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, Special Issue 1, March 2014

Proceedings of International Conference On Global Innovations In Computing Technology (ICGICT'14)

Organized by

Department of CSE, JayShriram Group of Institutions, Tirupur, Tamilnadu, India on 6th & 7th March 2014

Neighbor Position Verification in Mobile Ad Hoc Network

C. LOURDU RAJA

II M.E.,Dept of CSE Arasu Engineering College, Kumbakonam, Tamilnadu, India

Abstract—In a mobile ad hoc network without knowing neighbor node position which make a chance to attackers to easily enter into the network. A growing number of ad hoc networking protocols and location-aware services require that mobile nodes learn the position of their neighbors. 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 neighbor 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. Neighbor position verification to avoid attackers in a network .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: Neighbor position verification, mobile ad hoc networks, vehicular networks

1 INTRODUCTION

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 neighbor 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. In these cases, we need solutions that let nodes 1) correctly establish their location in spite of attacks feeding false location information, and 2) verify the positions of their neighbors, so as to detect adversarial nodes announcing false locations.

Mobile computing is human–computer interaction by which a computer is expected to be transported during normal usage. Mobile computing involves mobile communication, mobile hardware, and mobile software. Communication issues include ad hoc and infrastructure networks as well as communication properties, protocols, data formats and concrete technologies. Hardware includes mobile devices or device components. Mobile software deals with the characteristics and requirements of mobile applications.

Mobile Computing is "taking a computer and all necessary files and software out into the field", "Mobile computing: being able to use a computing device even when being mobile and therefore changing location. Portability is one aspect of mobile computing". Many types of mobile computers have been introduced since 1990. Below are some mobile computing devices.

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, Special Issue 1, March 2014

Proceedings of International Conference On Global Innovations In Computing Technology (ICGICT'14)

Organized by

Department of CSE, JayShriram Group of Institutions, Tirupur, Tamilnadu, India on 6th & 7th March 2014

- Personal digital assistant/enterprise digital assistant
- Smartphone
- Tablet computer
- Ultra-Mobile PC
- Wearable computer

A mobile ad hoc network (MANET) is a self-configuring infrastructure less network of mobile devices connected by wireless. Ad hoc is Latin and means "for this purpose". Each device in a MANET is free to move independently in any direction, and will therefore change its links to other devices frequently. Each must forward traffic unrelated to its own use, and therefore be a router. The primary challenge in building a MANET is equipping each device to continuously maintain the information required to properly route traffic. Such networks may operate by themselves or may be connected to the larger Internet. MANETs are a kind of Wireless ad hoc network that usually has a routable networking environment on top of a Link Layer ad hoc network.

Types of Mobile ad hoc network

- Vehicular Ad hoc Networks (VANETs) are used for communication among vehicles and between vehicles and roadside equipment
- Internet based mobile ad hoc networks (iMANETs) are ad hoc networks that link mobile nodes and fixed Internet-gateway nodes. In such type of networks normal ad hoc routing algorithms don't apply directly.
- Intelligent vehicular ad hoc networks (InVANETs) are a kind of artificial intelligence that helps vehicles to behave in intelligent manners during vehicle-to-vehicle collisions, accidents, drunken driving etc.

In this paper, we focus on the latter aspect, hereinafter referred to as neighbor position verification (NPV for short). 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 posi-tions 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 proce-dure that enables each node to acquire the locations advertised by its neighbors, 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. This approach has no need for lengthy interactions, e.g., to reach a consensus among multiple nodes, making our scheme suitable for both low- and high-mobility environments;
. It is reactive, meaning that it can be executed by any node, at any point in time, without prior knowledge of the neighborhood;
. It is robust against independent and colluding adversaries;

It is lightweight, as it generates low overhead traffic. Additionally, our NPV scheme is compatible with state-of-the-art security architectures, including the ones that have been proposed for vehicular networks [1], [2],

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, Special Issue 1, March 2014

Proceedings of International Conference On Global Innovations In Computing Technology (ICGICT'14)

Organized by

Department of CSE, JayShriram Group of Institutions, Tirupur, Tamilnadu, India on 6th & 7th March 2014

which represent a likely deployment environment for NPV.

The rest of the paper is organized as follows: In Section 2, we review previous works, highlighting the novelty of our solution. In Section 3, we describe the system model, while the communication protocol, the objectives of the verification procedure and our main results are outlined in Section 4. The details of the NPV protocol and of verification tests are then presented in section 5, and the resilience of our solution to different attacks is analyzed in Section 6. Finally, we provide a performance evaluation of the protocol in a vehicular scenario in Section 7, and draw conclusions in Section 8.

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

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, Special Issue 1, March 2014

Proceedings of International Conference On Global Innovations In Computing Technology (ICGICT'14)

Organized by

Department of CSE, JayShriram Group of Institutions, Tirupur, Tamilnadu, India on 6th & 7th March 2014

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-todevice 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].

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, Special Issue 1, March 2014

Proceedings of International Conference On Global Innovations In Computing Technology (ICGICT'14)

Organized by

Department of CSE, JayShriram Group of Institutions, Tirupur, Tamilnadu, India on 6th & 7th March 2014

III . SYSTEM MODEL

We consider a mobile network and define as communication neighbors of a node all the other nodes that it can reach directly with its transmissions [7]. We assume that each node knows its own position and its neighbor node position.

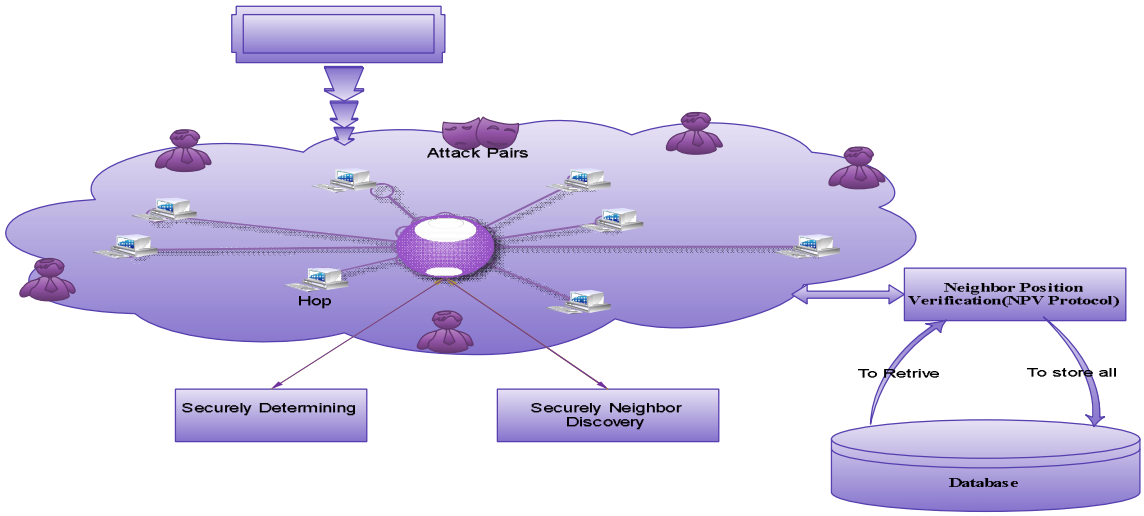

Fig1. System architecture

In this above picture explain the architecture using npv in each and every node. Its store and check their neighbor position at each time. In this check used to reduce time complexity and attacks free MANET.

Fig. 2. File transmission in mobile ad hoc network

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, Special Issue 1, March 2014

Proceedings of International Conference On Global Innovations In Computing Technology (ICGICT'14)

Organized by

Department of CSE, JayShriram Group of Institutions, Tirupur, Tamilnadu, India on 6th & 7th March 2014

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, includ-ing coordinated attacks by colluding adversaries. Also, unlike previous works, our solution is suitable for both low and high mobile environments.

File transmission in mobile ad hoc network is through node to node communication. In here using the NPV its allowed to free the attackers in this mobile ad hoc network.

Once NPV has derived, it runs several position verification tests in order to classify each candidate neighbor as either:

1. Verified, i.e., a node the verifier deems to be at the claimed position;
2. Faulty, i.e., a node the verifier deems to have announced an incorrect position;
3. Unverifiable, i.e., a node the verifier cannot prove to be either correct or faulty, due to insufficient information.

Clearly, the verification tests aim at avoiding false negatives (i.e., adversaries announcing fake positions that are deemed verified) and false positives (i.e., correct nodes whose
positions are deemed faulty), as well as at minimizing the number of unverifiable nodes. We remark that our NPV scheme does not target the creation of a consistent "map" of neighborhood relations throughout an ephemeral network: rather, it allows the verifier to independently classify its neighbors.

IV . NPV: AN OVERVIEW

We propose a fully distributed cooperative scheme for NPV, which enables each node, to discover and verify the position of its communication neighbors. For clarity, here we summarize the steps of npv algorithm,

In this algorithm used to check with their neighbour position and secure transmission of content to the proper destination.

The below steps are used to explain the NPV algorithm.

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

Neighbour position verification in each node:

In a mobile ad hoc network without knowing neighbour node position which makes a chance to attackers to easily enter into the network. If neighbour position verification done in separate node, then it would be a time consuming process. In previous works neighbour node check done through separate nodes. In this way of approach made a less performed application.

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

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, Special Issue 1, March 2014

Proceedings of International Conference On Global Innovations In Computing Technology (ICGICT'14)

Organized by

Department of CSE, JayShriram Group of Institutions, Tirupur, Tamilnadu, India on 6th & 7th March 2014

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 environments,

self-localization is mainly achieved through Global Navigation Satellite Systems, e.g., GPS, whose security can be provided by cryptographic and noncryptographic defense mechanisms. 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. Neighbor position verification is done through NPV algorithm.

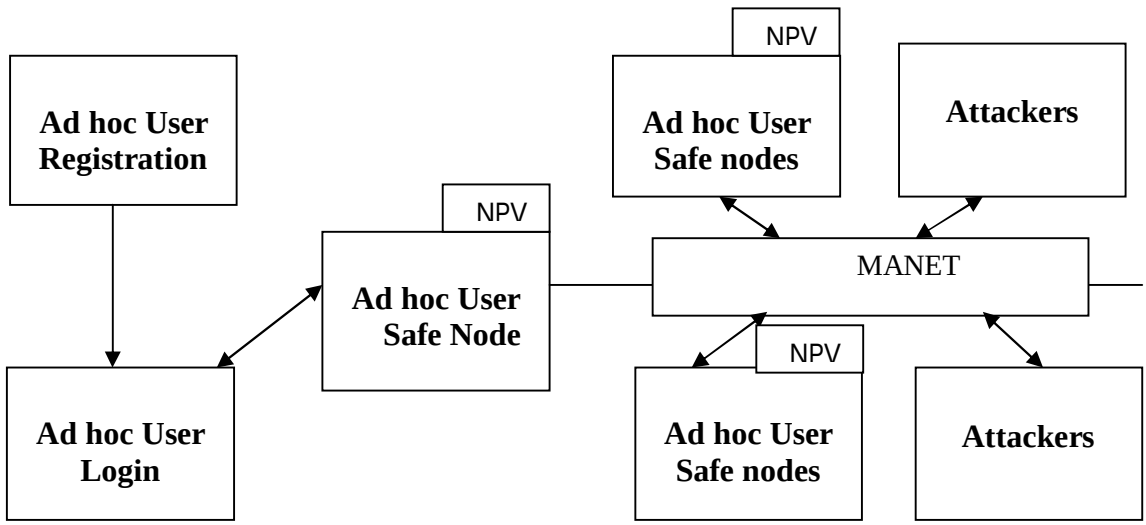

Fig. 3. NPV in manet

V . NPV in MANET

5.1 User registration and login for ad hoc usage

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

5.2 Discover own location and neighbour location

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

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, Special Issue 1, March 2014

Proceedings of International Conference On Global Innovations In Computing Technology (ICGICT'14)

Organized by

Department of CSE, JayShriram Group of Institutions, Tirupur, Tamilnadu, India on 6th & 7th March 2014

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

5.4 Secure content transaction

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

secure neighbour are happened to be here. Use send option after attachments and secure neighbour node selected.

VI . RESILIENCE ANALYSIS

We analyze the robustness of our scheme against different types of internal adversaries. We classify the conceivable attacks into two classes, depending on the goal of the

adversaries ToF-based ranging, we analyze the entire space of attacks against NPV. The effects of combinations of attacks of the first type is then investigated in our performance evaluation.

. Attacks where the adversaries aim at letting the verifier validate their own fake position;

. Attacks where the adversaries aim at disrupting the verification of correct node positions.

Attacks

6.1 Jamming

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

protocol run by the same verifier.

6.2 Clogging

An adversary could initiate the NPV protocol multiple times in a short period and get repeated REPLY and REPORT messages from other nodes, so as to congest the channel. In particular, REPORTs are larger in size, thus likely cause the most damage. However, NPV has a way of preventing that:

the initiator must unveil its identity before such messages are transmitted by neighbors. An exceedingly frequent initiator can be identified, and its REVEALs ignored, thanks to the use of certified keys. REPLYs instead are small in size and are broadcast messages (thus require no ACK): their damage is limited, but their unnecessary transmission is much harder to thwart. Indeed, REPLY messages are sent after an anonymous POLL; such an anonymity is a hard-to dismiss requirement, since it is instrumental for keeping the identity of the verifier hidden. As a general rule, correct nodes can reasonably self-limit their responses if POLLs arrive at excessive rates.

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, Special Issue 1, March 2014

Proceedings of International Conference On Global Innovations In Computing Technology (ICGICT'14)

Organized by

Department of CSE, JayShriram Group of Institutions, Tirupur, Tamilnadu, India on 6th & 7th March 2014

6.3 Sybil and Relay (Wormhole) Attacks
An adversary can assume several trusted identities, M ¼ fM1; . . .;MIg, if 1) it owns several certificated pairs of public/private keys (Sybil attack), or 2) it impersonates colluding adversaries at the end of wormholes. The availability of several identities could be used by an adversary to acquire its neighbor positions, i.e., to become knowledgeable. However, as shown in Section 6.1, attacks launched by independent, knowledgeable adversaries have no chance of success. Furthermore, by announcing timings
that are consistent among the identities inM, the adversary can behave as a group of colluders of size I.

VII . PERFORMANCE EVALUATION

We evaluated the performance of our NPV protocol in a vehicular scenario. Results obtained in a pedestrian scenario are available as supplemental material, which can be found on the Computer Society Digital Library at http:// doi.ieeecomputersociety.org/10.1109/TMC. 2011.258. We focus on knowledgeable adversaries whose goal is to make the verifier believe their fake positions, and we describe the best attack strategy they can adopt in Section 7.1. Such a strategy, which depends on the neighborhood of the adversary and builds on a combination of the attacks described in Sections 6.1 and 6.2, will be assumed while deriving the results shown in Section 7.2. The results, which therefore represent a worst case analysis of the proposed NPV, are shown in terms of the probability that the tests return false positives and false negatives as well as of the probability that a (correct or adversary) node is tagged as unverifiable. In addition, we plot the average difference between the true position of a successful adversary and the fake position it advertises, as well as the overhead introduced by our NPV scheme. The results on attacks aimed at discrediting the position of other nodes are omitted, since they are very close to those we
present later in this section. 7.1 Adversaries Attack Strategy The adversary decision on the kind of attack to launch is driven by the tradeoff between the chances of success and the freedom of choice on its fake position. The basic attack allows the adversary to choose any false position, but it requires a high percentage of colluders in the neighborhood in order to be successful. The hyperbola-based attack implies less freedom of choice but has higher chances of success. The collinear attack pins the adversary into a precise angle with the verifier, and strictly bounds its distance from the verifier itself. However, if the network topology features a sufficient number of collinear nodes, this attack has the highest success probability.

It follows from Section 6 that the best strategy that an
adversary can adopt depends on its neighborhood. First, if it colludes with other adversaries outnumbering the noncolluding neighbors, a basic attack is launched. Otherwise, if the ratio between colluding and noncolluding neighbors is not greater than (but close enough to) 1, a hyperbola-based attack is attempted. As a third option, if noncolluding neighbors greatly outnumber the colluding ones, but some of the former are collinear with the verifier and among themselves, the adversary launches a collinear
attack. Through it, the adversary can have the noncolluding, collinear neighbors thrown out of the cross-checks in the CST. If none of the above conditions are met, the adversary picks a hyperbola-based attack, i.e., the one with the highest chances of success in absence of noncolluding, collinear neighbors.

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, Special Issue 1, March 2014

Proceedings of International Conference On Global Innovations In Computing Technology (ICGICT'14)

Organized by

Department of CSE, JayShriram Group of Institutions, Tirupur, Tamilnadu, India on 6th & 7th March 2014

VIII.CONCLUSION

In this paper presented a distributed solution for NPV, 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. Our analysis showed that our protocol is very robust to attacks by independent as well as colluding adversaries, even when they have perfect knowledge of the neighbourhood of the verifier.Future work will aim at integrating the NPV protocol in higher layer protocols and that each node to constantly verify the position of its neighbour.

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.
[8] Y.-C. Hu, A. Perrig, and D.B. Johnson, "Packet Leashes: A Defense against Wormhole Attacks in Wireless Networks," Proc. IEEE INFOCOM, Apr. 2003.
[9] 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.
[10] R. Maheshwari, J. Gao, and S. Das, "Detecting Wormhole Attacks in Wireless Networks Using Connectivity Information," Proc. IEEE INFOCOM, Apr. 2007.
[11] 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.
[12] 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.
[13] 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.
[14] 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.
[15] J. Chiang, J. Haas, and Y. Hu, "Secure and Precise Location Verification Using Distance Bounding and Simultaneous Multi-lateration," Proc. Second ACM Conf. Wireless Network Security (WiSec), Mar. 2009.
[16] 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.
[17] 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.
[18] 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.
[19] J. Hwang, T. He, and Y. Kim, "Detecting Phantom Nodes in Wireless Sensor Networks," Proc. IEEE INFOCOM, May 2007.
[20] 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.
[21] J.-H. Song, V. Wong, and V. Leung, "Secure Location Verification for Vehicular Ad-Hoc Networks," Proc. IEEE Globecom, Dec. 2008.
[22] 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.
[23] Fed. Highway Administration, "High Accuracy-Nationwide Differential Global Positioning System Test and Analysis: Phase II

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, Special Issue 1, March 2014

Proceedings of International Conference On Global Innovations In Computing Technology (ICGICT'14)

Organized by

Department of CSE, JayShriram Group of Institutions, Tirupur, Tamilnadu, India on 6th & 7th March 2014

Report," FHWA-HRT-05-034, July 2005.
[24] http://www.nanotron.com/EN/pdf/Factsheet_nanoLOC-NA5TR1.pdf, 2012.
[25] PRECIOSA: Privacy Enabled Capability in Co-Operative Systems and Safety Applications, http://www.preciosa-project.org, 2012.
[26] 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.
[27] IEEE Standard Specifications for Public-Key Cryptography - Amend-ment 1: Additional Techniques, IEEE 1363a 2004, 2004.
[28] 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.
[29] 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.
[30] 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.
[31] J. Ha¨rri, M. Fiore, F. Filali, and C. Bonnet, "Vehicular Mobility Simulation with VanetMobiSim," Trans. Soc. Modeling & Simula-tion, 2009.