ENPV : Extended Neighbour Position Verification Approach for MANET

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

Asst. Prof. Yogesh Sayaji
Dr. D. Y. Patil College of Engineering, Ambi, Talegaon
University Of Pune, Pune, India

Abstract

In today's World a growing number of ad hoc networking protocols and location-aware services require that mobile nodes learn the position of their neighbours. However, such a process can be easily abused or disrupted by adversarial nodes. In absence of a priori trusted nodes, the discovery and verification of neighbour positions presents challenges that have been scarcely investigated in the literature. In this paper, we address this open issue by proposing a fully distributed cooperative solution that is robust against independent and colluding adversaries, and can be impaired only by an overwhelming presence of adversaries. Results show that our protocol can thwart more than 99 percent of the attacks under the best possible conditions for the adversaries, with minimal false positive rates.

Keywords:—Neighbour position verification, mobile ad hoc networks, and vehicular networks.

1. Introduction

1.1 What is ad-hoc network?

The ad-hoc networks is that they are "self-configuring" i.e., that a large number of wireless nodes organize themselves to efficiently perform the tasks required by the application after they have been deployed. After nodes are deployed, they do not have knowledge about the neighbours thus, they need to discover their neighbours in order to communicate with them. Knowledge of the neighbours is essential for almost all routing protocols, medium-access control protocols and several other topology-control algorithms. Neighbours discovery is, therefore, a crucial first step in the process of self-organization of a wireless ad-hoc network. The neighbours can be either physical neighbours or communication neighbour. The physical neighbours are those that are in the range of physical proximity of the discoverer. The communication neighbours are those that are reachable for communication but need not to be in the physical range of the discoverer.Neighbor discovery is the process by which a node in a network determines the total number and identity of other nodes in its vicinity. 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 neighbour information. Neighbour discovery is especially important to the proper functioning of wireless networks. In wireless networks, neighbours are usually defined as nodes that lie within radio range of each other. Thus, neighbour discovery can be considered as the exploration of the volume of space or"neighborhood" immediately surrounding a wireless node. Nodes found within the neighbourhood are neighbours 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 perform malicious activities ranging from simple denial of service to sophisticated deception. The correctness of node locations is therefore an all 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 correctly establish their location in

spite of attacks feeding false location information, and verify the positions of their neighbours, so as to detect adversarial nodes announcing false locations. In this project we are discussing about the neighbour 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 can operate autonomously in an open, ephemeral environment, without relying on trusted nodes. One recent solution is presented over this issue. 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 neighbours without relying 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.

2. Literature Survey

1. The neighbour 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.

2. In randomized neighbour discovery [2], each node transmits at randomly chosen times and discovers all its neighbours by a given time with high probability.

3. In deterministic neighbour discovery [2], on the other hand, each node transmits according to a predetermined transmission schedule that allows it to discover all its neighbours by a given time with probability one. The antenna models used in ad hoc networks are Omni directional antenna model or directional antenna model.

4. The Omni directional antenna model [3] propagates signal in all directions. The algorithm used by Omni directional antenna is 1-way algorithm where the receiver will not send any acknowledgement after receiving the discovery message. The sender broadcasts the DISCOVER message to advertise itself. The receivers will discover one neighbour if it receive the DISCOVER message correctly in the listen state.

5. The Omni directional antennas have drawbacks like reduced gain, increased signal distraction, high bandwidth consumption, and increased noise. Directional antennas provide longer transmission range and higher data rate. They strongly reduce signal interferences in unnecessary directions and reduce jamming susceptibility.

6. In direct discovery algorithm [4] the nodes discover the neighbours which communicate with it directly. The method 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 only those neighbours that communicate with it directly.

7. In gossip based algorithm [4] the neighbours are discovered indirectly through the interaction with other neighbours. Messages are exchanged to discover the neighbours. The message consists of the 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 can cause nodes to incorrectly infer another node as its neighbour.

8. The Direct Symmetry Test and Cross Symmetry Test was proposed in [5] is used to verify the position of the neighbours that the nodes declare.

9. In [6], Papadimitratos, et al. give an overview of the problems and challenges associated with SND. Their paper includes a set of real-world examples illustrating various threats to neighbour discovery.

10. Time-based solutions attempt to leverage time-of-flight measurement to ensure that transmitting nodes lie within the local neighbourhood. Packet leashes are a well-known example of this approach. Using both geographic and temporal leashes, Hu, et al. [7] propose mechanisms that incorporate high resolution synchronized clocks to calculate 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 kilometres.

11. SECTOR [8] 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, all face a common constraint.

12. In [9], Poturalski, et al. offer an impossibility proof showing that time-based protocols cannot guarantee SND unless the environment is free of obstacles and the distance between neighbours is small.

3. Existing system

In literature Survey we have seen a multitude of ad hoc security protocols addressing a number of problems related to NPV, there are no lightweight, robust solutions to NPV that can operate autonomously in an open, ephemeral 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 presented which allows any node in a mobile ad hoc network to verify the position of its communication neighbours 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 further suffered from the limitations related to false positive and false negative rates under the presence of different kinds of attacks. This protocol is further needs to extend under the proactive environment. This protocol is currently working only under reactive environment.

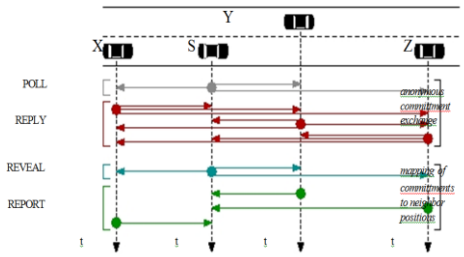

Fig. Existing System Model

4. Limitations of Existing system

1. No support for proactive paradigm.

2. Lower false positive and false negative rates.

5. Proposed Solution

Thus in this project we are presenting the 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 done by using the JAVA technology and compare its performances against the existing NPV protocols in order to claims its efficiency.

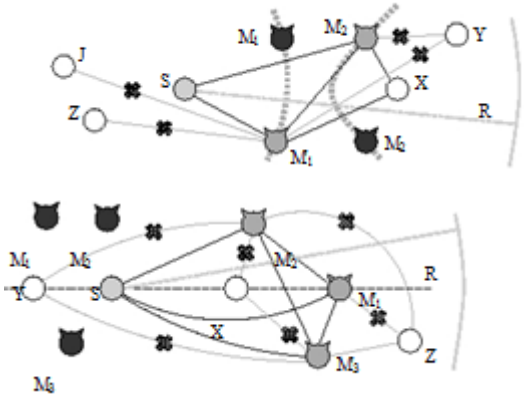

Fig. Proposed System Model

5.1 Advantages of Proposed Systems

- 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 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.

6. System Requirement & Specification

6.1 Software Requirement:

Front End : Java

Tools Used : Eclipse

Processor : Pentium iv 2.6 ghz

6.2 Hardware Requirement:

Ram : 512 mb dd ram

Monitor : 15" color

Hard disk : 20 gb

Floppy drive : 1.44 mb

CD drive : lg 52x

Keyboard : standard 102 keys

Mouse : 3 buttons

Operating System : Windows XP/7

7. Conclusion

Finally In Conclusion we are presenting the 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. It leverages cooperation but allows a node to perform all verification procedures autonomously.

8. References

[1] Marco Fiore, *Member*, *IEEE*, Claudio Casetti, *Member*, *IEEE*, Carla-Fabiana Chiasserini, *Senior Member*, *IEEE*, Panagiotis Papadimitratos, *Member*, IEEE, "Discovery and Verification of Neighbor Positions in Mobile Ad Hoc Networks", IEEE TRANSACTIONS ON MOBILE COMPUTING, VOL. 12, NO. 2, FEBRUARY 2013..

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

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

[4] Sudarsan Vasudevan, Jim Kurose, Don Towsley, "On Neighbor Discovery in Wireless Networks with Directional Antennas", UMass Computer Science Technical Report 04-53 ECC-0313747001.

[5] Marco Fiore, Member, IEEE, Claudio Casetti, Member, IEEE, Carla-Fabiana Chiasserini, Senior Member, IEEE,Panagiotis Papadimitratos, Member, IEEE , "Discovery and Verification of Neighbor Positions in Mobile Ad Hoc Networks".

[6] 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.

[7] 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.

[8] 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.
[9] 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.