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

Effective Neighbor Identification with False Report Verification Using Manets

M.Abinaya[1], Mrs K.Thamaraiselvi[2]

Student, Department of Information Technology, SNS college of Technology, Coimbatore, Tamilnadu, India[1]

Asst. Prof, Department of Information Technology, SNS college of Technology, Coimbatore, Tamilnadu, India[2]

ABSTRACT- Location awareness has become an important asset in mobile system where wide range of protocols and application require knowledge of position of participating nodes. The correctness of node locations is an important issue in mobile networks, and it becomes particularly challenging in the presence of adversaries aiming at harming the system. The proactive method is Decentralized Rapid Neighbor Mapping protocol (DRNM) helps to provide a proactive solution for fast neighbor verification, selection routing protocol to avoid the attacks and To identify and verify the position of sender nodes neighbor in mobile networks for exchanging message secretly and identifying the fake position of neighbor node using Proactive methods. The clock based concepts include Time Location Neighbor stamp with clock glide which changes the time interval for reporting the details of neighbor and uses Fast Neighbor verification algorithm to identify the wormhole and Sybil attacks efficiently.

KEYWORDS- Decentralized Rapid Neighbor Mapping, Time Location Neighbor stamp with clock glides, MANETs

I. INTRODUCTION

A MANET is a peer to peer multihop mobile wireless network that has neither a fixed infrastructure nor a central server. The node can move freely in MANETs, because it is self-organizing, self-administering wireless network. Location awareness has become an important asset in mobile system where wide range of protocols and application require knowledge of position of participating nodes. For instance Location specific services for handheld devices, Traffic monitoring in vehicular networks are all the examples of services that build on availability neighbor position information.

The correctness of node locations is one of the important issues in mobile networks, and it becomes very challenging in the presence of attackers aiming at harm the system. In these cases, need such solutions that let nodes

- Correctly identify the sender's neighbor location in spite of attacks feeding fake location information, and
- Verify the positions of their neighbors, to detect attacking nodes announcing fake locations.

A novel Verification-based secure Routing is proposed, in which several forwarding candidates cache the packet that has been received using acknowledgement information. If the node contains any negative feedback, forwarder does not forward the packet through the intermediate nodes; suboptimal candidates will take turn to forward the packet according to a locally formed order. Sybil attacks, in which a compromised or malicious node can claim several locations, are possible. A key objective of secure localization scheme is to provide a cost-effective countermeasure against Sybil attacks. Black hole and selective forwarding attacks, in which an adversary drops all or selected packets, are possible. In addition to avoiding Sybil attacks by using verified location information, aim to reduce the possible damage due to packet dropping attacks by taking multiple paths towards the destination and track trustworthiness of forwarders based on their behaviour. The simplest way adversarial nodes can cooperate to make the verifier S trust the fake positions announce is by extending the basic attack introduced. More precisely, other than individually announcing POLL reception timings that agree with their fake positions, colluding adversaries can mutually validate the false information generate. It can forge the reception times of reciprocal REPLY messages, so

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

that all cross-checks in the CST involving the colluders are passed. A perfect cooperation thus results in the colluding adversaries' ability to alter all distances between them without being noticed.

The colluding attackers agree not only on the position of the verifier (either guessed or multilaterated), but also pick a non collinear common neighbor, X, that share with S: each colluder then computes the hyperbola with foci S, X, and passing through its own real position, and announces a fake location on such a curve. It deals 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.

The field of wireless and mobile communications has experienced an unprecedented growth during the past decade. Current second-generation (2G) cellular systems have reached a high penetration rate, enabling worldwide mobile connectivity. Mobile users can use their cellular phone to check their email and browse the Internet. Recently, an increasing number of wireless local area network (LAN) hot spots are emerging, allowing travelers with portable computers to surf the Internet from airports, railways, hotels and other public locations. Broadband Internet access is driving wireless LAN solutions in the home for sharing access between computers. In the meantime, 2G cellular networks are evolving to 3G, offering higher data rates, infotainment and location-based or personalized services. Hover, all these networks are conventional wireless networks, conventional in the sense that as prerequisites, a fixed network infrastructure with centralized administration is required for their operation, potentially consuming a lot of time and money for set-up and maintenance. Furthermore, an increasing number of devices such as laptops, personal digital assistants (PDAs), pocket PCs, tablet PCs, smart phones, MP3 players, digital cameras, etc. are provided with short-range wireless interfaces. In addition, these devices are getting smaller, cheaper, more user friendly and more powerful. This evolution is driving a new alternative way for mobile communication, in which mobile devices form a self creating, self-organizing and self-administering wireless network, called a mobile ad hoc network.

II. RELATED WORKS

1) 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 no cryptographic defence mechanisms. Alternatively, terrestrial special purpose infrastructure could be used, along with techniques to deal with no honest beacons. This problem is orthogonal to the problem of NPV. This assumes that devices employ one of the techniques above to securely determine their own position and time reference. In wireless systems, neighbor discovery (ND) is a fundamental building block: determining which devices are within direct radio communication is an enabler for networking protocols and a wide range of applications. To thwart abuse of ND and the resultant compromise of the dependent functionality of wireless systems, numerous works proposed solutions to secure ND. Nonetheless, until very recently, there has been no formal analysis of secure ND protocols.

2) Secure neighbor discovery (SND):

It deals with the identification of nodes which a communication link can be recognized or that are within a given distance. SND is only a step toward the solution that simply place, 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 engaged to counter wormhole attacks practical solutions to the SND problem have been proposed in , while properties of SND protocols with proven secure solutions.

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

Pervasive computing systems will likely be deployed in the near future, with the proliferation of wireless devices and the emergence of ad hoc networking as key enablers. Coping with mobility and the volatility of wireless communications in such systems is critical. Neighborhood discovery (ND) the discovery of devices directly reachable for communication or in physical proximity becomes a fundamental requirement and building block for various applications. However, the very nature of wireless mobile networks makes it easy to abuse ND and thereby compromise the overlying protocols and applications. Thus, providing methods to mitigate this vulnerability and secure ND is crucial.

3) Neighbor position verification:

It studied in the context of ad hoc and sensor networks however, existing NPV scheme often rely on fixed or mobile truthful nodes, which are supposed to be always available for the verification of the positions announce by third parties. In ad hoc environments, however, the pervasive presence of either infrastructure or neighbor nodes that can be aprioristically trusted is quite idealistic. Thus, it devises a protocol that is autonomous and does not require truthful neighbors. The problem definition of neighbor position verification (NPV) deals with a mobile ad hoc network, where a pervasive infrastructure is not present, and the location data must be obtained through node-to-node communication. Such a scenario is of particular interest since it leaves the door open for adversarial nodes to misuse or disrupt the location-based services. Similarly, fake positions could grant adversaries unauthorized access to location-dependent services, let vehicles forfeit road tolls, disrupt vehicular traffic or endanger passengers and drivers.

III. SYSTEM AND ADVERSARY MODEL

A mobile network and communication neighbors of a node take that all the other nodes that it can reach directly with its transmissions. It take for granted that each node knows its own position with some fault and that it shares a common time position with the other nodes both requirements can be met by equip communication nodes with GPS receivers.

The colluding attackers agree not only on the position of the verifier, but also pick non-collinear common neighbors. In wireless and mobile communications proactive methods and clock based concepts in order to improve the identification of attacker performance. There was a chance to provide false position information. Security plays an important role in the ability to deploy and retrieve trustworthy data from a wireless sensor network. Secure location verification with mobile station to analyze a new approach for securing localization and location verification in wireless networks. It can correctly establish their location in spite of attacks feeding false location information, and verify the positions of their neighbors, so as to detect adversarial nodes announcing false locations.

A growing number of ad hoc networking protocols and location-aware services require that mobile nodes learn the position of their neighbours. However, such a process can be easily abused or disrupted by adversarial nodes. The open issue in Neighbor Position Verification is fully distributed cooperative solution that is robust against independent and colluding adversaries, and can be impaired only by an overwhelming presence of adversaries. It shows that protocol can identified and avoid the attacks under the best possible conditions for the adversaries, with minimal false positive rates. This Neighbor Position Verification uses Message Exchange Protocol and Position verification as 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

IV. SYSTEM ARCHITECTURE

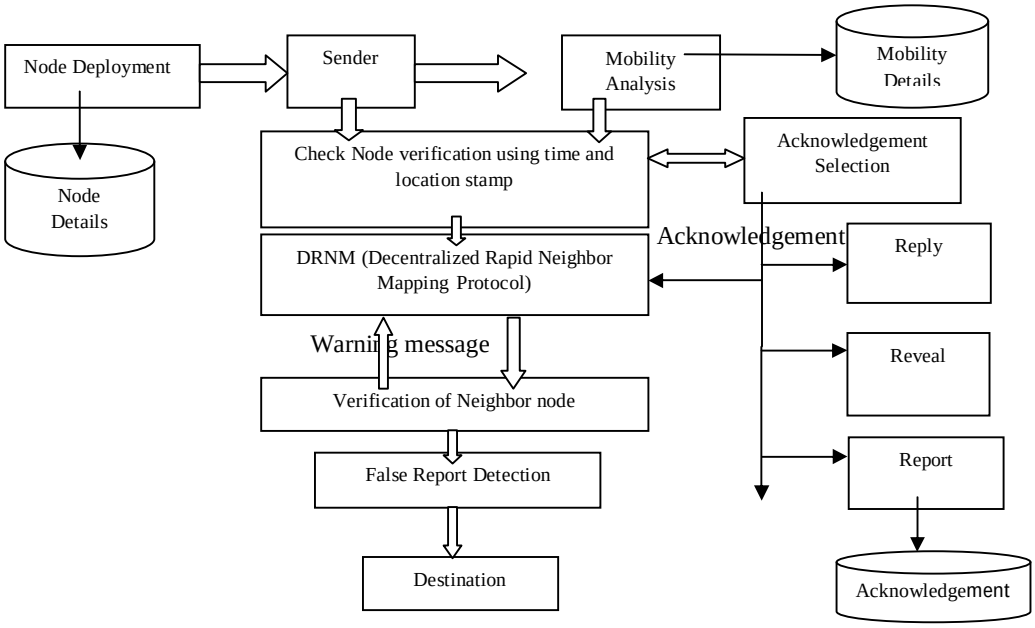

Fig:1 Architecture diagram for DRNM protocol

Architectural Design of the system includes identification of Location of neighbor nod by initializing various nodes into the network. Detailed Design is concerned with the methods involved in overall architecture includes time and location stamp, mobility analysis of particular nodes and neighbor analysis. Decentralized Rapid Neighbor Mapping protocol (DRNM) this proposed protocol helps to provide a proactive solution for fast neighbor verification and selection routing protocol to avoid the attacks. The above figure shows the source node verification by using DRNM protocol and Time Location Neighbor stamp with clock glides. Many nodes has selected for passing message secretly. Users enter the IpAddress, port number and Status of the node to register in the Database. While entering the next node the user must check the database for that node exists or new one. The positions are updated in the format of the beacon messages. The beacon messages are in the form of received Signal Strength. For accuracy verification the approximate location is verified with the updated location. The signals are converted into readable data after that the location is compared with the default map. If the approximation is wrong then the updating could be done a wrong node.

A. Basic Attack

The simplest way attacking nodes can work together to make the verifier to trust the fake positions they announce is by extending the basic attack introduced. More accurately, other than individually announcing POLL reception timings that agree with their fake positions, colluding adversaries can mutually validate the false information they generate. They can forge the reception times of reciprocal REPLY messages, so that all cross-checks in the Cross Symmetric Test involving the colluders are passed. A perfect cooperation thus results in the colluding adversary's ability to alter all distances between them without being noticed. The remark is that the adversary still needs to know the position in order to compute and present timings that confirm their fake position. This time, however, if at least three adversaries cooperate to perform the attack, they do not need to be knowledgeable. As a matter of fact, they can exploit their real positions and POLL reception times to multilaterate the coordinates of the verifier. DRNM protocol

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

correctly identifies such a basic attack through the Cross Symmetry Test, as long as the majority of the (no collinear) neighbors shared by verifier and an adversary are not colluding with the latter.

B. Hyperbola Attack

The colluding attackers agree not only on the position of the verifier (either guessed or multilaterated), but also pick a no collinear common neighbor, , that they share with each colluder then computes the hyperbola with focus and passing through its own real position, and announces a fake location on such a curve. This allows the adversaries to announce correct links

1) With the verifier

2) Among themselves

3) With the selected neighbor

which becomes an instinctive ally in the attack. Again, the location must be randomly guessed by two colluders, while it can be multilaterated by three or more cooperating adversaries. In presence of such a hyperbola-based attack, the CST correctly tags an adversary node as faulty if the no collinear common neighbors between the verifier and adversary node that do not collude with adversary node outnumber the colluding ones by 3. Note that the two additional correct neighbors are required to counter the effect of selected neighbor unintentionally taking part into the attack.

C. Jamming Attack

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, the node should jam the medium continuously for a long time, since it cannot know when exactly a node will transmit its REPLY or REPORT and could erase the REVEAL, but, again, jamming should cover the entire jitter time. Overall, there is no easy point to target: a jammer has to act throughout the DRNM execution, which implies high energy consumption and is a disruptive action possible against any wireless protocol. In addition, mobility makes it harder to continually jam different instances of the DRNM protocol run by the same verifier.

V. PERFORMANCE EVALUATION

Due to fake optimistic rates some attacks have not been identified properly like Sybil attack, hyperbola attack etc. The correctness of node locations is an important issue in mobile networks, and it becomes mostly challenging in the presence of adversaries aiming at harming the system. To identify and verify the position of sender nodes neighbor in mobile networks for exchanging message secretly and identifying fake position of neighbor node using Proactive methods and clock based concepts. The proactive method is Decentralized Rapid Neighbor Mapping protocol (DRNM) helps to provide a proactive solution for fast neighbor verification and selection routing protocol to avoid the attacks. The clock based concepts include Time Location Neighbor stamp with clock glide which changes the time interval for reporting the details of neighbor and uses Fast Neighbor verification algorithm to identify the hyperbola attack and Sybil attacks efficiently. The colluding attackers agree not only on the position of the verifier, but also pick non-collinear common neighbors. In wireless and mobile communications proactive methods and clock based concepts in order to improve the identification of attacks performance. There was a chance to provide false position information in using Neighbor Position Verification.. Security plays an important role in the ability to deploy and retrieve trustworthy data from a wireless sensor network. Secure location verification with mobile station to analyze a new approach for securing localization and location verification in wireless networks. It can correctly establish their location in spite of attacks feeding false location information, and verify the positions of their neighbors, so as to detect adversarial nodes announcing false locations.

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

VI. RESULTS

The dynamic number of mobile nodes will be initiated with the node properties such as node id, initial bandwidth etc. The movement of node pattern will follows the mobility analysis. The location and time stamp module helps to identify the position of mobile nodes and node entry time. The cluster head will collect the details frequently from the mobile node. It helps to analyze the sequence and frequent movement of the mobile node. In mobile ad-hoc network, nodes of position change due to dynamic nature. There should be a provision to monitor behavior and position of the on the regular basis. A node can selects a random destination uniformly distributed over a predefined region based on shortest distance, and moves to that destination at a random speed. A novel Verification-based secure Routing is proposed, in which several forwarding candidates cache the packet that has been received using acknowledgement information. The Geographic routing algorithm is used in DRNM protocol. If the node contains any negative feedback, forwarder does not forward the packet through the intermediate nodes; suboptimal candidates will take turn to forward the packet according to a locally formed order.

The implementation of the DRNM protocol has the following features,

- Neighborhood location information
- Neighbor list
- Distance analysis
- Candidate list
- Selecting and prioritizing the forwarding nodes.
- Mobility analysis using time stamp

For accuracy position verification the approximate location is verified with the updated location. The signals are converted into readable data after that the location is compared with the default map. If the approximation is wrong then the updating could be done a wrong node.
To enhance the protocol performance additionally the warning message has been used to overcome the large hole due to unsecure distribution in the Packet transmission scenario. In the module, the system transmits the warning message which contains the void handling mechanism based on virtual destination is proposed.

VII. CONCLUSION AND FUTURE WORKS

The results confirm that solution is effective in identifying nodes advertising false positions, while keeping the probability of false positives rates very low. The 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. 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. Decentralized Rapid Neighbor Mapping Protocol DRNM can identify only the presence of colluding adversaries in the neighbour of the verifier and the proposed protocol can overcome the problem of NPV. The Future work will aim at integrating the DRNM protocol in higher layer protocols and extending it to a Proactive methods and Clock based concepts, useful in presence of applications that need each node to constantly verify the position of its neighbours. Every node in mobile networks can send the message based on selection of first three shortest distances with the help of trusted node. The trusted node has been identified using digital signature.

REFERENCES

[1] Discovery and Verification of Neighbor Positions in Mobile AdHoc Networks (Marco Fiore, Member, IEEE, Claudio Ettore Casetti, Carla-Fabiana Chiasserini)2013
[2] P. Papadimitratos, L. Buttyan, T. Holczer, E. Schoch, J. Freudiger, M. Raya, and J.P. Hubaux, "Secure Vehicular Communications: Design and Architecture," IEEE Comm. Magazine, vol. 46, no. 11, pp. 100-109, Nov. 2008.

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

[3] P. Papadimitratos, M. Poturalski, P. Schaller, P. Lafcade, 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.
[4] P. Papadimitratos and A. Jovanovic, "GNSS-Based Positioning: Attacks and Countermeasures," Proc. IEEE Military Comm. Conf. (MILCOM), Nov. 2008.
[5] 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.
[6] R. Poovendran and L. Lazos, "A Graph Theoretic Framework for Preventing the Wormhole Attack," Wireless Networks, vol. 13, pp. 27-59, 2007.
[7] 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] R. Maheshwari, J. Gao, and S. Das, "Detecting Wormhole Attacks in Wireless Networks Using Connectivity Information," Proc. IEEE INFOCOM, Apr. 2007.
[9] R. Shokri, M. Poturalski, G. Ravot and J.P. Hubaux, "A Practical Secure Neighbor Verification Protocol for Wireless Sensor Networks," Proc. Second ACM Conf. Wireless Network Security (WiSec), Mar. 2009.
[10] 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
[11] R. Shokri, M. Poturalski, G. Ravot 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] Fed. Highway Administration, "High Accuracy-Nationwide Differential Global Positioning System Test and Analysis: Phase II Report," FHWA-HRT-05-034, July 2005.
[19] J. Hwang, T. He, and Y. Kim, "Detecting Phantom Nodes in Wireless Sensor Networks," Proc. IEEE INFOCOM, May 2007.
[20] PRECIOSA: Privacy Enabled Capability in Co-Operative Systems and Safety Applications, http://www.preciosa-project.org, 2012.
[21] 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.