Volume 4, Issue 6, June 2014 ISSN: 2277 128X
International Journal of Advanced Research in Computer Science and Software Engineering
Research Paper
Available online at: www.ijarcsse.com

ENPV: Extended Neighbor Position Verification Approach for MANET

Miss. Anuradha T. Thakre
Department of Computer Engineering
Dr. D. Y. Patil College of Engg. Ambi, Talegaon
University Of Pune, Pune, India

Prof. Sandeep Kadam
Department of Computer Engineering
Dr. D. Y. Patil College of Engg, Ambi, Talegaon
University Of Pune, Pune, India

Abstract— Since the number of protocols and location aware services used in Mobile Ad Hoc Network (MANET) is increases, the mobile nodes in the MANET wants to find out the position of their neighbors for better and well-organized routing communication. But this process in MANET is easily compromised by attacking mobile node and get information about location of mobile nodes in MANET. Thus we need to have efficient neighbor discover method to prevent such kinds of attacks and give the security. Newly many methods presented for the neighbor position verification, however those are suffered from some performance related restrictions. In this paper extended version of NPV protocol is planned with aim of civilizing the false positive and false negative rates under the presence of different attacks. In addition to this extend the working of NPV under the proactive pattern successfully. For improving the performance of NPV, the parameters like threshold value and time out parameters updating to the existing NPV protocol. This new protocol is named as ENPV (Extended NPV) which basically contract with a mobile ad hoc network, where a persistent communications is not found, and the location data must be obtained through node-to-node communication. Such a situation is of interest since it leaves the door open for adversarial nodes to misuse or disrupt the location-based services. Similarly, counterfeit positions might grant adversaries unauthorized access to location-dependent services, let vehicles forfeit road tolls, disrupt vehicular traffic or endanger passengers and drivers.

Keywords— Ad hoc networks, Neighbor position verification, mobile ad hocNetworks, Security, false positive, false negative.

I. Introduction

The most important prerequisite of the ad-hoc networks is that they are "self-configuring" i.e., that a vast number of wireless nodes put in order themselves to perform the task professionally required by the application and after they have been deployed. Once the nodes are deployed, they do not have information about their neighbors thus, they need to discover their neighbors in order to communicate with them. Knowledge of the neighbors is important for almost all routing protocols, medium-access control protocols and several other topology-control algorithms. Neighbor discovery is, thus, a crucial first step in the process of self-organization of a wireless ad-hoc network. The neighbors can be either communication neighbors or physical neighbors or communication neighbors. The physical neighbors are those which are in the range of physical proximity of the discoverer. The communication neighbors are those that are reachable for communication but not necessary to be in the physical range of the discoverer.

Neighbor discovery is the process in which a node which are present in network computes an identity and total no of other nodes in its surrounding area. It is a fundamental building block of many protocols including localization, routing, leader election, and group management. Time-based communications and many media access control mechanisms rely on accurate neighbor information. Neighbor discovery is important to the proper functioning of wireless networks.

Neighbors are usually defined as nodes that lie within radio range of each other in wireless network. Thus, neighbor discovery may be considered as the exploration of the volume of space or "neighborhood" immediately surrounding a wireless node. Nodes found within the neighborhood are neighbors and, depending on network configuration and topology, may cooperate in the performance of various tasks including communications, sensing and localization. However, wireless communications are susceptible to abuse. Attackers have the freedom to do malicious activities ranging from simple denial of service to sophisticated deception. The correctness of node locations is thusan important issue in mobile networks, and it becomes particularly challenging in the presence of adversaries aiming at harming the system. In these cases, we need solutions that let nodes (1) correctly establish their location in spite of attacks feeding not correct location information, and (2) verify the positions of their neighbors, so as to detect adversarial nodes announcing false locations.

In this paper the system discuss about the *neighbor position verification (NPV)* and its related issues. In the literature we have studied the many methods but there are no lightweight, robust solutions to NPV that may operate autonomously in an open, ephemeral environment, without relying on trusted nodes. One recent solution is presented over this issue in [1]. In this paper new protocol NPV is presented which allows any node in a mobile ad hoc network to verify the position

of its communication neighbors without depending on a-priori trustworthy nodes. However this protocol is further suffered from the limitations related to false positive and false negative rates under the presence of different kinds of attacks. Thus our proposed work in this project includes present algorithm enhancements for improved false negative and false positive rates and combination of this work with a localization protocol. In next section II we are presenting the literature survey over the various methods location verification in MANET. In section III, the proposed approach and its system block diagram is depicted. In section IV we are presenting the current state of implementation and results achieved. Finally conclusion and future work is predicted in section V.

II. Literature Survey

The neighbor discovery algorithms can be classified as Deterministic or Random, Directional or Omni – directional Antenna based, Location based approaches, and direct discovery or Gossip based algorithms.

- In Efficient Algorithms for Neighbor Discovery in Wireless Networks, Sudarshan Vasudevan, Micah Adler, Dennis Goeckel, Fellow, IEEE, and Don Towsley, Fellow, IEEE, ACM [1], each node transmits at randomly chosen times and discovers all its neighbors by a given time with high probability, each node transmits according to a predetermined transmission schedule that allows it to detect all its neighbors by a given time with probability one. The antenna models used in ad hoc networks are directional antenna model or Omni directional antenna model.
- In Neighbor Discovery in Mobile Ad Hoc Self-Configuring Networks with Directional Antennas: Algorithms and Comparisons, Zhensheng Zhang and Bo Li [2] propagates signal 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. The sender delivers the DISCOVER message to advertise itself. The receivers will discover one neighbor if it receive the DISCOVER message properly in the listen state,The Omni directional antennas have drawbacks like decreased gain, increased signal distraction, high bandwidth consumption, and increased noise. Directional antenna gives longer transmission range and higher data rate. They strongly reduce jamming susceptibility and signal interferences in unnecessary directions.
- In Neighbor Discovery in Wireless Networks with Directional Antennas, Sudarsan Vasudevan, Jim Kurose, Don Towsley, [3] the nodes discover the neighbors which communicate with it directly. The technique used to discover the neighbors is recording the angle of arrival of the beacon signal, determining the location based using GPS. The direct discovery algorithm will discover those neighbors that communicate with it directly, the neighbors are discovered indirectly through the interaction with other neighbors. Messages are exchanged which helps in discovery of the neighbors. The message contains list of neighbors‟ 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 neighbor.
- In Discovery and Verification of Neighbor Positions in Mobile Ad Hoc Networks, Marco Fiore, Member, IEEE, Claudio Casetti, Member, IEEE, Carla-Fabiana Chiasserini, Senior Member, IEEE,Panagiotis Papadimitratos, Member, IEEE , [4] is used to verify the position of the neighbors that the nodes declare.
- In Panos Papadimitratos and Marcin Poturalski, Secure Neighbor Discovery: A Fundamental Element for Mobile Ad-Hoc Networks [5], this paper provides an overview of the problems and challenges associated with SND and their paper includes a set of real-world examples illustrating various threats to neighbor discovery.
- In Packet leashes: a defense against wormhole attacks in wireless networks, Y. Hu, A. Perrig, and D. Johnson,[6] 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. With the help of both geographic and temporal leashes, Hu, et al. propose mechanisms that incorporate high resolution synchronized clocks to compute the time or distance of flight of a packet. However, the high level of precision needed exceeds the capabilities of most modern hardware at distances less than kilometers.
- In SECTOR: secure tracking of node encounters in multi-hop wireless networks, S. Capkun, L. Buttyan, and J. Hubaux [7] proposed tracking nodes 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.
- In Secure neighbor discovery in wireless networks: formal investigation of possibility, [8], Poturalski, et al. offer 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.
- In Secure Location Verification for Vehicular Ad-Hoc Networks, J.-H. Song, V. Wong, V. Leung [9], presented the method which exploits Time-of-Flight distance boundingand node cooperation to mitigate the problems of theprevious solutions. However, the cooperation is limited to couplesof neighbor nodes, which renders the protocol ineffectiveagainst colluding attackers.
- In Improved Security in Geographic Ad Hoc Routing through Autonomous Position Verification, T. Leinm¨uller, C. Maih¨ofer, E. Schoch, F. Kargl [10], the new scheme is presented for NPV protocol which allowsnodes to validate the position of their neighbors through localobservations only. This is done by checking whethersubsequent positions announced by one neighbor draw amovement over time that is physically possible. The limitation of this method is anadversary can fool the protocol by simply announcing falsepositions that follow a realistic mobility pattern.

III. Proposed Approach Framework and Design

3.1 Problem Definition

Even though the journalism carries a huge number of ad hoc security protocols addressing a number of problems related to NPV, there are no lightweight, robust solutions to NPV that may operate separately in an open, transient environment, without relying on trusted nodes. Most of present solutions are not suitable for both low and high mobile environments. One recent solution is presented over this issue in [1].

In this paper new protocol NPV is offered which allows any node in a mobile ad hoc network to check the position of its communication neighbors without relying on a-priori trustworthy nodes. The practical analysis of this protocol is showing that it outperforms all existing protocols and delivers efficiency. However this protocol is more suffered from the restrictions related to false positive and false negative rates under the presence of different kinds of attacks. This protocol is further needs to expand under the proactive environment. This protocol is currently working only under reactive situation.

Limitations of Existing System

- No support for proactive paradigm.
- Lower false negative and false positive rates.

3.2 Proposed Architecture and Design

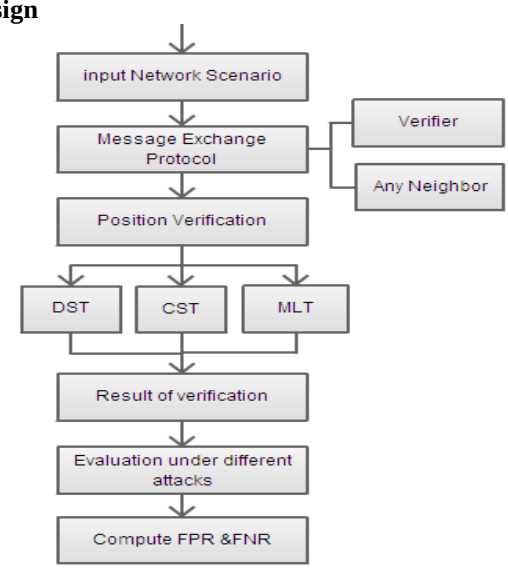


Figure 1: Proposed architecture

as a result in this project , presenting the extensive version of NPV protocol with aim of improving the false positive and false negative rates under the presence of different attacks as well as extend the working of NPV under the proactive pattern effectively. To improve the performances we have included the threshold value and time out parameters updating to the existing NPV protocol.

So a new protocol is developed and named as ENPV (Extended NPV) which fundamentally deal with a mobile ad hoc network, in a which consistent infrastructure is not present, and also the location data must be obtained through node-to-node communication. Such a scenario is of interest since it leaves the door open for adversarial nodes to abuse or disrupt the location-based services. Similarly, counterfeit positions would provide adversaries unauthorized access to location-dependent services, let vehicles forfeit road tolls, disrupt vehicular traffic or endanger passengers and drivers. 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.

Advantages of Proposed System:

- Our ENPV 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 develops low overhead traffic.
- It is robust against independent and colluding adversaries
- It leverages cooperation but allows a node to perform all verification procedures autonomously.
- Algorithms required for implementation are described as follows:

Algorithm 1: Message Exchange Protocol (MEP): verifier

1. If (node S) do

$S \rightarrow *: (POLL, K_S')$

$S:$ store t_S)

If (REPLY received from $X \in N_S$) do

$S:$ store $t_{XS}, t_{X,}$

end if

if($T_{max} + \Delta + T_{jitter}$ do

S: $m_S = \{(t_X, i_{X,}) | \exists t_{XS}\}$

S $\rightarrow *$: (REVEAL, m_S, $E_{K'_S}\left\{h_{K'_S}\right\}$, Sigs, C_S)

2. end if

Algorithm 2: MEPfor Any neighbor

1. For$X \in N_S$ do
2. If (POLL receive by S) do
   X: store t_{XS}
   X: extract T_X uniform r. v. $\in [0, T_{max}]$
3. End for
4. After T_X do
   X: extract nonce ρx
   X: $t_X = E_{K'_S}\{t_{XS}, \rho x\}$
   X $\rightarrow *$: (REPLY, t_X, $h_{K'_S}$)
   X: store t_{XS}
5. If (REPLY received from $Y \in N_S \cap N_X$) do
   X: store t_{YX}, t_Y
   end if
6. If (REVEAL received from S) do
   X: $t_X = \{(t_{YX}, i_Y) | \exists t_{YX}\}$

   X $\rightarrow$ S: (REPORT, $E_{K_S}\{\rho x, t_X, tt_X, px, Sig_X, C_X\}$)
7. End for

Algorithm 3: DST

1. If node S do
   S: $F_s \leftarrow \emptyset$

   For $X \in N_S$ do

   If($|d_{SX} - d_{XS}| > 2\epsilon_r + \epsilon_m$ or

   $|\|ps - px\| - d_{SX}| > 2\epsilon_p + \epsilon_r$ or $d_{SX} > R$) *then*

   S: $F_s \leftarrow \emptyset$

Algortim 4: CST

1. If node S do
   S: $U_s \leftarrow \emptyset, W_s \leftarrow \emptyset$
   For $X \in N_S, X \notin F_S$ do
   S: $l_X = 0, m_X = 0$
   End for
   For $(X, Y) | X, Y \in N_S, X, Y \notin F_S, X \neq Y$ do
   If$\left(\exists\ d_{XY} - d_{YX}\right.$ and ps $\notin$ line(px, py)$\left.\right)$then
   S: $l_X = l_X + 1, l_Y = l_Y + 1$
   If($|d_{XY} - d_{YX}| > 2\epsilon_r + \epsilon_m$ or
   $|\|pX - pY\| - d_{XY}| > 2\epsilon_p + \epsilon_r$ or $d_{XY} > R$) *then*

   S: $m_X = m_X + 1, m_Y = m_Y + 1$

   End if
   End if
   End for
   For $X \in N_S, X \notin F_S$ do
   if $l_X < 2$ *then*
   S: $U_S \leftarrow X$
   End if
   else switch $\frac{m_x}{l_X}$ do
   case 1: $\frac{m_x}{l_X} > \delta$ S: $F_S \leftarrow X$
   case 2: $\frac{m_x}{l_X} = \delta$ S: $U_S \leftarrow X$

   case 3: $\frac{m_x}{l_X} < \delta$ S: $W_S \leftarrow X$

   End else
   End for
2. End if

Algorithm 5: MLT

1. If node S do

S: $V_s \leftarrow \emptyset$

For $X \in W_S$ do

S: $L_X \leftarrow \emptyset$

End for

For $(X, Y)|X, Y \in W_S, X \neq Y$ do

If($\exists\, t_{XY}$ and $\nexists\, t_{YX}$)then

S: $L_X \leftarrow L_X(S, Y)$

End if

End for

For $X \in W_S$ do

$if\ |L_X| < 2\ then$

S:

$$p_X^{ML} = argmin_n \sum_{L_i, L_j \in L_X} \left\| p - L_i \cap L_j \right\|^2$$

$if\ \|p_X - p_X^{ML}\| > 2\epsilon_p$ then

$S: F_S \leftarrow X, W_S = W_S \setminus X$

End if

End if

end for

$$S: V_S = W_S$$

IV. Work Done

4.1 Input:

Input for practical implementation is the Network scenario that consists of mobile nodes.

4.2 Hardware and Software Used

Hardware Configuration

- Processor - Pentium –IV
- Speed - 1.1 Ghz
- RAM - 256 MB(min)
- Hard Disk - 20 GB
- Key Board - Standard Windows Keyboard
- Monitor - SVGA

Software Configuration

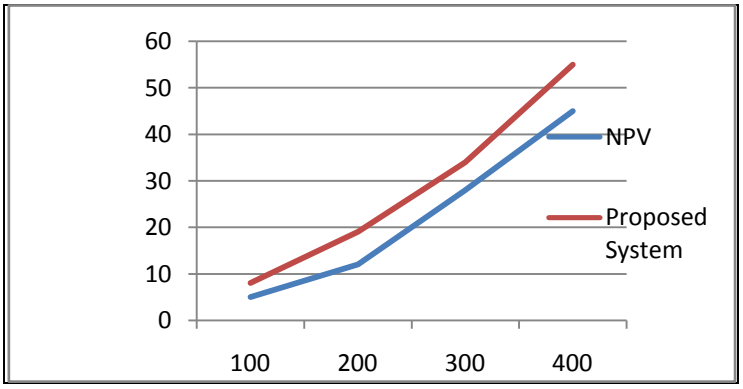
- Operating System - Windows XP/7/8
- Programming Language - Java,J2ME.
- Tool -NetBeans.

4.3 Matrix computation

In this paper we have computedTrue Positive, False positive as well as of the probability that a (similar or different) nodeis tagged as not verifiable[1].

4.4 Results of work done

The results in Figure 2 are analyse 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.



X axis-Transmission range

Y-axis-traffic load per verification

Figure 2: Performance comparison graph.

V. Conclusion and Future Work

This system conferred extended version of NPV protocol with aim of improving the false positive and false negative rates under the presence of different attacks as well as extend the working of NPV under the proactive paradigm successfully. To improve the performances we have 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. Such a scenario is of particular interest since it leaves the door open for adversarial nodes to misuse or disrupt the location-based services. Similarly, counterfeit positions could grant adversaries unauthorized access to location-dependent services, let vehicles forfeit road tolls, disrupt vehicular traffic or endanger passengers and drivers. 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 work will aim at integrating the NPV protocol in higher-layer protocols, as well as at extending it to a proactive paradigm, useful in presence of applications that need each node to constantly verify the position of its neighbours.

VI. Acknowledgement

I would like to thank my Project Guide Prof. Sandeep Kadam, Dr. D. Y. Patil College Of Engineering Ambi, Pune, for generating the idea for this project and for his help, advice and supported to advice proved essential to whatever small success this project may have achieved.

Also, I would like to thank my parents for their continual encouragement and the Positive support. I would also like to thank my wonderful colleagues and friends for listening to my ideas, asking questions and providing feedback and suggestions for improving my ideas.

References

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

[2] Zhen sheng 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.

