scheme. Graphical results are presented below.

The above graph illustrates the performance of throughput, which compares throughput for different node density. The above scenario indicates the performance of packet delivery ratio with the varying number of mobility nodes upto 10,000.



depicts packet delivery ratio with the increasing number of nodes.



Depicts packet delivery ratio, delay, throughput with the increasing number of nodes

The above graph describes about the comparison between the network throughput, packet delivery ratio, and the delay.

## V. PERFORMANCE EVALUATION

All mobile nodes are randomly scattered with a uniform distribution. Randomly select one of the deployed nodes as the source node.

To evaluate the proposed method with respect to the following metrics: PDR, Throughput, E2E latency, Packet loss ratio.

### Packet delivery ratio

It refers to the ratio of the number of report messages the sink receives to the total number of report messages the source node sends.

**QoS Throughput**

It is the ratio of the number of report messages the sink receives to the total number of report messages the source node sends.

**Packet loss ratio:**

It denotes the ratio of packets have been dropped during transmission time.

**End to end latency**

It refers to the time taken for a packet to be transmitted across a network from source to destination.

These parameter values are recorded in the trace file during the simulation by using record procedure. The recorded details are stored in the trace file. The trace file is executed by using the Xgraph to get graph as the output.

## VI. CONCLUSION

In many real time applications the technology such as MANET was used that allow the wireless devices to communicate with each other and also allow to access the information by exploiting external intermediate mobile nodes. The performance of routing protocol in MANET, was improved by using Neighbor Position Verification (NPV) routing protocol. NPV, leads to delay and does not provide security in identification of neighbor nodes. To overcome this issue the hash function was introduced for the node verification process. In hash function, hash id was generated by the source node to verify the neighbor nodes. At last to show the performance analysis with various parameters are resulting the improvement of proposed system. The results shows the effectiveness and efficient when compared to other existing system.

## REFERENCES

[1] Discovery and Verification of Neighbor Positions in Mobile AdHoc Networks (Marco Fiore, Member, IEEE, Claudio Ettore Casetti, CarlaFabiana Chiasserini)2013.

[2] P. Papadimitratos, L. Buttyan, T. Holczer, E. Schoch, J. Freudiger, M. Raya, 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, M. Poturalski, P. Schaller, P. Lafcade, 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.

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

[5] 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.

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

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

[8] R. Maheshwari, J. Gao, and S. Das, “Detecting Wormhole Attacks in Wireless Networks Using Connectivity Information,” Proc. IEEE INFOCOM, Apr. 2007.

[9] R. Shokri, M. Poturalski, G. Ravot and J.P. Hubaux, “A Practical Secure Neighbor Verification Protocol for Wireless Sensor Networks,” Proc. Second ACM Conf. Wireless Network Security (WiSec), Mar. 2009.

[10] M. Poturalski, P. Papadimitratos, and J.P. Hubaux, “Secure Neighbor Discovery in Wireless Networks: Formal Investigation of Possibility,” Proc. ACM Symp. Information, Computer and Comm. Security (ASIACCS), Mar. 2008.