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

State of the Art Design for the Spontaneous and Dynamic Detection of Adjacent Nodes in Mobile Ad Hoc Networks (MANETS) With Minimal Adversaries

Kavuri Venkataramu
M.Tech Student ,
Computer Science Engineering Department,
B V Raju Institute of Technology, Narsapur, Medak.

Dr.V.Ramesh
Professor,
Computer Science Engineering Department,
B V Raju Institute of Technology, Narsapur, Medak.

Abstract:

The global smart phone audience surpassed the 1 billion mark in 2012 and will total 1.75 billion in 2014. As per our research and expectation smart phone adoption to continue on a fast-paced trajectory through 2017. Nearly two-fifths of all mobile phone users—close to one-quarter of the worldwide population—will use a smart phone at least monthly in 2014. By the end of the forecast period, smart phone penetration among mobile phone users globally will near 50%. With increase of usage of smart phones, there will be an exponential increase in the peer-to-peer data transfer among smart phones. As a result we need newer methods of connectivity for data transfer among smart phones. In this paper we studying and implementing a method in which geographical position of the neighboring and adjacent nodes is determined. This system is having practical applications where in the need for location based services. Established Routes may perhaps be cut off due to technical issues or due to random movement of nodes.

Such types of evolving and changing networks are exposed to internal and external attacks owing to the existence of adversarial and rouge nodes. These rouge nodes disturb the overall performance of routing protocol in MANETS. As a result, it becomes very important to identify the geographical position of the neighbors. The "Neighbor Position Verification" (NPV), is a state of the art design in order to safeguard the network from adversary nodes by validating the true position of neighbor nodes to increase safety, effectiveness and overall performance.

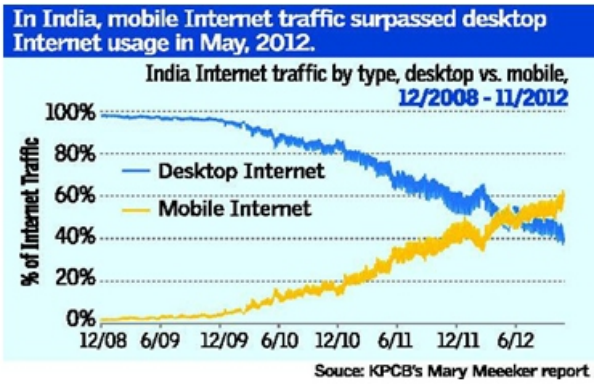
Keywords:

Neighboring nodes, neighbor location, location-based service, Mobile Networks, Rouge nodes.

Introduction:

A Smartphone is a mobile phone that performs many of the functions of a computer, typically having a touch-screen interface, Internet access, and an operating system capable of running downloaded apps. Aided by affordability of cheap Smartphones and availability of 3G and 4G networks the number of Smartphone users is supposed to reach around 1.75 billion users. Although the growth rate of mobile phone users has reached a threshold in developing countries, the burgeoning increase of users in Asia Pacific, Middle East & Africa is supposed to drive the number of mobile phone users to 4.5 billion users.

In 2012 around 1.58 billion users used their mobile phones for internet, which is around 67% of internet users. The number of users using mobile phones for internet grew by 21% to 1.91 billion users, which is around 74% of internet users. This number is further expected to increase by 17% in 2014 to 2.23 billion users, which is around 79% of total internet users. India is ranked fifth in number of smartphone users and has shown one of the highest year-on-year growth rates (in smartphones). It, however, ranks second in the addition of new users to the Internet over the last five years.



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

As smartphones are equipped with large screens, high resolution cameras and with advanced audio codecs, users are increasingly using these phones to share the Audio/Video/Image content. But this content sharing is still complicated as the data/content that is shared is not directly transmitted from one phone to other, but via various servers, which has various restrictions in terms of registrations etc.

Over the past few years, the number of smart phone users has rapidly increased. As smart phone interfaces are now convenient and user friendly, users can create various types of content.

However, content sharing remains troublesome. It requires several user actions, such as registration, uploading to central servers, and searching and downloading contents. One way to reduce a user's burden is to rely on an ad hoc method of peer-to-peer content sharing.

Although ad hoc networks can easily be constructed with smart phones as they are equipped with various network interfaces, such as Bluetooth and Wi-Fi, the connectivity between smart phones is expected to be intermittent due to the movement patterns of carriers and the signal propagation phenomena.

In this method, contents are spontaneously discovered and shared. The effectiveness of this sharing method depends on the knowledge of locations of adjacent and neighboring nodes. In this paper, we mainly focus on the verification & validation of the true positions of nodes in the network in the absence of prior trusted nodes.

Existing System:

Geographic routing in unstructured networks, data gathering in sensor networks, movement management among autonomous robotic nodes, location-based services for mobile devices, and danger threatening or traffic monitoring in vehicular networks are all examples of services that build on the availability of neighbor position information.

The precision of node locations is consequently an all significant issue in MANETS, and it becomes predominantly challenging in the existence of adversaries targeting at damaging the network.

Disadvantages of Existing System:

- Appropriately establish their location in spite of attacks feeding incorrect location information, and

- Validate the locations of their neighbors, so as to distinguish adversarial nodes proclaiming false locations.

Proposed System:

In this paper, we give more emphasis on the neighbor position verification (NPV). Unambiguously, we deal with a mobile ad hoc network (MANETS), where a universalstructure is absent, and the location information must be acquired through node-to-node communication. Such a situation is of specificconcernas it gives opportunity for adversarial nodes to abuse or disturb the location-based services.

Advantages of Proposed System:

- Our NPV scheme is compatible with state-of the-art security architectures, including the ones that have been proposed for vehicular networks.

- It is lightweight, as it generates low overhead traffic.

- It is robust against independent and colluding adversaries.

- It leverages cooperation but allows a node to perform all verification procedures autonomously.

The parameter to be considered in MANETS and related work:

1) Dynamic Neighbour Discovery

2) Movement Tracking

3) Mobility Learning

4) Discovering and Learning Meaningful Places

5) Mobility Prediction

6) Trustworthiness of Peer

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

1) Dynamic Neighbour Discovery:

A Neighbour discovery is an important task for routing protocols. Especially in delay-tolerant networking, efficient neighbour discovery significantly improves the performance of the routing protocols. However, most protocols validated with simulations do not address this issue as these protocols assume that nodes always perceive neighbours with frequent hello messages. In real implementations, frequent hello messages are not acceptable due to high energy consumption. In our implementation, we have found that the content sharing performance can be improved with a simple dynamic neighbour discovery. In dynamic neighbour discovery, each peer node can discover its neighbours by adding their neighbours in the database. This is achieved by adding peer name, port number and system name for each neighbour. Thus neighbours are easily discovered.

2) Movement Tracking:

In Life Map, the Activity Manager monitors the acceleration vector of a three-axis accelerometer and detects the motion of the user. Themotion detector function of the Activity Manager is basically a classifier M that has two outputs: moving or stationary. When the user is walking, running, or moving in a vehicle, the motion is classified as moving, whereas when the user stays at a certain location, the motion is classified as stationary.

3) Mobility Learning:

In daily life, people typically visit a number of places, but not all of these are meaningful for learning people's mobility. Indeed, DPD requires the discovery of locations where content sharing can be performed. Content sharing is successfully performed in places where Smartphone users stay long enough, as perceiving the existence of other nodes and message exchanging requires several minutes depending on the size of the message, the bandwidth, and the network interface.

Hence, we are basically interested in discovering places where the user stays longer than certain duration (i.e., meaningful places) and the context in user movement (i.e., paths).Currently available location technologies focus on providing geographical information. This information is insufficient to discover meaningful places because the physical location is not exactly generated at the same place despite the fact that a user generally has a similar life pattern every day. In addition, this information cannot distinguish a place that has a similar geocode but different floors. In modern society, places are normally located in multiple floor buildings. Thus, the logical information of meaningful places has more benefit to the proposed scheme as content sharing is conducted in indoor environments.

4) Discovering and Learning Meaningful Places:

Currently available location technologies focus on providing geographical information. This information is insufficient to discover meaningful places because the physical location is not exactly generated at the same place despite the fact that a user generally has a similar life pattern every day. In addition, this information cannot distinguish a place that has a similar geocode but different floors. In modern society, places are normally located in multiple floor buildings. Thus, the logical information of meaningful places has more benefit to the proposed scheme as content sharing is conducted in indoor environments.

5) Mobility Prediction:

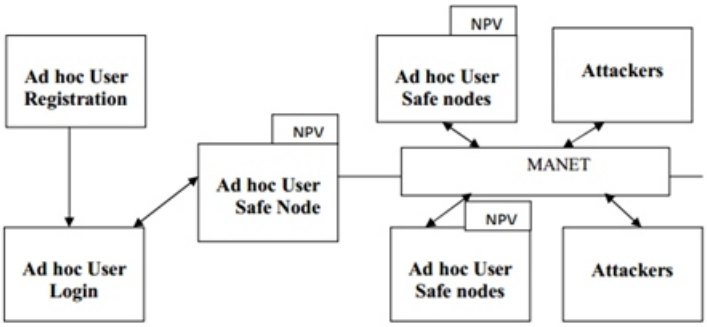
As DPD uses location information to estimate if a node approaches the destination of the content or diverges from the destination, the prediction of nodes' mobility information is essential.

6) Trustworthiness of peers:

Here we present distributed algorithms that enable a peer to reason about the trustworthiness of other peers based on past interactions and recommendations. Peers can create their own trust network in their proximity by using local information. Two contexts of trust, service, and recommendation are defined to measure trustworthiness in providing services and giving recommendations. Interactions and recommendations are evaluated based on importance, recentness, and peer satisfaction parameters.

NPV in MANETS:

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



We propose a fully distributed cooperative scheme for NPV, which enables each node, to discover and verifythe position of its communication neighbors.

For clarity, here we summarize the steps of npv algorithm,In this algorithm used to check with their neighbour position and secure transmission of content to the properdestination.

The below steps are used to explain the NPV algorithm.

step 1: discover nodes in range.
step 2: send request to nodes
step 3: wait for connection
step 4: get location from peers with time.
step 5: maintain location table
step 6: broadcast the location to other nodes
step 7: get response from other
step 8: verify the destination location and response from other nodes
step 9: check for location data at every request or operation
step 10: if the location of peer is invalid mark it as spam (by its mac id)
step 11: broadcast the spammed peer mac id to all other nodes.

Neighbour position verification in each node:

In a mobile ad hoc network without knowing neighbour node position which makes a chance to attackers toeasily enter into the network. If neighbour position verification done in separate node, then it would be a timeconsuming process.

In previous works neighbour node check done through separate nodes. In this way ofapproach made a less performed application.

User registration and login for ad hoc usage:

Every application needs to allow authorized user through authentication process. In this stage it's used tocreate the ad hoc user for this application using both registration and login for ad hoc user screen. To avoidattackers in mobile ad hoc network this login and registration process is preliminary task to provide security. Adhoc user registers their account in this application. Those who are already registered their account in thisapplication; they can access their account through login. In this ad hoc user login and registration provideauthentication check in this paper.

Discover own location and neighbour location:

Discovering own location and neighbour location is tedious task in mobile ad hoc network. In this stage ofprocess it's used to find the own location and Neighbour location through the wifi integrated service. Thesefindings are used to involve in the neighbour position verification. This verification is done through the NPValgorithm. Secure transmission in mobile ad hoc network is complex and it's achieved by NPV algorithm.

Connection between neighbour nodes :

Connection establishment with neighbour and accept connection by their neighbours made a connection more secure. In this stage it's used tofollow initial security mechanism through the cryptography techniques. Connections with their neighbours areestablished here using AES cryptography technique. Connection need to be accepted in both ends then onlysource can sent secure message transaction. Neighbour position verification algorithm used to check all withtheir neighbour through above mentioned steps to verify their neighbours.

Secure content transaction:

In final stage of this application implementation is secure content transaction to secure discoveredneighbour destination. Position verification done through NPV algorithm and the message and attachments,whatever I need to send to thesecure neighbour are happened to be here.

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

Use send option after attachments and secure neighbour nodeselected.

Robustness Analysis:

Jamming:

This is the only external attack that can harm the system. Any adversary (internal or external) can jam thechannel and erase REPLY or REPORT messages. However, to succeed, M should jam the medium continuouslyfor a long time, since it cannot know when exactly a node will transmit its REPLY or REPORT. Or, M coulderase the REVEAL, but, again, jamming should cover the entire Tjitter time. Overall, there is no easy point totarget: a jammer has to act throughout the NPV execution, which implies a high energy consumption and is adisruptive action possible against any wireless protocol. In addition, mobility makes it harder to repeatedly jamdifferent instances of the NPVprotocol run by the same verifier.

Clogging:

An adversary could initiate the NPV protocol multiple times in a short period and get repeated REPLY andREPORT messages from other nodes, so as to congest the channel. In particular, REPORTs are larger in size,thus likely cause the most damage. However, NPV has a way of preventing that: the initiator must unveil its identity before such messages are transmitted by neighbors. An exceedingly frequentinitiator can be identified, and its REVEALs ignored, thanks to the use of certified keys. REPLYs instead aresmall in size and are broadcast messages (thus require no ACK): their damage is limited, but their unnecessarytransmission is much harder to thwart. Indeed, REPLY messages are sent after an anonymous POLL; such ananonymity is a hard-to dismiss requirement, since it is instrumental for keeping the identity of the verifierhidden. As a general rule, correct nodes can reasonably self-limit their responses if POLLs arrive at excessiverates.

Sybil and Relay (Wormhole) Attacks:

An adversary can assume several trusted identities, M ¼ fM1; . . .;MIg, if 1) it owns several certificated pairs ofpublic/private keys (Sybil attack), or 2) it impersonates colluding adversaries at the end of wormholes.

Theavailability of several identities could be used by an adversary to acquire its neighbor positions, i.e., to becomeknowledgeable. However, as shown in Section 6.1, attacks launched by independent, knowledgeable adversarieshave no chance of success. Furthermore, by announcing timings that are consistent among the identities inM, the adversary can behave as a group of colluders of size I.

Conclusion:

Methods for discoveryof neighbors efficiently in a non prioritrusted environment are studied and discussed. The suggested techniqueswill ultimatelyoffer security frommalicious nodes. Theprotocol is robust to adversarial attacks. This protocol willalso update the position of the nodes in an activeenvironment. The performance of the proposed scheme willbe effective one. Future work will aim at integrating the NPVprotocol in higher layer protocols, as well as at extending it to a proactive paradigm, useful inpresence of applications that need each node to constantly verify the position of its neighbors.

References:

[1] Marco Fiore,Claudio Ettore Casetti and Panagiotiespapadimitratos " Discovery And Verification OfNeighbor Position In Mobile Ad Hoc Networks",Members IEEE,feb 2013

[2] R. Maheshwari, J. Gao, and S. Das, "DetectingWormhole Attacks in Wireless Networks UsingConnectivity Information," Proc. IEEE INFOCOM,Apr. 2007.

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

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

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

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

[6] S. Zhong, M. Jadliwala, S. Upadhyaya, and C. Qiao, "Towards a Theory of Robust Localizationagainst 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 HocNetworks," 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 Attacksin Wireless Networks," Proc. IEEE INFOCOM, Apr. 2003.

[9] J. Eriksson, S. Krishnamurthy, and M. Faloutsos, "TrueLink: A Practical Countermeasure to theWormhole Attack in Wireless Networks," Proc. IEEE 14th Int'l Conf. Network Protocols (ICNP), Nov. 2006.

[10] R. Maheshwari, J. Gao, and S. Das, "Detecting Wormhole Attacks in Wireless Networks UsingConnectivity Information," Proc. IEEE INFOCOM, Apr. 2007.

[11] R. Shokri, M. Poturalski, G. Ravot, P. Papadimitratos, and J.P. Hubaux, "A Practical SecureNeighbor Verification Protocol for Wireless Sensor Networks," Proc. Second ACM Conf. Wireless Network Security (WiSec), Mar. 2009.

[12] M. Poturalski, P. Papadimitratos, and J.-P. Hubaux, "Secure Neighbor Discovery in WirelessNetworks: Formal Investigation of Possibility," Proc. ACM Symp. Information, Computer andComm. Security (ASIACCS), Mar. 2008.

[13] M. Poturalksi, P. Papadimitratos, and J.-P. Hubaux, "Towards Provable Secure NeighborDiscovery in Wireless Networks," Proc. Workshop Formal Methods in Security Eng., Oct. 2008.

[14] E. Ekici, S. Vural, J. McNair, and D. Al-Abri, "Secure ProbabilisticLocation Verification inRandomly Deployed Wireless Sensor Networks," Elsevier Ad Hoc Networks, vol. 6, no. 2, pp.195-209, 2008.

[15] J. Chiang, J. Haas, and Y. Hu, "Secure and Precise Location Verification Using DistanceBounding and Simultaneous Multilateration," Proc. Second ACM Conf. Wireless NetworkSecurity (WiSec), Mar. 2009.

[16] S. _Capkun, K. Rasmussen, M. Cagalj, and M. Srivastava, "Secure Location Verification withHidden and Mobile Base Stations," IEEE Trans. Mobile Computing, vol. 7, no. 4, pp. 470-483,Apr. 2008.