ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Monthly Peer Reviewed Open Access International e-Journal

Neighbor Position Verification protocol with spontaneous in Mobile Ad Hoc Networks

Suresh Patra
M.Tech Student,
Department of CSE,
Srinivasa Institute of Engineering and Technology.

S.N.V.S.S.S.T. Murty, M.Tech
Associative Professor,
Department of CSE,
Srinivasa Institute of Engineering and Technology.

Abstract:

Location awareness is an important asset in mobile systems and many protocols require knowledge of position of the participating nodes. A secure protocol for spontaneous wireless ad hoc networks is used by the hybrid symmetric and asymmetric schemes. It gives the trust between end users for exchanging the initial data. The data can be encrypted by using a secret key which hides the data. First visual contact between users is the main basis for trust. Using the complete self-configured secure protocol, it is being able to create the network and it also shares the secure services without any infrastructure. The network allows resource sharing and offers new services among users in a secure environment. Providing this protocol to a wireless ad hoc network makes it to be more secure. Our proposal is that, by integrating the Neighbor Position Verification protocol with spontaneous ad hoc network protocol, each node in the network can constantly verify the position of its neighbors as well as security analysis of the system.

Index Terms: Neighbor position verification, mobile ad hoc networks, vehicular networks.

Introduction:

MANET is an autonomous collection of mobile users that communicated over relatively bandwidth constrained wireless links, and the MANETs is to solve challenging real world problems. Since the nodes are mobile so it is dynamic in nature. The network topology may change rapidly and unpredictably over time. It is a unstructured network. It doesn't work constantly under any topology. The network is decentralized where all network activity including discovering and topology and delivering message must be executed by the nodes themselves.

Neighbor discovery (ND) provides an essential functionality for wireless devices that is to discover other devices that they can communicate directly through the wireless networking. Routing begin the most essential in the context of wireless communication makes it easy to abuse ND. The verification of node locations is an important issues in mobile networks, and it becomes particularly challenging in the presence of adversaries aiming at harming the system. 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. 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.

ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Monthly Peer Reviewed Open Access International e-Journal

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 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], 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.

Related work:

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 environments, self-localization is mainly achieved through Global Navigation Satellite Systems, e.g., GPS, whose security can be provided by cryptographic and non cryptographic defense mechanisms [3].

Alternatively, terrestrial special purpose infrastructure could be used [4], [5], along with techniques to deal with non honest 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.

ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Monthly Peer Reviewed Open Access International e-Journal

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 multi round 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].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.

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. 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. RF signal doesn't support for to discover the neighbor position.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.

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.

ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Monthly Peer Reviewed Open Access International e-Journal

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. 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. 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.

NPV protocol that has the following features:

1.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;

2.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;

3.It is reactive, meaning that it can be executed by any node, at any point in time, without prior knowledge of the neighborhood;

4.It is robust against independent and colluding adversaries;

5.It is lightweight, as it generates low overhead traffic.

We propose a fully distributed cooperative scheme for NPV, which enables a node, hereinafter called the verifier, to discover and verify the position of its communication neighbors. For clarity, here we summarize the principles of the protocol as well as the gist of its resilience analysis. Detailed discussions of message format, verification tests,and protocol resilience are provided in Sections 5 and 6. A verifier, S, can initiate the protocol at any time instant,by triggering the 4-step message exchange depicted in Fig. 1, within its 1-hop neighborhood.

The aim of the message exchange is to let S collect information it can use to compute distances between any pair of its communication neighbors. To that end, POLL and REPLY messages are first broadcasted by S and its neighbors, respectively.

These messages are anonymous and take advantage of the broadcast nature of the wireless medium, allowing nodes to record reciprocal timing information without disclosing their identities. Then, after a REVEAL broadcast by the verifier, nodes disclose to S, through secure and authenticated REPORT messages, their identities as well as the anonymous timing information they collected.

The verifier S uses such data to match timings and identities; then, it uses the timings to perform ToF-based ranging and compute distances between all pairs of communicating nodes in its neighborhood. Once S has derived such distances, 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.

ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Monthly Peer Reviewed Open Access International e-Journal

relations throughout an ephemeral network:rather, it allows the verifier to independently classify its neighbors. The basic principle the verification tests build upon is best explained. There, M is a malicious node announcing a false location Mo, so as to fraudulently gain some advantage over other nodes. The figure portrays the actual network topology with black edges, while the modified topology, induced by the fake position announced by M, is shown with gray edges.

It is evident that the displacement of M to Mo causes its edges with the other nodes to rotate, which, in turn, forces edge lengths to change as well. The tests thus look for discrepancies in the node distance information to identify incorrect node positions. A malicious node, knowing the protocol, can try to outsmart the tests in a number of different ways. Section 6 contains a comprehensive discussion of the protocol resilience, covering conceivable attack strategies that adversarial nodes could adopt. Overall, our analysis proves that:

An unknowledgeable adversary has no possibility of success against our NPV protocol;An independent knowledgeable adversary M can move at most two links (with the verifier S and with a shared neighbor X) without being detected: however, any additional link (e.g., with another shared neighbor Y) leads to inconsistencies between distances and positions that allow to identify the attacker: this is the situation depicted .

In a nutshell, independent adversaries, although knowledgeable, cannot harm the system; Colluding knowledgeable adversaries can announce timing information that reciprocally validate their distances, and pose a more dangerous threat to the system. However, we prove that an overwhelming presence of colluders in the verifier neighborhood is required for an attack to be successful. Additionally, simulations in realistic scenarios prove the robustness of the NPV protocol even against large groups of colluding knowledgeable adversaries.

POLL message Sending:

The verifier starts the protocol by broadcasting a POLL whose transmission time is stores locally. The POLL is anonymous, since 1) it does not carry the identity of the verifier, 2) it is transmitted employing a fresh, software-generated MAC address, and 3) it contains a public key KoS taken from S's pool of anonymous one-time use keys that do not allow neighbors to map the key onto a specific node. We stress that keeping the identity of the verifier hidden is important in order to make our NPV robust to attacks. Since a source address has to be included in the MAC-layer header of the message, a fresh, software-generated MAC address is needed.

Position Verification:

Once the message exchange is concluded, verifier can decrypt the received data and acquire the position of all neighbors that participated in the protocol. The verifier also knows the transmission time of its POLL and learns that of all subsequent REPLY messages, as well as the corresponding reception times recorded by the recipients of such broadcasts. Applying a ToF-based technique, verifier thus computes its distance from each communication neighbor, as well as the distances between all neighbor pairs sharing a link.The Direct Symmetry Test (DST):-In the DST, verifier verifies the direct links with its communication neighbors. To this end, it checks whether reciprocal ToF-derived distances are consistent 1) with each other, 2) with the position advertised by the neighbor, and 3) with a proximity range. The latter corresponds to the maximum nominal transmission range, and upper bounds the distance at which two nodes can communicate.

The Cross-Symmetry Test (CST):

The CST ignores nodes already declared as faulty by the DST and only considers nodes that proved to be communication neighbors between each other, i.e., for which ToF-derived mutual distances are available. The CST verifies the symmetry of the reciprocal distances, their consistency with the positions declared by the nodes, and with the proximity range. For each neighbor, verifier maintains a link counter and a mismatch counts. The former is incremented at every new cross-check on neighbor, and records the number of links between neighbors and other neighbors of verifier.

The Multi Lateration Test (MLT):

In MLT, it ignores nodes already tagged as faulty or unverifiable and looks for suspect neighbors in WWS.

ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Monthly Peer Reviewed Open Access International e-Journal

For each neighbor that did not notify about a link reported by another node a curve is computed and added to the set ILX .Such a curve is the locus of points that can generate a transmission whose Time Difference of Arrival (TDoA) at verifier and neighbor matches that measured by the two nodes.

Protocol Message Exchange:

The value pX is the current position of X, and INX is the current set of its communication neighbors. We denote by tX the time at which a node X starts a broadcast transmission and by tXY the time at which a node Y starts receiving it. Note that these time values refer to the actual instant at which the node starts transmitting/receiving the

ALGORITHMS USED:

Message exchange protocol: verifier.
Message exchange protocol: any neighbor.

Algorithm 1. Message exchange protocol: verifier.

1 node S do
2 $S \to *$: {POLL, K'_S}
3 S : store t_S
4 when receive REPLY from $X \in N_S$ do
5 S : store t_{XS}, c_X
6 after $T_{max} + \Delta + T_{jitter}$ do
7 S : $n_S = \{(c_X, i_X) \mid \exists t_{XS}\}$
8 $S \to *$: {REVEAL, $n_S, E_{K'_S}\{k_{K'_S}\}$, Sig_S, C_S}

Algorithm 2. Message exchange protocol: any neighbor.

1 forall $X \in N_S$ do
2 when receive POLL by S do
3 X : store t_{SX}
4 X : extract T_X uniform r.v. $\in [0, T_{max}]$
5 after T_X do
6 X : extract nonce ρ_X
7 X : $\epsilon_X = E_{K'_S}\{t_{SX}, \rho_X\}$
8 $X \to *$: {REPLY, $\epsilon_X, k_{K'_S}$}
9 X : store t_X
10 when receive REPLY from $Y \in N_S \cap N_X$ do
11 X : store t_{YX}, c_Y
12 when receive REVEAL from S do
13 X : $k_X = \{(t_{YX}, i_Y) \mid \exists t_{YX}\}$
14 $X \to S$:
{REPORT, $E_{K'_S}\{p_X, t_X, k_X, \rho_X, Sig_X, C_X\}$}

POLL message. The verifier starts the protocol by broadcasting a POLL whose transmission time tS it stores locally (Algorithm 1, lines 2-3). The POLL is anonymous, since

1) it does not carry the identity of the verifier, 2) it is transmitted employing a fresh, software-generated MAC address, and 3) it contains a public key KoStaken from S' spool of anonymous one-time use keys that do not allow neighbors to map the key onto a specific node.

We stress that keeping the identity of the verifier hidden is important in order to make our NPV robust to attacks (see the protocol analysis in Section 6). Since a source address has to be included in the MAC-layer header of the message, a fresh, software-generated MAC address is needed; note that this is considered a part of emerging cooperative systems [2], [25]. Including a one-time key in the POLL also ensures that the message is fresh (i.e., the key acts as a nonce).

CONCLUSION:

We presented a distributed solution for NPV, which allows any node in a mobile ad hoc network to verify the position of its communication neighbors 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 neighborhood of the verifier. Simulation results confirm that our solution is effective in identifying nodes advertising false positions, while keeping the probability of false positives low. Only an overwhelming presence of colluding adversaries in the neighborhood of the verifier, or the unlikely presence of fully collinear network topologies, can degrade the effectiveness of our NPV. 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 neighbors.

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.

ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Monthly Peer Reviewed Open Access International e-Journal

[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] P. Papadimitratos, M. Poturalski, P. Schaller, P. Lafourcade, D. Basin, S. _Capkun, and J.-P. Hubaux, "Secure Neighborhood Discovery:AFundamental Element for Mobile Ad Hoc Networks," IEEE Comm. Magazine, vol. 46, no. 2, pp. 132-139, Feb. 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 Multilateration," 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.

ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Monthly Peer Reviewed Open Access International e-Journal

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

[24]http://www.nanotron.com/EN/pdf/Factsheet_nanoLOCNA5TR1. 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 – Amendment 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 & Simulation, 2009.