ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 2, Issue 10, October 2014

Neighbour Position Discovery and Verification in MANETs

S.Feroz Ahammad[1] and M.Vikram[2] and Kadiyala Ramana[3]

[1]PG Student, Dept. of CSE, SV College of Engineering, Tirupathi, Andhra Pradesh, India

[2]Associate Professor, Dept. of CSE, SV College of Engineering, Tirupathi, Andhra Pradesh, India

[3]Assistant Professor, Dept. of IT, Annamacharya Institute of Technology and Sciences, Rajampet, Andhra Pradesh, India

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

KEYWORDS: Neighbor Position Verification” (NPV), MANET.

I. INTRODUCTION

The emerging wireless ad hoc network paradigm enables a new type of network in which collaborating devices relay packets from one device to another across multiple wireless links in a self-organizing manner. A number of applications based on this type of network have been established or are expected in the near future, such as environmental and building monitoring, disaster relief and military battlefield communication. Due to the self-organizing nature of ad hoc networks, every node in the network can be alternately functioning as a transmitter or a receiver. Oftentimes, a node can communicate directly with only several other nodes around itself, which are called its “neighbors”. In absence of a central controller, every node has to discover its neighbors before efficient routing is possible. The process for a node to identify all its neighbors is called *neighbor discovery*, which is a crucial first step of constructing reliable wireless ad hoc networks.

Neighbor discovery in ad hoc networks is a critical and non-trivial task. Algorithms such as “birthday protocol” [1], directional antenna neighbor discovery [2], [3] and slotted random transmission and reception [4] have been proposed to enable all nodes in a network to find out their neighbors either synchronously or asynchronously. These algorithms can be categorized as random access discovery, which requires nodes to be randomly in a “transmitting” or “listening” state in each time slot so that each node gets a chance to hear every neighbor for at least once in a sufficient amount of time. Such random access discovery schemes allow one transmission to be successful at a time, and hence generally require a large number of time slots until reliable neighbor discovery is achieved.

Timely discovery of a node’s neighbors is a critical issue in wireless networks, especially when the nodes are mobile. References [5]–[7] suggest solution of the neighbor discovery problem from the multiuser detection perspective. The idea is to let all neighbors simultaneously send their unique signature waveforms which identify themselves, and let the center node detect which signatures are at presence. The advantage is rapid detection achieved using multiuser detectors, which are well-understood in the context of code-division multiple access (CDMA). However, the difficulties of scaling the scheme as well as implementing coherent detection without training have not been adequately addressed (training for channel estimation is evidently impossible before the discovery of neighbors).

1.1 Finding the position of a neighbour

Neighbor discovery deals with the identification of nodes with which a communication link can established or that are within a given distance. An adversarial node could be securely discovered as neighbour and be indeed a neighbour (with in some range),but it could still cheat about its position within the same range. In other words, SND lets a node assess whether another node is an actual neighbour but it does not verify the location it claims to be at. This is most often employed to counter wormhole attacks.

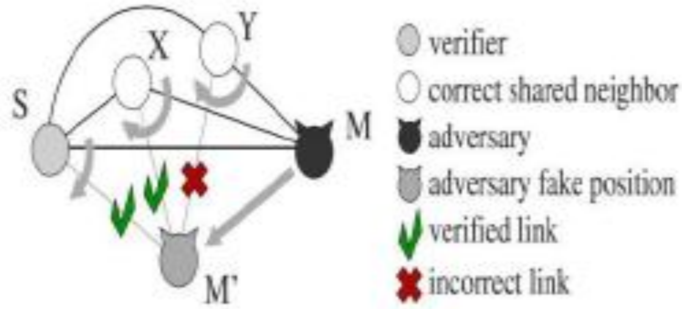

Figure1. Neighbor discovery in adversarial environment

1.2 Confirmation of claimed position.

Neighbor verification schemes often rely on fixed or mobile trustworthy nodes, which are assumed to be always available for the verification of the positions announced by third parties. In ad hoc environments, however the pervasive presence of either infrastructure or neighbor nodes that can be aprioristically trusted is quite unrealistic. Thus, a protocol is devised that is autonomous and does not require trustworthy neighbours.

1.3 Importance Of Neighbor Position Update

An ad hoc network is the collection of wireless mobile hosts forming a temporary without the aid of any established infrastructure or centralized administration. In such an environment , it is necessary for one mobile host to enlist the aid of other hosts in forwarding packet to its destination, due to the limited range of each mobile host's wireless transmissions. In order to procure the position of other nodes while moving, an approach is proposed such a way that it helps in obtaining the position of dynamic mobile node. This paper presents a protocol for updating the position of node in dynamic ad hoc networks. The protocol adapts quickly to position changes when host movement is frequent, yet requires little or no overhead during periods in which hosts move less frequently.

II.RELATED WORK

Location awareness has become an asset in mobile systems, where a wide range of protocols and applications require knowledge of the position of the participating nodes. Geographic routing in spontaneous networks, data gathering in sensor networks, movement coordination among autonomous robotic nodes, location-specific services for handheld devices, and danger warning or traffic monitoring in vehicular networks are all examples of services that build on the availability of neighbour position information.

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. Specifically, we 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. For example, by advertising forged positions, adversaries could bias geographic routing or data gathering processes, attracting network traffic and then eavesdropping or discarding it. 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. In this context, the challenge is to perform, in absence of trusted nodes, a fully distributed, lightweight

NPV procedure that enables each node to acquire the locations advertised by its neighbours, and assess their truthfulness. We therefore propose an NPV protocol that has the following features. It is designed for spontaneous ad hoc environments, and, as such, it does not rely on the presence of a trusted infrastructure or of a priori trustworthy nodes. It leverages cooperation but allows a node to perform all verification procedures autonomously.

Although the literature carries 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. Below, we list relevant works and highlight the novelty of our contribution. For clarity of presentation, we first review solutions to some NPV-related problems, such as secure positioning and secure discovery, and then we discuss solutions specifically addressing NPV. Securely determining own location. In mobile environ-ments, self-localization is mainly achieved through Global Navigation Satellite Systems, e.g., GPS, whose security can be provided by cryptographic and noncryptographic defense mechanisms [3]. Alternatively, terrestrial special-purpose infrastructure could be used [4], [5], along with techniques to deal with nonhonest beacons [6]. We remark that this problem is orthogonal to the problem of NPV. In the rest of this paper, we will assume that devices employ one of the techniques above to securely determine their own position and time reference.

Secure neighbor discovery (SND) deals with the identification of nodes with which a communication link can be established or that are within a given distance [7]. SND is only a step toward the solution we are after: simply put, an adversarial node could be securely discovered as neighbor and be indeed a neighbor (within some SND range), but it could still cheat about its position within the same range. In other words, SND is a subset of the NPV problem, since it lets a node assess whether another node is an actual neighbor but it does not verify the location it claims to be at. SND is most often employed to counter wormhole attacks [8], [9], [10]; practical solutions to the SND problem have been proposed in [11], while properties of SND protocols with proven secure solutions can be found in [12], [13].

Neighbor position verification was studied in the context of ad hoc and sensor networks; however, existing NPV schemes often rely on fixed [14], [15] or mobile [16] trustworthy nodes, which are assumed to be always available for the verification of the positions announced by third parties. In ad hoc environments, however, the pervasive presence of either infrastructure or neighbor nodes that can be aprioristically trusted is quite unrealistic. Thus, we devise a protocol that is autonomous and does not require trustworthy neighbors.

In [17], an NPV protocol is proposed that first lets nodes calculate distances to all neighbors, and then commends that all triplets of nodes encircling a pair of other nodes act as verifiers of the pair's positions. This scheme does not rely on trustworthy nodes, but it is designed for static sensor networks, and requires lengthy multiround computations involving several nodes that seek consensus on a common neighbor verification. Furthermore, the resilience of the protocol in [17] to colluding attackers has not been demonstrated. The scheme in [18] suits static sensor networks too, and it requires several nodes to exchange information on the signal emitted by the node whose location has to be verified. Moreover, it aims at assessing not the position but whether the node is within a given region or not. Our NPV solution, instead, allows any node to validate the position of all of its neighbors through a fast, one-time message exchange, which makes it suitable to both static and mobile environments. Additionally, we show that our NPV scheme is robust against several different colluding attacks. Similar differences can be found between our work and [19].

In [20], the authors propose an NPV protocol that allows nodes to validate the position of their neighbors through local observations only. This is performed by checking whether subsequent positions announced by one neighbor draw a movement over time that is physically possible. The approach in [20] forces a node to collect several data on its neighbor movements before a decision can be taken, making the solution unfit to situations where the location information is to be obtained and verified in a short time span. Moreover, an adversary can fool the protocol by simply announcing false positions that follow a realistic mobility pattern. Conversely, by exploiting cooperation among nodes, our NPV protocol is 1) reactive, as it can be executed at any instant by any node, returning a result in a short time span, and 2) robust to fake, yet realistic, mobility patterns announced by adversarial nodes over time.

The scheme in [21] exploits Time-of-Flight (ToF) distance bounding and node cooperation to mitigate the problems of the previous solutions. However, the cooperation is limited to couples of neighbor nodes, which renders the protocol ineffective against colluding attackers. To our knowledge, our protocol is the first to provide a fully distributed, lightweight solution to the NPV problem that does not require any infrastructure or a priori trusted neighbors and is robust to several different attacks, including coordinated attacks by colluding adversaries. Also, unlike previous works, our solution is suitable for both low and high mobile environments and it only assumes RF communication. Indeed, non-RF communication, e.g., infrared or ultrasound, is unfeasible in mobile networks, where non-line-of-sight conditions are frequent and device to device distances can be in the order of tens or hundreds of meters. An early version of this work, sketching the NPV protocol and some of the verification tests to detect independent adversaries, can be found in [22].

III.PROPOSED WORK

In this paper we propose a fully distributed cooperative scheme for neighbor position verification(NPV), which enables a node, hereinafter called the verifier, to discover and verify the position of its communication neighbors.

A. NPV Protocol

The proposed NPV protocol is designed for spontaneous mobile ad hoc environments, and, as such, it does not rely on the presence of a trusted infrastructure or of a priori trustworthy nodes. This protocol leverages cooperation but allows a node to perform all verification procedures autonomously. This method has no need for lengthy interactions, e.g., to reach a consensus among multiple mobile nodes, making our scheme suitable for both low and high mobility environments. It is reactive, meaning that it can be executed by any mobile node, at any point in time, without prior knowledge of the neighborhood. It is robust against independent and colluding attacks. It is lightweight, as it generates low overhead routing traffic.

Algorithm 1

```
Step 1: node S do
Step 2: S ->* : (POLL, K’s)
Step 3: S: store ts
Step 4: When receive REPLY from X E
Step 5: S : store txs, cx
Step 6: after Tmax + Tjitter do
Step 7: S : ms={(cx, ix)/txs)}
```

B. Direct Symmetry Test

The Direct Symmetry Test (DST) verifies the direct links with its communication neighbor nodes. To this end, DST checks whether reciprocal to F-derived distances are consistent with each other and with the position advertised by the neighbor node and with a proximity range. The latter corresponds to the maximum nominal transmission range, and upper bounds the distance at which the two nodes can communicate.

Algorithm 2

```
Step 1: node S do
Step 2: S: Fs<-0
Step 3: For all X E Ns do
Step 4: If dsx – dxs > 2 or
Step 5: ps – px / - dxs > 2 or
Step 6: dsx > R then
Step 7: S:Fs<-X
```

C. Cross Symmetry Test

The cross symmetry test(CST) ignores nodes already declared as faulty by the DST and only considers mobile nodes that proved to be communication neighbor nodes between each other, i.e., for which To F derived mutual distances are available. However, pairs of neighbor nodes declaring collinear positions with respect to S are not taken into account. This choice makes our NPV robust to attacks in many particular situations. For all other pair the cross test verifies the symmetry of the reciprocal distances and their consistency with the positions declared by the neighbor nodes and with the proximity range. For each neighbor maintains a link counter and a mismatch counter. The former is incremented at every new crosscheck on X, and records the number of communication links between neighbor and other neighbors. The latter is incremented every time at least one of the cross checks on distance and the position fails and identifies the potential for neighbor being faulty.

Algorithm 3

```
Step 1: node S do
Step 2: S:Us<- 0, Ws<- 0
Step 3: For all X E Ns, X E Fs do
Step 4: if dxy , dyx and
Step 5: Ps E line(px , py)
```

Step 6: S:lx=lx+1, ly=ly+1
Step 7: If dxy-dyx > 2x+e or
Step 8: dxy > R then
Step 9: S: mx=mx+1.

IV. ROBUSTNESS ANALYSIS OF THE PROPOSED SYSTEM

A single independent adversary cannot perform any successful attack against the NPV scheme. When the shared neighbourhood increases in size, the probability that the adversary is tagged as faulty rapidly grows to 1. Multiple independent adversaries can only harm each other, thus reducing their probability of successfully announcing a fake position. In coordinated attacks, it is the nature of the neighbourhood that determines the performance of the NPV scheme in presence of colluders. However, in realistic environments, our solution is very robust even to attacks launched by large groups of knowledgeable colluders. This system yields small advantage to the adversaries in terms of displacement. Finally, the overhead introduced by the NPV protocol is reasonable, as it does not exceed a few tens of Kbytes even in the most critical conditions.

V. CONCLUSION

Techniques for finding neighbours effectively in a non priori trusted environment are identified. The proposed techniques will eventually provide 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.

REFERENCES

[1]. 1609.2-2006: IEEE Trial-Use Standard for Wireless Access in Vehicular Environments - Security Services for Applications and Management Messages, IEEE, 2006.

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

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

[4]. L. Lazos and R. Poovendran, "HiRLoc: High-Resolution Robust Localization for Wireless Sensor Networks," IEEE J. Selected Areas in Comm., vol. 24, no. 2, pp. 233-246, Feb. 2006.

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

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

[7]. Y.-C. Hu, A. Perrig, and D.B. Johnson, "Packet Leashes: A Defense against Wormhole Attacks in Wireless Networks," Proc. IEEE INFOCOM, Apr. 2003.

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

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

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

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

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

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

[14]. J. Chiang, J. Haas, and Y. Hu, "Secure and Precise Location Verification Using Distance Bounding and Simultaneous Multilateration," Proc. Second ACM Conf. Wireless Network Security (WiSec), Mar. 2009.

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

[16]. S. Capkun and J.-P. Hubaux, "Secure Positioning in Wireless Networks," IEEE J. Selected Areas in Comm., vol. 24, no. 2, pp. 221- 232, Feb. 2006.

[17]. A. Vora and M. Nesterenko, "Secure Location Verification Using Radio Broadcast," IEEE Trans. Dependable and Secure Computing, vol. 3, no. 4, pp. 377-385, Oct.-Dec. 2006.

[18]. J. Hwang, T. He, and Y. Kim, "Detecting Phantom Nodes in Wireless Sensor Networks," Proc. IEEE INFOCOM, May 2007.

[19]. T. Leinmu¨ller, C. Maiho¨fer, E. Schoch, and F. Kargl, "Improved Security in Geographic Ad Hoc Routing through Autonomous Position Verification," Proc. ACM Third Int'l Workshop Vehicular Ad Hoc Networks (VANET), Sept. 2006.

[20]. J.-H. Song, V. Wong, and V. Leung, "Secure Location Verification for Vehicular Ad-Hoc Networks," Proc. IEEE Globecom, Dec. 2008.

[21]. M. Fiore, C. Casetti, C.-F. Chiasserini, and P. Papadimitratos, "Secure Neighbor Position Discovery in Vehicular Networks," Proc. IEEE/IFIP 10th Ann. Mediterranean Ad Hoc Networking Workshop (Med-Hoc-Net), June 2011.

[22]. Fed. Highway Administration, "High Accuracy-Nationwide Differential Global Positioning System Test and Analysis: Phase IIReport," FHWA-HRT-05-034, July 2005.

[23]. http://www.nanotron.com/EN/pdf/Factsheet_nanoLOC-NA5TR1.pdf, 2012.

[24]. PRECIOSA: Privacy Enabled Capability in Co-Operative Systems and Safety Applications, http://www.preciosa-project.org, 2012.

[25]. G. Calandriello, P. Papadimitratos, A. Lioy, and J.-P. Hubaux, "On the Performance of Secure Vehicular Communication Systems," IEEE Trans. Dependable and Secure Computing, vol. 8, no. 6, pp. 898-912, Nov./Dec. 2011.

[26]. IEEE Standard Specifications for Public-Key Cryptography - Amend-ment 1: Additional Techniques, IEEE 1363a 2004, 2004.

[27]. M. Ciurana, F. Barcelo-Arroyo, and F. Izquierdo, "A Ranging System with IEEE 802.11 Data Frames," Proc. IEEE Radio and Wireless Symp., Jan. 2007.

[28]. F. Carpenter, S. Srikanteswara, and A. Brown, "Software Defined Radio Test Bed for Integrated Communications and Navigation Applications," Proc. Software Defined Radio Technical Conf., Nov. 2004.

[29]. E. Del Re, L.S. Ronga, L. Vettori, L. Lo Presti, E. Falletti, and M. Pini, "Software Defined Radio Terminal for Assisted Localization in Emergency Situations," Proc. First Int'l Conf. Wireless Comm., Vehicular Technology, Information Theory and Aerospace Electronic Systems Technology (CTIF Wireless Vitae), May 2009.

[30]. J. Ha¨rri, M. Fiore, F. Filali, and C. Bonnet, "Vehicular Mobility Simulation with VanetMobiSim," Trans. Soc. Modeling & Simulation, 2009.