Secure Position Verification Approach for Wireless Ad-hoc Networks

Samir A. Elsagheer Mohamed
(Corresponding author: Samir A. Elsagheer Mohamed)

Computer Engineerng Department, College of Computer, Qassim University, P.O.B 6688, Buryadah 51453, KSA
Electrical Engineering Department, Faculty of Engineering, South Valley University, Aswan, Egypt.
(Email: samhmd@qu.edu.sa; samirahmed@yahoo.com)

(Received Nov. 20, 2011; revised and accepted Mar. 7, 2012)

Abstract

Wireless ad-hoc networks technologies share a common requirement: each node in the network has to know its current position at any time and to share this knowledge with other nodes in the network. An attacker can deliberately attack the network by claiming to be at a different location or by injecting erroneous location information to the used positioning system. As a result, there is a great need to provide a secure position verification system for the wireless ad-hoc networks. This paper proposes a new secure and efficient approach to detect any node that announce fake location information and warn the other nodes in the networks. The proposed approach is immune against the internal and the external attacks and uses the minimum communication overhead. Another advantage is that no extra hardware is required because it uses the received signal strength to estimate the distance by the verifiers.

Keywords: Mobile ad-hoc networks, network security, position verification, vehicular ad-hoc networks, wireless ad-hoc networks, wireless sensor networks

1 Introduction

Most of the computer applications nowadays is becoming Wireless or based on the Wireless Network. A special kind of the wireless networks is the Wireless Ad-Hoc networks, where a group of wireless-capable computing devices (nodes) can randomly be connected together without using an infrastructural wireless access point. The nodes can be dispersed in a geographical area, and each node may have the ability to move in this area and still being reachable by the other nodes via the routing protocol(s). If a node is in a covering area of a node, the communication between these nodes is direct. However, if the two nodes cannot communicate directly, then a third node that can hear from both will do the routing between these two nodes. From that, the position of the nodes in the Wireless Ad-Hoc networks is of great importance to guarantee the normal operation of the networks and the supporting applications and services.

The importance of the Wireless Ad-Hoc Networks increases due to the diversity and the increasing number of their applications. In Wireless Ad-Hoc Networks, nodes may be mobile or stationary, and they have to announce their position in real time to the surrounding nodes. Malicious nodes can announce incorrect position information to threaten the network users or even collapse the network or even make the network behave unexpectedly. As a result, the security attacks and threats based on the fake position announcement of any node have to be thoroughly studied. Solutions to these attacks and threats have to be found and implemented.

The study of the position-based security attacks and weakness in the Wireless Ad-Hoc Networks [1, 18] is currently one of the most security issues in the wireless network security research community because it is impacting many other based technologies. Some examples include: 1) the Mobile Ad-hoc Networks [2, 8], where the nodes can move freely; 2) the Vehicular Ad-Hoc Networks [3, 12, 16, 19, 20], where a group of vehicles can form a network in the road to provide safety, traffic management and car entertainment applications to the passengers; 3) Wireless Sensor Networks [6, 8, 9], where a group of wireless computing devices can form an ad-hoc network and each device has a sensing ability in addition to the wireless communication capability; 4) Wireless Mesh Networks [18], an equivalent of the wireless distribution systems where a group of multi-radio wireless base stations can form an infrastructure-like network by extending the covering area of the network and providing high throughput.

It is clear that all these wireless technologies have in common the position as a basic and essential operating component. Each node has to know and broadcast its position to the surrounding nodes. This information will propagate to all the other nodes in the network. As a result, all the other nodes will make use of this information to compute something or to take some decision or action. However, if a malicious node announces its location to be at a different position, the other nodes will compute wrong information and will take a wrong action. Thus, the network will behave incorrectly and the malicious node can control the network and drive the other nodes to do harmful actions.

In this paper, a secure and efficient position verification protocol will be proposed. The proposed protocol can detect both the internal and external position-based attacks. It is uses the minimum traffic overhead of the control signals. This makes it ideal in the application having low network bandwidth (almost the case of most of the wireless technologies). A group of elected nodes in the network play the role of the position verifiers. No extra hardware is required because the received signal strength will be used as an estimate of the distance between the claiming node and the position verifiers. To provide secure communications and eliminate the possible network security attacks, a certificate authority (CA) is used and each node has to have a private and a public key.

The rest of this paper is organized as follows. First, the state-of-the-art positioning techniques used in the wireless ad-hoc networks as well as the possible attacks against them are presented in Section 2. In Section 3 the related research works are summarized. The proposed secure position verification approach is given in Section 4. A secure mechanism for warning the other nodes of the detected malicious nodes is provided in Section 5. The security analysis of the proposed approaches is detailed in 6. Finally, the conclusions and the future research directions are given in Section 7.

2 Positioning Techniques and the Attacks Against them

In this Section, we are going to provide the identified attacks and weaknesses on the wireless ad-hoc networks based on the false announcements of positions of the nodes. The attacks are classified into Internal and external attacks as given in [5]. External attacker is the one which cannot authenticate itself as an honest network node to other network nodes or to a central authority. Similarly, internal attacker refers to a compromised node or if the user controlling the node is malicious. The internal attackers announce false location information in order to cheat on their position. However, external attackers can modify (spoof) the measured positions and distances of wireless nodes. In the internal attacks the malicious and compromised nodes can authenticate themselves to the authority and to other network nodes.

It is known that GPS [21] is the most used positioning technique that can be used for Wireless Ad-hoc Networks despite its limitations: it cannot be used indoors or in dense areas or near high buildings or obstacles. Additionally, the civilian GPS is not very accurate as some measures can deviate from the true by more than 50 meters. However, the announced accuracy says 8 meters in 95% of the time. This problem can be solved by using DGPS, in which a ground base station calculate the error and send the correcting information to the surrounding nodes [21].

Attacks on the GPS positioning information if it is the civilian one is very simple. Satellite signal can be simulated and broadcast with high signal strength and hence spoof the GPS receiver by making it neglect the weak legitimated signal and use the fake one. This can lead the receiver to calculate false position information [4].

For Wireless Ad-hoc Networks, the positioning may be obtained using the Ultrasound by measuring the Time of Flight (ToF). It can be used to measure the distance between two objects. However, due to the interference, it is suitable only to the indoor applications and it is prone to two types of attacks: the enlargement and the reduction of the distance. An attacker can do so by lying about the signal sending/reception times or by simply delaying its response to honest nodes [4, 13, 20].

Another way of determining the position of the nodes in the Wireless Ad-hoc Networks is by using the received Signal Strength. Naturally, nodes in Wireless Networks possess wireless antenna and have to emit radio signals in order to transmit data. The emitted signals decay with distance, and hence it is possible to estimate the distance to an emitting node by simply measuring the received signal strength [5, 9, 19]. One nice advantage of this technique is that it does not require extra hardware and it is very simple and efficient.

However, attacks on the received signal strength exist and in some cases very simple. The node that would like to cheat on the measured distance can simply increase or decrease power level to an honest node. Malicious attackers can also modify the measured distance between two honest nodes by jamming the nodes' mutual communication and by replaying the messages with higher or lower power strengths [5].

3 Related Works

In the literature, there are two groups of approaches for location verification problem: infrastructure-based and infrastructure-less verification systems [21]. In the infrastructure-based methods, the base stations will send probe messages to the nodes and measure the distances to them, then localization algorithms will be executed to find the positions of these nodes. However, the infrastructure in this scheme will become the bottle neck of the whole system. In addition, these methods are very expensive and add additional cost to the wireless ad-hoc technology that may limit its deployment. Therefore, an infrastructure-based method is not suitable for Wireless Ad-Hoc networks [8].

On the other hand, in an infrastructure-less verification system, no base station will be used to verify the correct claimed location of the nodes. Nodes in the network will cooperate to verify the position of each other. They use several distance measure methods to localize their neighbors. These measurement techniques require that the nodes be able to measure some physical quantities that include: the RF received signal strength (RSS), time of flight (TOF) or time of arrival (TOA), angle of arrival

(AOA), etc. In some situations, challenge-response procedures are used to verify position claims. All the techniques except those using the RSS has a severe limitation which is the necessity of having ranging hardware which increases the costs of building such networks. Moreover, the effectiveness of these approaches relies heavily on the accuracy of distance or time estimation.

Examples of the infrastructure-less verification systems are as follows. In [13], there are five different independent sensors and they can give an estimation of the reliability of the other nodes position claims. These sensors can detect malicious nodes if the nodes are out of communication range or moving too fast. In [5], an approach for securing localization and location verification in wireless networks based on hidden and mobile base stations is presented. This approach uses all the mentioned physical quantities. In [4], the authors analyze the resistance of positioning techniques to position and distance spoofing attacks. They also propose a mechanism for secure positioning of wireless devices that is called verifiable multilateration. In [7], a solution to location estimation of malicious nodes based on genetic algorithms is presented. The node broadcasts a number of short messages to calculate its distance from the neighbors through the RSS.

In the literature, there are many related works that focus on the position verification approaches of a specific wireless ad-hoc network technology. Examples include the Mobile Ad-hoc Networks [8, 10], the Vehicular Ad-Hoc Networks [13, 20, 21], Wireless Sensor Networks [6, 8, 9, 19], and Wireless Mesh Networks [18].

4 The Proposed Secure Position Verification Approach

We propose the following system architecture to detect any node that try to attack the wireless ad-hoc networks by announcing false information about itself.

In order to make the position verification process secure and to illuminate the attacks coming from outside the network, the following assumptions have to be satisfied by the Wireless Ad-Hoc Network:

- Certificate Authority (CA), a predefined node that issues certificate to any node in the network and to be able to prove the identity of any node using the cryptography [14].
- Any node in the network must possess a valid certificate issued by the CA. Normally, the certificate include many fields like the serial number, the public key of the node, the encryption algorithm, the issuer, and the digital signature of the CA, etc. All the nodes know the Public Key of the CA [18].
- Any node in the network possesses a protected private key; that corresponds to the public key found in the certificate.
- The network must maintain a group of nodes to serve the function of verifying the position of any node that announces its position to the others. We refer to them as the position-verifier nodes (the more nodes used the better accuracy, details about that is given in Section 4.1). All the position-verifier nodes have a certificate like the other nodes, but additionally their certificates have special entry indicating that they are position verifiers.
- Any node that announces its position will send the information using its wireless interface. The signal will propagate to the nodes in its covering area including the position-verifier nodes. Any of the position-verifier nodes estimate the distance to the announcing node based on the received signal strength. Hence the absolute distance between the position verifiers and the announcing nodes can be estimated (details on how to map the received signal strengths into distance can be found in [7] and [9]).
- To increase the accuracy of the detection, it is preferable to have other measures to estimate the inter-distance between announcing node and the position-verifier nodes using for example Time of Arrival, etc. However, this may requires a perfect synchronization between the clocks of all the nodes. Additionally, malicious node can change its clock to tweak the system.
- To minimize the traffic overhead, nodes in the position-verifier group have to elect a leader, using the famous leader election protocol [17]. If this node fails, the group will reelect another one. Detection of node failure (e.g. battery power shortage, moving far away from the covering area of the group, etc) is possible using a simple keep-alive mechanism.
- Each node in the position-verifier group will estimate the distance to the announcing node. Then this position estimate has to be sent to the leader (See the Security Consideration in Section 5.2). Using the following technique (Section 0), the leader can verify if the announcing node is cheating in its position or not.
- Again, to minimize the traffic overhead and hence save the network bandwidth, if the leader finds that the node is announcing coherent information about its position, then it will simply do nothing.
- If the node is attacking the network by announcing erroneous location information, then the leader can detect that and sends a broadcast message informing all the other nodes to blacklist this node and not rely on the recently received information from that node (See the Security Consideration in Section 5.2).

4.1 Node’s Position Verification by the Leader

4.1.1 Case of Two-dimension Systems

The position-verifier nodes now have estimate to the distance between them and the announcing node. All the nodes in the group send their estimate to the leader. However, the distance estimate is not accurate: it can be *d*±Δ*d*. For a single node (the leader only), this can be viewed as two concentric circles as shown in Figure 1, with the small circle represent the minimum possible distance and the big circle represent the maximum possible distance estimate. The announcing node can be located at any point in the shaded area (the annulus**)** in the Figure. It is clear that the accuracy using only one position verifier is fair. However, it can detect with some confidence if the announcing node is cheating in its position or not. If the absolute location of the announcing node is not in the shaded region, then it is cheating in its position, otherwise, we are not sure.

To improve the accuracy, let’s consider two position verifiers: the leader and another node. This can be illustrated by the Figure 2. In this case, the cross-intersection between the four circles gives only two small regions. Thus, if the announcing node is estimated by the leader to be outside these regions, then it is cheating; otherwise we are almost sure that it is not cheating.

Using three position verifiers, the accuracy can be improved significantly as shown in Figure 3. The intersection of the 6 circles gives only very tiny single region for a possible location of the announcing node. It is clear now that adding more position-verifier nodes to the network will increase the accuracy. But, if we rethink about it, we can find that it is not required. Let’s explain. The announcing node cannot know how many position-verifier nodes in the network, and it cannot know their locations. Thus, even if with only two position-verifier nodes, the probability of not detecting a malicious node is very small.

4.1.2 Case of Three-dimension Systems

From the above explained mechanism, it is clear that for the 3D position verification, each circle will be replaced with a sphere. In this case, extra node is required to obtain high accuracy. For example, if with two position-verifier nodes the accuracy is acceptable in the 2D, then one need three position-verifier nodes in the 3D to obtain the equivalent accuracy. One extra condition is that the position-verifier nodes in the 3D have not be located in a straight line, but spread in the space.

5 A Proposed Secure Mechanism to Warn other Nodes of the Discovered Malicious Node

In this Section, I will provide a mechanism to warn other nodes in the network by the malicious node to avoid all the attacks that can be launched by this malicious node.

Once a malicious node is detected that is announcing false location information about itself, I am proposing the following mechanism to warn all the nodes in the Wireless Ad-hoc Network.

- Any node in the Wireless Ad-hoc Network is identified by its unique ID and in some situations by its location. In most cases, the unique ID is the MAC or physical address and/or its IP address. Since the node may cheat in its location, it is not possible to rely on the identification of the node by its location solely.

- We refer to the node that detects a malicious node as the *warning node (the leader of the position-verifier nodes or the CA)*. It can authenticate itself to the other mobile nodes in the network. To allow secure transaction and the origin authentication (from the basics of the cryptography and as mentioned before), using the Public Key Infrastructure (PKI) [14, 18], all the nodes in the network dispose of a certificate that includes their public key, the certificate serial number and the Certification Authority (CA).

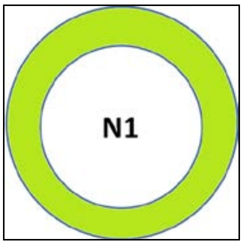

Figure 1: Position estimate using only one position verifier (the Leader): the announcing node can be located at any place in the shaded area.

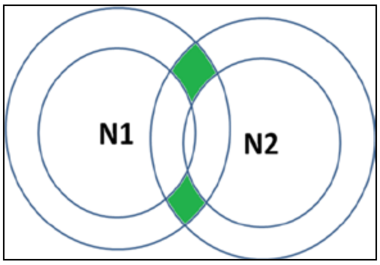

Figure 2: Position estimate using only two position verifiers: the announcing node can be located at any place in the two shaded areas (the intersection of the 4 circles). Fair accuracy of the estimate is obtained.

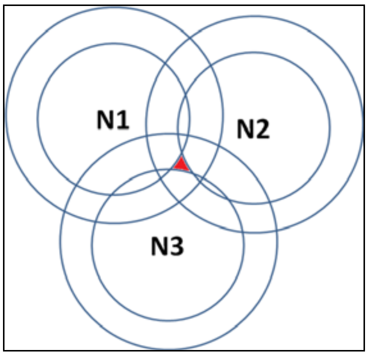

Figure 3: Position estimate using three position verifiers: the announcing node can be located at the very small

shaded region (the intersection of the 6 circles). Very good accuracy of the estimate is obtained.

- Any mobile node must maintain three lists, namely:
    - *Malicious-node* list, to hold the detected malicious nodes or the ones which have been warned by other nodes. This list has to be refreshed periodically (by removing the old entries) to reduce its size and to avoid blocking a node that has been mistakenly identified as a malicious node.
    - *Not-trusted* list, to hold the nodes that has sent a warning message but they are not authenticated by the CA. This list may be refreshed to keep the size of the list small.
    - *Trusted* list, to hold the nodes that has sent a warning message and they are authenticated by the CA. This list may be refreshed to keep the size of the list small.
- If the *warning* node detects a malicious node, it checks the *malicious-node* list first, and if it is found, then it will do nothing. If not found, it will create a *warning-of-a-malicious-node* message containing the physical ID of the malicious node.
- The *warning* node then encrypts the message using its private key and send broadcast message to the mobile nodes.
- When any of the mobile nodes receives the *warning-of-a-malicious-node* message, it has to propagate it to the nearby nodes before decrypting it.
- To avoid flooding the network, this broadcast mechanism is used. The *warning-of-a-malicious-node* message has to have a sequence number (preferably to use the timestamp: the creation time.). Thus, any node that receives a *warning-of-a-malicious-node* message, it stores in a small table the sequence number. This table is very short as it will hold only few records.
- Any node that receives a *warning-of-a-malicious-node* message, it will check if the sequence number is stored in the table or not. If it is found, then it will simply ignore this message. But if not, it will first check if the sequence number is too old (using threshold value is a must), then it will also discard the message. But if recent, it will save a record in the table and propagate it to the surrounding nodes.
- The node that receives a *warning-of-a-malicious-node message*, have then to decrypt the message using the public key of the fixed node (found in the digital certificate).
- The digital certificate of the *warning* node contains also the Certification Authority (CA), thus, to prove the identity of the fixed node, it has to communicate securely with the CA (to avoid the man-in-the-middle attack), by sending only the serial number of the digital certificate of the *warning* node.
- The CA will check the serial number. If it is not found or it is not valid (ex. Expired certificate or a revocation process is performed for this one), it will securely send a *not-valid-certificate* message to all the nodes in the networks using the broadcast mechanism described before. If on the other hand the serial number exists and the certificate is valid, then the CA will create a *valid-certificate* message having the ID and the public key of the node to be trusted by all the nodes in the networks and then send the message to all the nodes using the described broadcast mechanism. In both cases to avoid all the attacks to the communication between the nodes and the CA, the CA will encrypt the message using its private key. All the other nodes dispose for sure of the public key of the CA. Then if they could decrypt the message, then it is sent from the valid CA, otherwise, they will simply ignore the message.
- Once the node receives a *not-valid-certificate* message from the CA, it will simply add the ID of the sending node to its "*not-trusted* list". In this case, the node will ignore all the future messages from the sending node. If the node receives a *valid-certificate* message from the CA, it will add it to the "*trusted* list".
- In the previous three steps, it is expected that all the nodes will proceed with a *node-verification* process with the CA upon the reception of a message from any node. This may generate too much traffic on the network and may block the CA (it will receive too many requests in a very short period). This may be considered as a Distributed Denial of Service (DDoS) attack against the CA. To solve this problem, we have to proceed as follows:
    - Once a message is received from any node, it is very likely that all the nodes in the network receive the same message using the described broadcast mechanism (as in the *warning-of-a-malicious-node* message). Moreover, it is expected that the *warning* node is unknown by most of the nodes in the network. Thus, they have to authenticate the *warning* node.
    - If the ID of the *warning* node exists in any of the "*not-trust*" or the "*trust*" lists, then the node will not need authenticate the *warning* node with the CA. Otherwise, all the other nodes will start a random back-off timer and upon the expiration of this timer, the node

will send *a certificate-verification* request to the CA.

- Upon the reception of the first request, the CA will send using the described broadcast mechanism the status of the certificate. In this case, nodes that have their timer not yet expired, will not send a verification request to the CA. Hence, it is most likely that only very few nodes send the verification request to the CA and the others are still waiting. They will receive the status from the CA without sending a request message. Hence this decreases the traffic, and reduces the load on the CA.

- If the *warning* node is authenticated and trusted by the CA, the node will decrypt the *warning-of-a-malicious-node message* received from the *warning* node. It will then know the ID of the malicious node, and add it to its "*malicious-node* list". It will then ignore all the forthcoming messages from this node.

5.1 Features of this Mechanism

The described mechanism has several features that can be summarized as follows:

- It is very efficient and scalable to warn all the nodes in the network about the existence of the malicious node. All the nodes will be warned in the minimum possible time.

- All the communications involved are secured, thus confidentiality, data integrity, origin authentication and anti-replay are guaranteed.

- A minimum communication overhead is also guaranteed using the broadcast mechanism and the use of the *"trusted"*, *"not-trusted"*, and the *"malicious-node"* lists.

A minimum communication with the CA authenticates the sending nodes. Only a very few nodes may send the request to authenticate a sending node and the CA will send the authentication message to all the nodes at once using an efficient broadcast mechanism. This is very important to reduce the load on the CA and reduce the overhead traffic on the network. Additionally, it will conserve the battery life of the nodes as it is well-known that sending requires more power; however receiving requires almost no power.

6 Security Analysis

This Section presents the security analysis and considerations for the proposed secure position verification approach and the secure waning mechanism.

In the proposed approach and mechanism, all the communications among the nodes are secured. If the confidentiality of the exchanged data is required by the network application, then data can be encrypted using any traditional cryptosystem. Moreover, the network must take into consideration the outside attackers, the origin authentication (to be sure that the sent information is coming from the claiming node).

Outside attacks are completely avoided using the digital certificate possessed by any node. If any node does not have a valid certificate, it will be considered as intruder and hence can be black listed. Any node (normal nodes, the position verifiers and the CA) that sends to the others encrypt the data using its private key and it attach the serial number of its certificate. If any node receiving this message does not have the certificate of the sending node, then it will ask the CA by sending only the serial number encrypted using the private key of the enquiring node (this is to prove that the enquire is coming from an authenticated legitimated node). The CA knows all the public keys of the other nodes, and hence if it could decrypt the message using the public key of the inquiring node, then it will send the Certificate of the node having the serial number received, otherwise, it will send Block-this-sender message as it will be considered intruder or compromised node.

Once the inquiring node obtain the certificate of the sender, it can check if it is coming from the valid CA or not using its public key and its digital signature found in the certificate. If valid, it will use the public key of the sender to decrypt the message and proceed.

The aim of this approach is to securely provide position verification approach, thus internal attacks (any node that tries to claim to be in a different position) will be detected by the described approach. Other network security attacks will be eliminated (e.g. man-in-the-middle attack) because of the use of the previously described approach.

7 Conclusions and Future Directions

In this paper, I have presented a secure and efficient position verification approach for the wireless ad-hoc networks. A group of position-verifier nodes estimate the distance to the announcing node using the received signal strength intensity. They elect a leader that computes if the announcing node is cheating in its position or not. Upon detection of malicious node, I have presented a secure warning protocol, where the leader sends a warning-of-malicious node to all the other nodes in the network. All the communications between the nodes and the position verifiers is secured using the PKI infrastructure. The proposed approach is immune to both the internal and external attacks; it is using the minimal traffic overhead; and requires no extra hardware. The future directions may include extending this work for specific wireless ad-hoc networks for example VANET, WSN and WMN.

Acknowledgments

This study was supported by the Scientific Research Deanship, Qassim University. The author gratefully acknowledges the anonymous reviewers for their valuable comments.

References

[1] S. Abbas, M. Merabti, and D. Llewellyn-Jones, “Signal strength based sybil attack detection in wireless ad hoc networks,” *Second International Conference on Developments in eSystems*, pp. 190-195, Dec. 2009.

[2] K. Ammayappan, V. N. Sastry, and A. Negi “A new secure route discovery protocol for MANETs to prevent hidden channel attacks” *International Journal of Network Security*, vol. 14, no. 3, pp. 121-141, 2012.

[3] J. J. Blum, A. Eskandarian, and L. J. Hoffman, “Challenges of inter-vehicle ad hoc networks,” *IEEE Transactions on Intelligent Transportation Systems*, vol. 5, pp. 347-351, 2004.

[4] S. Capkun and J. P. Hubaux, “Secure positioning in wireless network,” *IEEE Journal on Selected Areas in Communications*, vol. 24 , no. 2, pp. 221-232, 2006.

[5] S. Capkun, K. B. Rasmussen, M. Cagalj, and M. Srivastava, “Secure location verification with hidden and mobile base stations,” *IEEE Transactions on Mobile Computing*, vol. 7, no. 4, pp. 470-483, Apr. 2008.

[6] Y. Chen, W. Trappe, and R. P. Martin, “Detecting and localizing wireless spoofing attacks,” in *Proceedings of the Fourth Annual IEEE Communications Society Conference on Sensor, Mesh and Ad Hoc Communications and Networks* (SECON), pp. 193-202, CA, USA, June 2007.

[7] C. J. Debono and E. Sammut, “Location estimation of an intruder in wireless ad hoc networks”, in *Proceedings of the 14th IEEE Mediterranean Electrotechnical Conference*, pp. 158-162, May 2008.

[8] D. Djenouri, L. Khelladi, and A. N. Badache, “A survey of security issues in mobile ad hoc and sensor networks,” *IEEE Communications Surveys & Tutorials*, vol. 7, no. 4, pp. 2-28, 2005.

[9] E. Elnahrawy, X. Li, and R. P. Martin, “The limits of localization using signal strength: A comparative study,” in *Proceedings of the First IEEE International Conference on Sensor and Ad hoc Communications and Networks (SECON 2004)*, pp. 406-414, CA, USA, Oct. 2004,

[10] V. C. Giruka, M. Wang, and M. Singhal, “A secure position-based protocol framework for multi-hop ad-hoc networks”, in *Third IEEE International Conference on Wireless and Mobile Computing, Networking and Communications*, pp. 55-55 , NY, USA, 2007.

[11] B. Hofmann-Wellenhof, H. Lichtenegger, and J. Collins, *Global Positioning System Theory and Practice (4th ed,*. Springer-Verlag, Vienna, 1997.

[12] J. P. Hubaux, S. Capkun, and J. Luo, “The security and privacy of smart vehicles,” *IEEE Security and Privacy*, vol. 2, no. 3, pp. 49-55, 2004.

[13] T. Leinmuller, E. Schoch, and F. Kargl, “Position verification approaches for vehicular ad hoc networks,” *IEEE Wireless Communications* ,vol. 13, no. 5, pp. 16 – 21, 2006

[14] B. Pradeep, M. M. M. Pai, M. Boussedjra, and J. Mouzna, “Global public key algorithm for secure location service in VANET,” in the *9th International Conference on Intelligent Transport Systems Telecommunications*, pp. 653-657, Oct. 2009.

[15] N. Sastry, U. Shankar, and D. Wagner, “Secure verification of location claims,” in *Proceedings of the 2nd ACM workshop on Wireless security*, pp. 1-10, NY, USA, 2003.

[16] J. H. Song, V. W. S. Wong, and V. C. M. Leung, “Secure location verification for vehicular ad-hoc networks,” in *IEEE Global Telecommunications Conference, (GLOBECOM)*, pp. 1-5, 2008.

[17] S. Vasudevan, J. Kurose, and D. Towsley, “Design and analysis of a leader election algorithm for mobile ad hoc networks,” in *The 12th IEEE International Conference on Network Protocols*, pp. 350-360, Berlin, Germany, Oct. 2004

[18] B. Wu, J. Wu, E. Fernandez, and S. Magliveras, “Secure and efficient key management in mobile ad hoc networks,” in *Proceedings of the 19th IEEE International Parallel and Distributed Processing Symposium (IPDPS),* Colorado, Apr. 2005.

[19] X. Xiaoping L. Nizhong, J. Ding, and J. Yiwen “A trusted neighbor table based location verification for VANET Routing,” in *IET 3rd International Conference on Wireless, Mobile and Multimedia Networks*, pp.1-5, Sep. 2010.

[20] G. Yan, S. Olariu, and M. Weigle, “Providing location security in vehicular Ad Hoc networks,” *IEEE Wireless Communications*, vol. 16, no. 6, pp. 48-55, 2009.

[21] G. Yan, S. Olariu, and M. C. Weigle, “Cross-layer location verification enhancement in vehicular networks,” in the *IEEE Intelligent Vehicles Symposium*, pp.95-100, CA, USA, June 2010.

[22] H. Yang, F. Ricciato, S. Lu, and L. Zhang, “Securing a wireless world,” *Proceedings of the IEEE*, vol. 94, no. 2, pp. 442-454, 2006.

[23] Y. Zeng, J. Cao, J. Hong and L. Xie, “Secure localization and location verification in wireless sensor networks,” in *IEEE 6th International Conference on Mobile Adhoc and Sensor Systems*, pp.864-869, Macau, 12-15 Oct. 2009.

Samir A. Elsagheer Mohamed obtained a B.Sc. degree in Computer and Control Systems, from the Faculty of Engineering at the University of Assuit, Egypt, in May 1994. He worked as a teaching assistant in the Faculty of Engineering at Aswan from 1995 to 1997. He obtained his M.Sc. degree in Computer Science from the University of Rennes I, France, in 1998. He obtained his Ph.D. degree in Computer Engineering from the INRIA/IRISA, University of Rennes, France, in January 2003. Then, he worked as R&D Expert Engineer at the INRIA/IRISA until June 2006. After that he moved to the Faculty of Engineering at Aswan (Egypt) to work as assistant professor. Currently, he is with the College of Computer, Computer Engineering Department, at the Qassim University, Saudi Arabia. He is also the manager of the research unit in the College of Computer. In addition, he worked as a consultant for the IT center, Qassim University. His research interests are in vehicular ad hoc networks, ad hoc network security, audio and video quality assessment in computer networks; rate based control mechanisms; video codecs; sensor networks; traffic prediction; learning algorithms for neural networks; text classifications; cryptography; and road traffic safety.