Improving Performance of Neighbor Discovery in MANET by using Threshold value and Time out Parameter

Anuradha T. Thakre
Department of Computer Engg
Dr. D. Y Patil College of Engg.
Ambi , Talegaon, Pune

Sandeep Kadam
Department of Computer
Dr. D. Y Patil College of Engg.
Ambi , Talegaon, Pune

ABSTRACT

In Mobile Ad Hoc network (MANET), various protocols and known location services that are used keeps growing, it is necessary for MANET mobile nodes to identify their neighbor's position for effective and truthful communication. However, this MANET process is quite negotiable by attacking mobile node and retrieving their information of respective locations in MANET. Hence it is very essential to have proficient method of discovering neighbors to avoid such attacks for high level security. In recent days, various methods are presented for verifying neighbor positions, but those methods absorbs few limitations with respect to performance. In this paper, "Improving Performance of Neighbor discovery In MANET by Using Threshold value and Time out parameter" the protocol offers false positive and false negative rate improvement within the existence of various attacks for improving the performance of an existing method (NPV) parameters such as; threshold value and time out are introduced. This new protocol fundamentally deals with Mobile Ad Hoc network where a persistent infrastructure is unavailable and the location identification is necessarily learnt via. Node to node communication. Such scenario is highly noticeable because it has a loophole for oppositional nodes to abuse the location based services.

Keywords

Ad hoc networks, Neighbor position verification, mobile Ad Hoc Networks, Security, False Positive, False Negative.

1. INTRODUCTION

A Mobile Ad Hoc Network is defined as a set of self decisive mobile nodes that can communicate to each other by means of radio waves. The mobile nodes which are present in radio range of each other can communicate directly, while others need the support of intermediate nodes to route their packets in network. Each of the nodes has a wireless interface to communicate with each other. These networks are fully distributed; means can work at any place without the help of any permanent infrastructure such as access points or base stations. The most essential necessity of Ad Hoc network is that they are "self-configuring", that means almost all wireless nodes have a capability to rearrange themselves proficiently to perform the task of an application that has been deployed. Post deployment, as their neighbor's information is not available hence, they need to find out their neighbors position for communication within them. Having knowledge of neighbors is very critical for most of the routing protocols because this (Neighbor Discovery) stands as the very initial step in self organization in a wireless Ad Hoc network. Neighbors can act as; Physical neighbor or Communication neighbor, the physical neighbors are known because of their presence within physical proximity of the discoverer. However the communication neighbors can be within physical range or out of it for communication. Communication that is time based and mechanisms such as media access control are dependent on appropriate neighbor information. For proper wireless network functionality 'Neighbor Discovery' is the key to it. Neighbors are mostly termed as node that exists within radio range of an available node. Hence, discovering the neighbors can also be assumed as the exploration of the volume of space nearby a wireless node. Wireless communications are always open for the attackers to misuse because attackers always have the liberty to do malicious activities that can range from simple service rejection activity to complex fraud. Node locations accuracy is thus an important aspect in mobile networks, which is specifically challenging in existence of oppositional aiming for the systems to be harmed. Within such cases, it is important to have a resolution to enable nodes for building their location details regardless of incorrect location information feeded by an attacker. For detecting the fake locations of oppositional nodes, there must be a mechanism to authenticate the neighbor's position.

Within this paper presentation the issues that are related to neighbor position verification (NPV) has bring forth. In literature various methods are presented but there are no easy methods of having existing NPV recorded issues which are seen to be functional in an open wireless network surrounding without keeping faith on trusted nodes. The very recent remedy to the problem has been brought into light in [1]. So one new set of rule to be represented in NPV which permit any wireless node in a mobile Ad Hoc network for continuously verifying the position of their nearer communication neighbor node without depending on priori faithfully nodes. But further this mechanism has also some drawbacks related to false positive and false negative rates underneath the occurrence of various attacks. Thus there is need to expand the existing algorithm and presented it in proposed system. And this expanded system only concentrates on improving the false positive and false negative rate proactively and also improving the performance in this section. After that the survey on various methods to be included in the literature reviews. In third part the proposed scheme and its overall architecture is illustrated. Then in forth segment the results which are getting from expanding system is to be displayed. And at last the conclusion and future scope will be forecasted.

2. LITERATURE REVIEW

[1] In Analysis of Black Hole Attack on MANETs Using Different MANET Routing Protocols", Irshad Ullah, Shoaib Ur Rehman.

In this base paper, Security which is the most important aspect in wireless adhoc network is being analysed. Attach discussed here affects the performance of system. Black Hole attach is one of the security threat where traffic is routed to such a node that doesn't exist in the network. The study carried out here shows the effects of Black Hole attack in MANET by using both Proactive & Reactive routing protocols (OLSR & AODV). This security attack has a direct impact on the performance of system and thus comparative analysis of this attach is taken into account by using both these protocols. **Extracting Idea for dissertation:** From this paper the proposed system referred the concept of attacks in reactive as well as proactive protocol.

[2] Efficient Algorithms for Neighbour Discovery in Wireless Networks", Sudarshan Vasudevan, Micah Adler, Dennis Goessel, Fellow, IEEE, and Don Towsley, Fellow, IEEE, ACM.

In this paper, neighbour discovery algorithms that are used (Randomized and Deterministic) represent an efficient algorithm for wireless networks that address various limitations of earlier approaches. In Randomized neighbour discovery; every node transmits at randomly chosen times and discovers all its neighbours by a given time with high probability where as in Deterministic neighbour discovery every node transmits according to a pre-determined transmission schedule that allows to discover all its neighbours by a given time with probability one. These algorithms do not require estimates of node density and allow asynchronous operation. In addition to this, these algorithms allow nodes to begin execution at different times and also allow nodes to detect termination.

Extracting Idea for dissertation: From this paper, each node transmits at randomly chosen times and discovers all its neighbours by a given time with high probability, each node transmits according to a predetermined transmission schedule that allows it to detect all its neighbours by a given time with probability one. The antenna models used in ad hoc networks are directional antenna model or Omni directional antenna model.

[3] On Neighbour Discovery in Wireless Networks with Directional Antennas", Sudarshan Vasudevan, Jim Kurose, Don Towsley, Jim Kurose, Don Towsley.

The proposed two classes of probabilistic neighbour discovery algorithms that are; Direct-Discovery algorithm and Gossip-Based algorithm have considered the problem of neighbour discovery in wireless networks with directional antennas within this paper. The working of these algorithms is considered in a slotted, synchronous system and find the transmission probability the maximizes the probability of discovering its neighbours. In Gossip-Based algorithm, the time required to discover a given fraction of neighbours remains unaffected with the increase in node density. Another interesting property of Gossip-Based algorithm is that it operates without any modification even if only a fraction of nodes have location information. Its performance degrades significantly when none of the nodes have location information compared to that of Direct-Discovery algorithm. In Direct-Discovery algorithm, nodes discover their neighbours only when they hear transmissions from their neighbours where as in Gossip-Based algorithm, nodes gossip about location information of their neighbours.

Extracting idea for Dissertation: The technique used to discover the neighbours is recording the angle of arrival of the beacon signal, determining the location based using GPS. The direct discovery algorithm will discover those neighbours that communicate with it directly, the neighbours are discovered indirectly through the interaction with other neighbours. Messages are exchanged which helps in discovery of the neighbours. The message contains list of neighbours‟ IDs and their locations. The main drawbacks of gossip based algorithm are message length grows as more and more nodes are discovered and the presence of physical obstacles may cause nodes to incorrectly infer another node as its neighbour.

[4] Improved Security in Geographic Ad Hoc Routing through Autonomous Position Verification", T. Leinm¨ uller, C. Maih¨ofer, E. Schoch, F. Kargl.

In this paper, the mechanisms to detect and mitigate the influence of false position information in geographic routing protocols have been developed. In distinct to other position verification approaches, this doesn't rely on special hardware to measure signal strengths or time-to flight nor does it rely on preinstalled infrastructure networks. To improve reliability of position information; the goal here is to quickly estimate the positions of trustworthy nodes who claim of being their neighbored node. This method will not completely eliminate malicious nodes from using false position information but it will significantly limit on having options of fake positions resulting reduction in possibility of leaving space for attackers to make use of fake positions. Since the position dissemination is critical for geographic routing, fake position information has severe impact on performance as well as security. The mechanism of malicious node detection not only reduces the choice of fake position but also prevents malicious node from using the false position information. Therefore, potential attackers using faked positions information are significantly reduced.

Extracting idea for Dissertation: From above paper the new scheme is presented for NPV protocol which allows nodes to validate the position of their neighbors through local observations only. This is done by checking whether subsequent positions announced by one neighbor draw movement over time that is physically possible. The limitation of this method is an adversary can fool the protocol by simply announcing false positions that follow a realistic mobility pattern.

[5] In Secure neighbor discovery in wireless networks: Formal Investigation of Possibility", Poturalski, P. Papadimitratos, and J. Hubaux.

In this paper the problem of secure neighbor discovery in wireless network is investigated where a formal framework is build to provide specifications of neighbor discovery. Here the two general classes of protocol i.e. Time-Based protocol and Location-Based protocol are proposed to investigate the problem of secure neighbor discovery. T-Protocol class has a fundamental limitation governed by a threshold value based on neighbor discovery range and is proven that no T-Protocol can have solution for neighbor discovery problem if unfavorable nodes transmits messages faster than that of its threshold. This result of T-protocol stood a key measure to have further investigation done on other classes of protocols. TL-protocol in extension brought this limitation to an end with a justifying solution to neighbor discovery problem. In particular, it is proved that TL-Protocol has no such limitations and can solve the neighbor discovery problem as long as the Time and Location measurements are accurate.

Extracting idea for Dissertation: The problem investigation of secure neighbor discovery offers an impossibility proof showing that time-based protocols will not guarantee SND unless the environment is free of obstacles and the distance between neighbors is small.

[6] In MANET: Vulnerabilities, Challenges, Attacks, Application", Priyanka Goyal, Vinti Parmar, Rahul Rishi.

Devices in mobile Ad-Hoc network should be able to detect the presence of other devices in the network and perform necessary setup to smoothen the progress of communication, Data sharing and other related services of message routing. Because of nodal mobility the network topology may change rapidly and unpredictably over time. In decentralized network, message routing is a problem where topology keeps fluctuating and in such decentralized network environment message delivery must be taken up by the nodes itself. MANET is more open than wired network because of mobile nodes, threats from compromised nodes within the network, limited physical security, changing topology and lack of centralized management leaving a gap for malicious attacks. The related work for above paper was that the popularity, efficiency and some great features of MANET like their decentralized set up, use anytime, anywhere and cheap communication has been discussed. Also this contains an overview of routing protocol and their applications. But along with above characteristics there are discussed some challenges, attacks and vulnerabilities in MANET. One major drawback is related to security, limited bandwidth and power.

Extracting idea for Dissertation:

From this paper, the system acquires the various applications as well as routing protocols for MANET. It also deals with security issues.

[7] In Secure Location Verification for Vehicular Ad-Hoc Networks", J.-H. Song, V. Wong, V. Leung.

In this base paper, for detection of location spoofing attack has been overcome by using an infrastructure less Secure Location Verification scheme. In this paper main focus is on the secure location and RF based distance bounding routing protocol which is used for preventing the occurrence of malicious nodes. Also this scheme deals with the Time of flight technique for measuring the distance between pairs of nodes and increase the ratio higher packet send in network. SLV scheme guarantees the minimum distance between fake and estimated location of power by a certain value. The results have demonstrated that in the presence of position spoofing attackers; SLV can identify such vehicles and avoid them from being used as forwarders. SLV give way to a higher packet delivery ratio than both APV and Greedy forwarding especially when there are black-hole attackers in the ad-hoc network.

Extracting idea for Dissertation:

For proposed system one method is used which exploits Time-of-Flight distance bounding and node cooperation to mitigate the problems of the previous solutions.

[8] In SECTOR: Secure Tracking of Node Encounters in Multi-Hop Wireless Networks", S. Capkun, L. Butty an, and J. Hubbub.

As explained in an introduction, one scheme is represented i.e. SECTOR (Secure Tracking of Node Encounters in Multi Hop wireless Networks) which deals with secure verification of time encounters between nodes in multi hop network by using distance bounding techniques along with clocks. These set of protocols are build on well-established cryptographic techniques including Hash chains and Merkle hash trees. This solution has been applied to various problems including prevention of Worm-hole attacks, securing routing protocols based on last encounters as well as cheating detection by means of topology tracking. This solution is very likely to be the first solution for addressing secure topology problem and encounter attacking along with an exception of worm-hole attack prevention. It includes the analysis of communication, storage problem. This work addresses the problem of changing topology security.

Extracting idea for Dissertation:

From this paper proposed system tracking the node encounters and using these encounters for verification of identity. As the authentication phase of SECTOR relies on nanosecond clocks and special hardware, it is impractical for many adhoc networks. Time-based solutions, however, face a common constraint.

[9] In Packet leashes: A Defence Against Wormhole Attacks in Wireless Networks ", Y. Hu, A. Perrig, and D. Johnson.

The wormhole attack is possible even if the attacker has not compromised any hosts, and even if all communication provides authenticity and confidentiality. This paper includes the technique for defending the occurrence of wormhole attack which directly affects on the security in network. This also affects on the transmission of packets in communication. 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. It uses one common method i.e. Time of Flight. To defend from this problem one technique was used called as "Packet Leashes". It restricts the maximum transmission distance of a packet. The general mechanism 'Packet Leashes' represented here is for detecting and thus defending against wormhole attacks by presenting a very specific protocol named as TIK. To implement temporal leashes, the design and performance analysis of this efficient protocol (TIK) provides instant authentication of received packets.

Extracting the Idea for Dissertation:

This paper gives Time-based solutions attempt to leverage time-of-flight measurement to ensure that transmitting nodes lie within the local neighborhood. Packet leashes are known example of this approach.

[10] Secure Neighbourhood Discovery: A Fundamental Element for Mobile Ad Hoc Networking", P. P. Papadimitratos, M. Poturalski, P. Schaller, P. Lafourcade, D. Basin, S. Capkun, and J.-P. Hubaux.

As explained in an above paper, the neighbourhood discovery is the most crucial step for wireless communication with changing topologies. Here the focus is on this problem and provide definitions of neighbourhood and ND protocol properties and also as a broad classification of attacks. Two types of NDs like Physical and communication which are very useful for communication. But for providing the security for neighbour discovery used various methods like distance bounding. Also discuss about some attacks and vulnerabilities.

Extracting Idea for Dissertation:

This paper provides an overview of the problems and challenges associated with Secure Neighborhood Discovery

(SND) and also include a set of real-world examples illustrating various threats to neighborhood discovery.

[11] In Neighbour Discovery in Mobile Ad Hoc Self-Configuring Networks with Directional Antennas: Algorithms and Comparisons”, Zhensheng Zhang and Bo Li.
In this paper the problem related to neighbor discovery with directional antennas. In this technique the Omni antenna algorithm is used for transmission but this having some limitation. So by using bidirectional antenna algo which use for two way communication. So by using this method the issue related to transmission in directions to be solved.
Extracting Idea for Dissertation:

This method is used for propagating the signals in all directions. The algorithm used by Omni directional antenna is 1-way algorithm and the receiver will not send any acknowledgement after receiving the discovery message.

[12] In Discovery and Verification of Neighbour Positions in Mobile Ad Hoc Networks”, Marco Fiore, Member, IEEE, Claudio Casetti, Member, IEEE, Carla-Fabiana Chiasserini, Senior Member, IEEE,Panagiotis Papadimitratos, Member, IEEE.
This paper includes one method for verifying the position of neighbour position in distributed approach. This is used providing robustness against various attacks for neighbour position. The position and location aware services can be easily disrupted by using an adversarial node in network. So one cooperative solution has been forwarded with the help of cooperative neighbor position verification protocol. And most important factor about this protocol is that the result can thwart more than 99% of attacks under possible conditions. All process should proceed by network nodes only.
Extracting Idea for Dissertation:
From above method the proposed system requires the nodes which are used to verify the position of the neighbors that the nodes declare.

3. PROPOSED DESIGN FRAMEWORK

3.1 Problem Definition

Even if the past research brings a huge number of Ad Hoc security protocols deals with some issues that are correlated with verification of neighbor position, there is not present any frivolous, strong explanation to neighbor position verification that may work separately in an unlock, persistent surrounding, without trusting on any faithful wireless nodes. For both high and low movable situations the majority of answers are not appropriately. So one modern resolution is put forth for avoiding this issue in [1].

So one new protocol (NPV) is to be represented in this paper, which gives a permission to any wireless nodes to continuously verify its neighbor’s position in network devoid of trusting on a priori faithful nodes. The practical implementation of this protocol is viewing that it do better than all other existing protocols and improves the efficiency. But this NPV protocol is again undergo some pitfalls that are related to the rates of false positive and False negative in presence of various attacks and also recover the performance of existing system. Hence, for overcoming these restrictions, an existing protocol is further want to expand along with proactive surroundings. And also improve the performance by adding two parameters like threshold value and time out entity. Boundaries of an Existing structure:

- Low performance.
- Not supported for proactive environment.
- False positive and false negative rates should be lower.

3.2 Proposed Structural Design

Therefore, this proposed system signifies the expanded version of Neighbor position Verification protocol. The main purpose of this system is to improve the FPR and FNR, along with different kinds of attacks. Also extend the functioning of existing NPV proactively in wireless Ad Hoc network. Two parameters i.e. threshold value and time out are to be included for improving the performance.

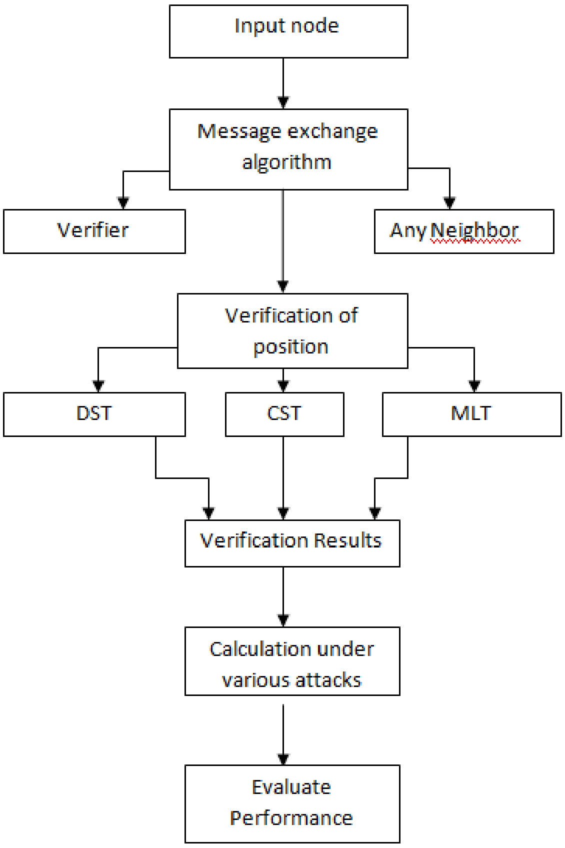

Figure 1. Proposed Design

And this new developed technology is termed as IPND (Improving the Performance of Neighbor Discovery) which having the mobile Ad hoc network where a persistent communication is not present. And using node to node communication the proposed system can easily get the node location information. The realistic implementation of newly developed system will do by using the JAVA platform and evaluate its performances against the existing protocols. Also it supports for getting high efficiency. There is present a mathematical model for implementation.

MATHEMATICAL MODEL

1. A node X in MANET has its position p with max. error er, time reference tr. For Security purpose each node X in MANET has its private key kx, public key Kx, one time use key (k’x, K’x)
   X € {p, tr, kx, Kx, (k’x, K’x)} where
   X = node in system
   P= own position of node

Tr= time reference of node
Kx = private key of node
Kx = public key of other nodes
(k'_x, K'_x) = One time use key

- **Message exchange**

The value pX is the current position of X, and NX is the current set of its communication neighbors. We denote by tX the time at which a node X starts a broadcast transmission and by tXY the time at which a node Y starts receiving it.

1. Verifier S initiates protocol.
2. S broadcast poll massage with public key k's.
3. S → *(poll, K's)
4. X € Ns receives poll massage
5. S : store tXS i.e. receiver time
6. If Tx elapsed
   Broadcast reply massages with MAC
7. After a time Tmax + Δ + Tjitter, the verifier broadcasts a REVEAL message using its real MAC address.
   Δ= propagation and contention lag of reply massage
   Tjitter= random time
   Reveal (ms, EkS{hK′S}, pk)
   Ms= associates each commitment cX received by the verifier
   EkS{hK′S},= encrypted hash
   Pk= certified public key
8. Reveal massage broadcast, each neighbor X that previously received S's POLL unicasts to S an encrypted, signed REPORT message.
9. Report (xp, Tr, lr, Trid)
   Xp= X node position
   Tr= traission time of reply massage
   Lr= list of pair reception time
   Trid= temporary idetintity of reply massage

- **Message verification**

1. Once the message exchange is concluded, S can decrypt the received data and acquire the position of all neighbors that participated in the protocol, i.e., {pX, ∀X ∈ NS}.
2. The verifier S also knows the transmission time tS of its POLL and learns that of all subsequent REPLY messages, i.e., {tX, ∀X ∈ NS}, as well as the corresponding reception times recorded by the recipients of such broadcasts, i.e., {tXY , ∀X, Y ∈ NS ∪{S}}.
3. Applying a ToF-based technique,
4. S thus computes its distance from each communication neighbor, as well as the distances between all neighbor pairs sharing a link
5. By denoting with c the speed of light, the verifier computes, for any communicating pair (X, Y) with X, Y ∈ NS ∪ {S}, two distances: dXY = (tXY − tX) · c, from the timing information related to the broadcast message sent by X, and dY X = (tY X − tY) · c, from the information related to the broadcast message by Y .

- **Direct Symmetry Test (DST)**

1. There, |·| denotes the absolute value operator and kpX − pY k the Euclidean distance between locations pX and pY .
2. In the **DST**, S verifies the direct links with its communication neighbors.
3. To this end, it checks whether reciprocal ToF-derived distances are consistent (i) with each other, (ii) with the position advertised by the neighbor, and (iii) with a proximity range R.
4. For all node in system, the first check verifies that the distances dSX and dXS, obtained from ranging, do not differ by more than twice the ranging error plus a tolerance value ϙm
5. Check dsx > R then node is faulty

- **Cross-Symmetry Test (CST)**

1. It checks on the information mutually gathered by each pair of communication neighbors. The **CST** ignores nodes already declared as faulty by the **DST.**
2. For all other pairs (X, Y), the **CST** verifies the symmetry of the common distances, their consistency with the positions declared by the nodes and with the proximity range.
3. For each neighbor X, S maintains a link counter lX and a mismatch counter mX. The former is incremented at every new cross-check on X, and records the number of links between X and other neighbors of S
4. Specifically, X is added to FS or US, depending on whether the ratio of the number of mismatches to the number of checks is greater or equal to a threshold δ.
5. If such a ratio is less than δ, X is added to a temporary set WS for conditionally verified nodes.
6. If δ is high then it is high positives.

- **The Multilateration Test**

7. For each neighbor X that did not notify about a link reported by another node Y , with X, Y ∈ WS, a curve LX(S, Y) is computed and added to the set LX.
8. Time Difference of Arrival at S and Y matches that measured by the two nodes, i.e., |tXS − tXY |.
9. It is easy to verify that such a curve is a hyperbola, with foci in pS and pY , and passing through the actual position of X

10. Once all couples of nodes in WS have been checked, each node X for which two or more notified links, hence two or more hyperbolas in LX, exist is considered as suspect

11. X is moved to the faulty set FS. At the end of the test, all nodes still in WS are tagged as verified and moved to VS.

4. SOFTWARE SPECIFICATION

4.1 Input

The Network scenario that consists of mobile nodes are the Input for realistic execution.

4.2 Hardware and Software Used

1. **Processor** - Pentium –IV
2. **Speed** - 1.1 GHz
3. **RAM -** 256 MB (min)
4. **Hard Disk** - 20 GB
1**. Operating System -** Windows XP/7/8

2. **Programming Language:** JAVA
3. **Technology Used -** J2ME
4. **Development IDE-** Net Beans.
5. **Analysis & Designing Tool:** Rational Rose

4.3 Results of Work Done

The results in Figure 2 are analysed based on the type of attack launched by the fortunately adversary, and are defined to the impact of the transmission range, since another parameters did not show significant effect on the displacement of fortunate attackers.

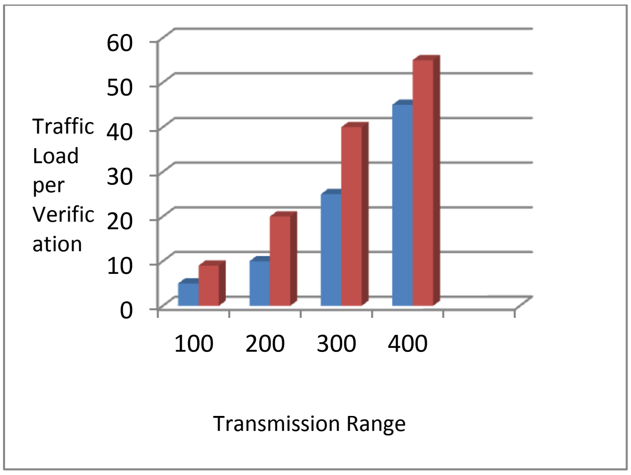

Figure 2. Performance Enhancement Graph

5. ACKNOWLEDGMENTS

Today, on completion of my project thesis I take this opportunity to express my profound gratitude and deep regards to my guide (Prof. Sandeep Kadam) for his exemplary guidance, monitoring and constant encouragement throughout the course of this thesis. The blessing, help and guidance given by him time to time hall carry me a long way in the journey of life on which I am about to embark. I am obliged to staff members for the valuable information provided by them in their respective fields. I am grateful for their cooperation during the period of my assignment. Lastly, I thank almighty, my parents and friends for their constant encouragement without which this assignment would not be possible.

6. CONCLUSION & FUTURE SCOPE

The proposed techniques will eventually provide prevention from occurring the malicious node and also provide the security from malicious nodes. The protocol is robust to adversarial attacks. This protocol will also update the position of the nodes in an active environment. The performance of the proposed scheme will be effective one. The proposed system conferred extended version of NPV protocol with aim of improving the false positive and false negative rates under the existence of diverse attacks as well as enlarge the working of NPV under the proactive hypothesis successfully. To improve the performance the proposed system has included the threshold value and time out parameters updating to the existing NPV protocol. This new protocol is named as ENPV (Extended NPV) which basically deal with a mobile ad hoc network, where a pervasive infrastructure is not present, and the location data must be obtained through node-to-node communication. The practical analysis of proposed protocol will do by using the JAVA technology and compare its performances against the existing NPV protocols in order to claims its efficiency.

Future exertion will aim at integrating the NPV protocol in higher-layer protocols, useful in presence of applications that need each node to constantly verify the position of its neighbours.

7. REFERENCES

[1] SudarshanVasudevan, Micah Adler, Dennis Goeckel, Fellow, IEEE, and Don Towsley, Fellow, IEEE, ACM ,” Efficient Algorithms for Neighbor Discovery in Wireless Networks”.

[2] Zhensheng Zhang and Bo Li, “Neighbor Discovery in Mobile Ad Hoc Self-Configuring Networks with Directional Antennas: Algorithms and Comparisons”.

[3] SudarsanVasudevan, Jim Kurose, Don Towsley, “On Neighbor Discovery in Wireless Networks with Directional Antennas”, UMass Computer Science Technical Report 04-53 ECC-0313747001.

[4] Marco Fiore, Member, IEEE, Claudio Casetti, Member, IEEE, Carla-FabianaChiasserini, Senior Member, IEEE,PanagiotisPapadimitratos, Member, IEEE , “Discovery and Verification of Neighbor Positions in Mobile Ad Hoc Networks”.

[5] P. P. Papadimitratos, M. Poturalski, P. Schaller, P. Lafourcade, D. Basin, S. Capkun, and J.-P. Hubaux, “Secure Neighborhood Discovery: A Fundamental Element for Mobile Ad Hoc Networking,” *IEEE Communications Magazine*, vol. 46, no. 2, 2008.

[6] Y. Hu, A. Perrig, and D. Johnson, “Packet leashes: a defense against wormhole attacks in wireless networks,” in *International Conference on Computer Communications (Infocom)*, 2003.

[7] S. Capkun, L. Buttyan, and J. Hubaux, “SECTOR: secure tracking of node encounters in multi-hop wireless networks,” in *ACM Workshop on Security of Ad Hoc and Sensor Networks*, 2003.

[8] M. Poturalski, P. Papadimitratos, and J. Hubaux, “Secure neighbor discovery in wireless networks: formal investigation of possibility,” in *ACM Symposium on Information, Computer and Communications Security (ASIACCS)*, 2008.

[9] J.-H. Song, V. Wong, V. Leung, “Secure Location Verification for Vehicular Ad-Hoc Networks,” *IEEE Globecom*, New Orleans, LO, Dec. 2008.

[10] T. Leinm¨uller, C. Maih¨ofer, E. Schoch, F. Kargl, “Improved Security in Geographic Ad Hoc Routing through Autonomous Position Verification,” *ACM VANET*, Los Angeles, CA, Sept. 2006.

[11] In Analysis of Black Hole Attack on MANETs Using Different MANET Routing Protocols, Irshad Ullah, Shoaib Ur Rehman [11], presented hoe the backhole security threat affect on network. So a new scheme is represented which support for both proactive and reactive. So overcome traffic.

[12] In MANET: Vulnerabilities, Challenges, Attacks, Application, Priyanka Goyal, Vinti Parmar, Rahul Rishi[12], discuss how efficiently MANET works but after certain limits there are also created some challenges like limited bandwidth, battery power, computational power, and security. A new method is used to discussed vulnerabilities, application, and security aspects in MANET.