

Providing Location Security in Vehicular Ad-hoc Networks

Gongjun Yan, Stephan Olariu, Michele C. Weigle

Computer Science Department

Old Dominion University

Norfolk, VA 23529

{ygongjun, olariu, mweigle}@cs.odu.edu

Abstract

It is fair to say that most, if not all, Vehicular Ad-hoc Networks (VANET) applications rely on accurate location information. It is, therefore, imperative to provide mechanisms that ensure the integrity, availability, and confidentiality of location information. In this work, we present a number of location security mechanisms specifically designed for VANET. Proposed mechanisms for location integrity range from the use of on-board radar devices and GPS to simpler methods that rely on information fusion. We also address ways to enhance the availability of location information by selecting and maintaining stable routing paths. Finally, we discuss a mechanism that promotes location confidentiality through encryption/decryption and access control using geographical information. Our location information security mechanisms meet the requirements of the Confidentiality, Integrity, and Availability (CIA) information security model.

I. INTRODUCTION

Given its paramount importance, information security in wireless networks has received a great deal of attention. In this paper, we focus on the security of location information in Vehicular Ad Hoc Networks (VANET). As vehicles are highly mobile, most VANET applications require trustworthy location information in order to function. We base our security approach on the widely-used Confidentiality, Integrity, and Availability (CIA) information security model [1], [2].

We present validation mechanisms to provide location *integrity* in VANET. In our approach, we use network cells as security as well as communication units. Providing location integrity is thus split into intra-cell integrity and inter-cell integrity. Intra-cell integrity consists of three mechanisms. First, we assume that all vehicles are endowed with an on-board radar device, a GPS unit and a standard transceiver. To ensure intra-cell position information integrity, we propose an active validation mechanism (called *active location integrity*) which relies on the help of on-board radar to detect neighboring vehicles and to confirm their alleged coordinates. Since radar is not currently installed in all vehicles, we propose a second mechanism (called *passive location integrity*) which relies on information fusion to filter out malicious data and refine low-resolution location information into high-resolution location information. Mindful of the fact that some of the vehicles participating in the traffic may not have any of these devices, we propose a third validation method (called *general location integrity*) which combines the active and passive location integrity mechanisms. Since VANET applications often need position information of vehicles that belong to different cells, we address inter-cell position information integrity as well. Vehicles request that their neighbors or vehicles in oncoming traffic check the alleged position information of remote vehicles. Both the request and response messages are propagated among cells.

The *availability* of location information is also important in VANET. Because of the high mobility of vehicles, routing paths are often fragile and prone to disconnection. This results in situations where vehicles in different cells may not be able to communicate with each other. We propose a routing scheme that selects and maintains stable routing paths based on a better understanding of the probability distribution of car-to-car communication links under realistic traffic and radio propagation assumptions.

Given the insecure nature of wireless communication, we propose both encryption/decryption and access control mechanisms to provide location *confidentiality*. Often position information from multiple vehicles is aggregated to reduce the number of messages that are sent. In our approach, the aggregated position message is encrypted using

a key based on a geographic location that specifies the decryption region. Vehicles have to be physically present in the decryption region to decrypt and access the aggregated position information.

The relationship between the various mechanisms mentioned above is illustrated in Figure 1. By ensuring position information confidentiality, integrity, and availability, we achieve position information security that is compliant with the security requirements outlined in the Confidentiality, Integrity, and Availability (CIA) information security model.

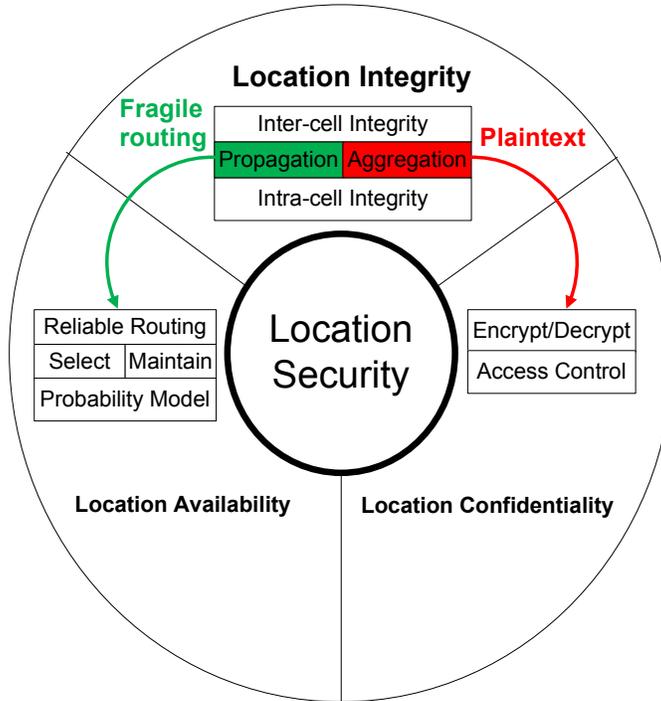


Fig. 1. Illustrating the interaction between the proposed security mechanisms.

II. SECURITY MODEL

A. CIA model

The CIA model [1], [2] is widely used in information security. The goal of the CIA model in information systems is to protect computers, software, and networks and the information they store, process and transmit. Confidentiality involves preventing disclosure of information to unauthorized individuals or systems and is often achieved by encryption. Integrity means that data cannot be modified without authorization. Availability aims to provide access to information whenever it is needed.

We are investigating a subset of information security in VANET, location information security. Guided by the requirements of the CIA model, we turn our attention to location confidentiality, location integrity, and location availability. Each of the three parts will be addressed in the following sections.

B. The attack model

Since position information is of fundamental importance in VANET, malicious parties are apt to perpetrate the following types of attacks [3]:

- Fabrication attack: involves creating and injecting spurious information in the system, examples include falsified position and/or identity information. An attacker can fabricate its own position and post it to the other participants;
- Alteration attack: involves modifying messages by tampering (among others) with the location information they contain. An attacker can modify its own position information. As a cell leader or router, an attacker can modify other vehicles' position information as well;

- Packet dropping: involves systematically (or selectively) dropping packets. As a router, an attacker can drop packets directly to launch either a black-hole attack (by dropping all packets) or a gray-hole attack (by selectively dropping packets).
- Replaying: involves re-injecting previously received/overheard packets into the network. For example, the attacker can pollute a node’s location table by replaying beacon messages.

III. LOCATION INTEGRITY

Location integrity in wireless networks is often achieved by location validation. Sastry *et al.* [4] proposed a validation protocol for wireless networks that can prove or disprove alleged location information. Vora *et al.* [5] presented a location verification method that works in wireless sensor networks. Both protocols are based on the validation of verifiers which are assumed to be trusted entities. However, this is very strong assumption that may not be realistic in VANET. Ekici *et al.* [6] proposed a location verification method for wireless sensor networks that uses a probabilistic model. The probabilistic model is based on the claim that the distribution of k -hop distances in a linear network of node density λ and communication range R is approximately Gaussian. To the best of our knowledge, however, the relationship between the k -hop distance and the Gaussian distribution has not been confirmed in the VANET literature.

A. Active location integrity

We begin by presenting our first contribution, an *active location integrity* mechanism [7]. This is motivated by the need to provide secure topology information in VANET and to build a secure network for applications. Underlying our solution is the well-known adage: “*Seeing is believing*”. We assume vehicles are equipped with GPS, an on-board radar device, a computer and a wireless transceiver. In our scheme, the on-board radar acts as a virtual *eye* of the vehicle, while the wireless transceiver acts as a virtual *ear* of the vehicle. Although the *eyesight* is rather limited due to the modest radar transmission range, a vehicle can see the surrounding vehicles and hear reports of their GPS coordinates. We expect the on-board radar device to provide useful corroboration of alleged location information, except for short transient periods. For example, the line-of-sight that radar needs may be temporarily obstructed by a large truck. Due to the dynamic nature of traffic, even if there are transient obstructions, the line of sight will eventually be restored. In accord with other VANET researchers [8], we assume that the majority of cars (about 85%) are honest players.

To overcome the inherent range limitations of radar and the wireless transceiver, we build network cells as basic security and communication units as shown in figure 2. The cells are sized such that each vehicle can directly communicate with all other vehicles in its own cell. To achieve intra-cell security, a vehicle may use its radar to verify the alleged position of neighboring vehicles in its own cell. Thus, it is reasonable to assume that each vehicle knows, with high certainty, the position of the other vehicles in its own cell. At the same time, since many applications require position information beyond the current cell boundary, we propose a method for inter-cell position information integrity. In our scheme, when a vehicle receives an aggregated message which alleges the position of a remote vehicle, it can randomly challenge the position of a vehicle in a remote cell. The challenging vehicle uses the on-board radar of remote vehicles and/or enlists the help of vehicles in the oncoming traffic. When radar is not available, vehicles can rely on reports from oncoming traffic or trusted neighbors.

B. Passive location integrity

In this subsection we propose a method to validate position information in scenarios where an on-board radar device is not available or its use is hampered by various traffic/weather conditions. Specifically, we propose a *passive location integrity* model. As already mentioned, we forgo the requirement of an on-board radar device but assume the presence of on-board GPS and transceiver. Vehicles collect location information from neighbors and oncoming vehicles. After validating and filtering out false or inaccurate locations using a data fusion algorithm, vehicles store the validated locations into memory to create a track-record (called a *Map History*) of the mobility of other vehicles. Based on the Map History, position prediction can be used to validate the announced positions. The data fusion algorithm achieves intra-cell location integrity by counting the number of location reports and abandoning reports that highly deviate from the majority of reports. For inter-cell location integrity, we apply the intra-cell position validation method in the the cell that includes the announced position.

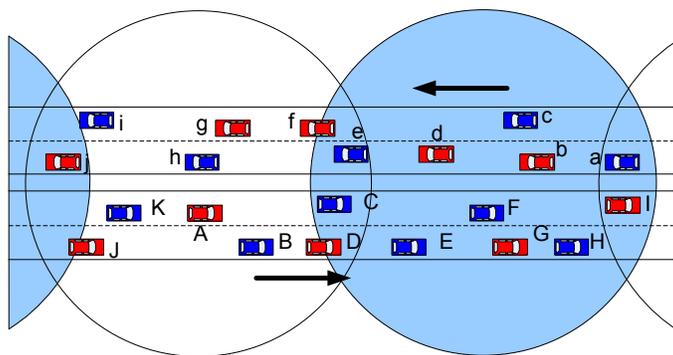


Fig. 2. Network cells.

C. General location integrity

As VANET technology will be deployed incrementally, not all vehicles will have on-board radar, GPS, and a transceiver. Some vehicles will have all three, some will have only GPS and a transceiver, while others will have none of the devices. Mindful of this, we propose a validation system that works in this scenario. Vehicles will create a Map History table using radar-validated locations, opposite traffic detected positions, and neighbor location information to achieve location integrity. Each type of data is given a weight, and we apply data fusion algorithms to filter out spurious location information.

IV. LOCATION AVAILABILITY

To provide inter-cell position information integrity, the aggregated position packets are propagated among cells. However, due to special features of traffic (*e.g.*, high speeds, rapidly changing topologies), routing paths in VANET tend to be fragile and short-lived. Key to selecting stable routing paths is a solid understanding of the probability distribution of path duration under realistic traffic and radio communication assumptions. Such a probabilistic model for car-to-car link duration was recently developed by one of the authors [9]. By incorporating this probability model into the route selection mechanism, we obtain routing paths that are reasonably stable while being, at the same time, easier to construct and maintain, both locally and globally.

A. Multi-hop path model

Not surprisingly, schemes to reduce connection failure have been proposed in the literature. For example, redundant routing paths were proposed in [10]. Geographic routing that relies on accurate position of vehicles was proposed in [11]. Ho *et al.* [12] obtained a multi-hop path using the help of structured mobility (*e.g.*, bus systems). However, these schemes are empirical and cannot determine, with any degree of accuracy, the duration of links or the probability of the existence of communication links. Further, these models consider only a few parameters such as radio signal strength or distance between sender and receiver, while ignoring important mobility and radio propagation parameters. In contrast, we assume that the inter-car headway distance (*i.e.*, the instantaneous gap between consecutive vehicles) obeys a log-normal distribution. Using this assumption and a classic radio propagation model, we derive the probability and the mean duration of a link. For details that are not discussed here we refer the interested reader to [9].

Our routing algorithm uses a unique vehicle ID (*e.g.*, electronic license plate) as the network address. The source vehicle broadcasts a probing request *Prb* on the wireless channel. All vehicles in the transmission range receive the request and compute the distance from the sender, the duration of the link, and the probability of the existence of the link. The computation is based on the formulas developed in [9]. An acknowledgment packet *AckP* will be constructed that contains the computed distance, duration, and probability of the link. The *AckP* is sent back to the sender who will collect multiple *AckPs* and select the best link – *i.e.*, the one with the highest probability and whose expected duration matches the routing path duration requirement *EDur*. The sender then sends a confirmation packet *CfmP* to the next hop on the best link. This node will further explore the routing path by broadcasting the *Prb*. When the destination node receives the *Prb*, it will terminate the probing process and will send an *AckP* back to the source vehicle along the newly formed routing path. This completes the routing path exploration stage.

B. Repairing a routing path

The basic idea of maintaining a routing path is to repair those links that are expected to break soon. The expiring links can be predicted using the link duration estimation developed in [9]. These links can be *locally* repaired by replacing them with new links formed by neighboring vehicles or *globally* reconstructed using the path discovery protocol discussed above. For a local repair, the destination vehicle initiates the process by sending a routing break packet *RBRK* at the expected expiration time of the routing path (*i.e.*, the minimum duration of the links). Vehicles which comprise the weakest link replace it with more reliable links. A global repair is similar to finding an entirely new routing path.

V. LOCATION CONFIDENTIALITY

To ensure inter-cell location integrity, the aggregated position information of several vehicles is transmitted over the wireless medium which is open to the public. If the aggregated message is in plaintext, it is vulnerable to an assortment of attacks. One simple solution is to encrypt the plaintext message by using conventional cryptography (*e.g.*, using symmetric or asymmetric keys). However, key management is a very challenging task given the huge number of participating vehicles. In addition, attackers can crack conventional cryptography by employing several well-known techniques.

To provide location confidentiality, we propose a geographic location-based security mechanism to provide physical security on top of conventional methods. Messages are encrypted with a geographic location key that specifies a decryption region. This provides *physical* security because a vehicle has to be physically present in the decryption region in order to decrypt ciphertext encrypted with this geographic location key. As an example, Figure 3 shows a shaded square which is a location-based security region. The sender vehicle *a* specifies the region, creates the location key, encrypts the message, and sends ciphertext to vehicles in this region. Vehicles outside this region, such as *b, c, d, e*, cannot decrypt the message. Only vehicle *f* can decrypt the message because it is physically inside the decryption region. Since the decryption region can be dynamically specified, attacks are extremely expensive and difficult to mount.



Fig. 3. Geographic location-based security mechanism. The shaded square is the naval base at Norfolk, VA. Only the vehicles in the shaded rectangle region can decrypt and access the received ciphertext.

A. An overview of encryption and decryption

We now discuss geographic location-based security in a client-server scenario where the server is fixed, and its public information such as GPS location and public key are known to all client vehicles. The assumptions for location-based authentication are the following:

- A trusted authority which releases the map, GPS coordinates, keys, etc.;
- Tamper-proof hardware to protect GPS information;
- Homogeneous system: vehicles are pre-installed with the proposed hardware and software.

We extend Scott and Denning's GeoEncryption algorithm [13] by removing the public key and private key requirement on client vehicles. If vehicles use PKI to communicate, they have to exchange the public key before they can communicate. Constantly broadcasting public keys is not efficient for communication, especially in real-time applications. In our scheme, client vehicles do not need public/private keys of vehicles. Only the fixed servers

have to maintain public and private key pairs. A symmetric encryption algorithm is used on clients (vehicles) because a symmetric algorithm encrypts/decrypts faster than an asymmetric one.

We use Scott and Denning’s [13] idea of a GeoLock to map the geographic location of the decryption region of the server into a lock value. This ensures that a vehicle be physically present inside the decryption region to decrypt the message. In Scott and Denning’s GeoLock algorithm, the mapping is based on a fixed table which has to be synchronized on all nodes. In our technique, the inputs to the tamper-proof GeoLock function are a GPS position and the length of the square decryption region. The GPS coordinates are divided by the length of the decryption region. The concatenation of the integral remainders of the GPS coordinates are then hashed to produce the GeoLock. To create regions of varying size, we allow the length to be specified as 1 meter, 10 meters, 100 meters, or 1000 meters. An example is shown in Figure 4.

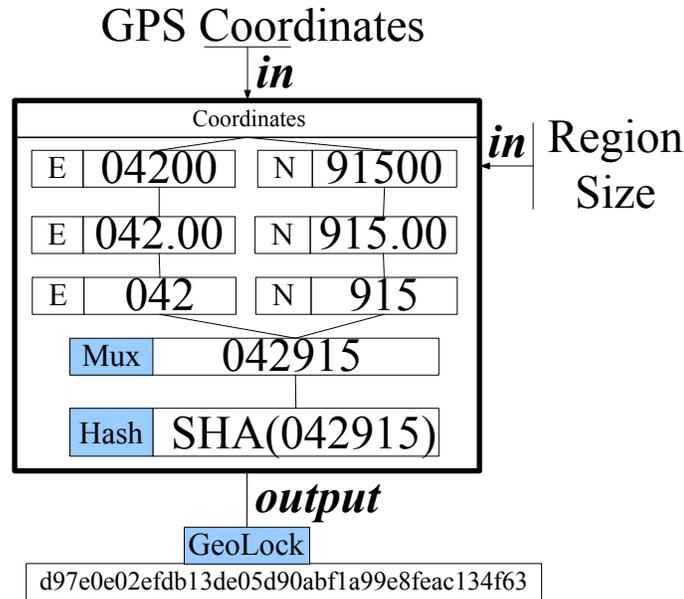


Fig. 4. An example of GeoLock. The input of region size is 100m. The GPS coordinates are divided by the region size (100), and the integral remainders are concatenated to form an input to the hash algorithm. The hash algorithm produces the GeoLock output.

Our technique involves a security key handshake stage and a message exchange stage, as shown in Figure 5. In the key handshake stage, the client and the server negotiate a shared symmetric key. The client generates two random numbers as keys Key_S and Key_C . Key_S is used to encrypt a message composed of the aggregated location message and Key_C . This encrypted message is $E\{Req\}$. The client generates a GeoLock based on the location of the server. This value is XOR-ed with Key_S and then encrypted using the server’s public key Key_E to produce the ciphertext $E\{Key\}$. Both $E\{Req\}$ and $E\{Key\}$ are transmitted to the server through the wireless channel. When the server receives $E\{Key\}$, it is decrypted using the server’s private key Key_D to produce the XOR of the GeoLock and Key_S . The GeoLock generated from the GPS location of the server is used to recover the secret key Key_S . Then, Key_S is used to decrypt $E\{Req\}$ to obtain the aggregated location message and the secret key Key_C .

In the message exchange stage, the server and client use the shared Key_C to communicate. When the server wants to reply to a client, it generates a random number, Key_S' . The reply message is directly encrypted using Key_S' to generate a ciphertext, $E\{Rep\}$. Since the aggregated location message contained the client’s GPS position, the server can generate a GeoLock of the client vehicle’s decryption region. This GeoLock is XOR-ed with Key_S' and then encrypted with Key_C to generate a ciphertext, $E\{Key'\}$. Both $E\{Rep\}$ and $E\{Key'\}$ are transmitted to the client through the wireless channel. $E\{Key'\}$ is then decrypted using Key_C to recover the XOR of the client’s GeoLock region and Key_S' . The client generates its GeoLock based on its current location. This is used to recover the secret key Key_S' . $E\{Rep\}$ is decrypted using Key_S' , and the reply message is recovered. The client repeats the algorithm in the message exchange stage to communicate with the server.

For more details on GeoLock and our geolocation encryption/decryption technique, readers are referred to [14].

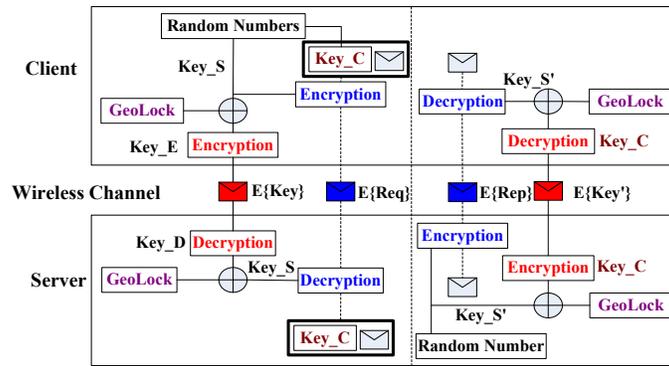


Fig. 5. Illustrating the proposed encryption and decryption scheme.

B. Location-based access control

Access control is usually granted by a unique entity that plays the role of an authenticator. Access (e.g. read, write, delete, modify, etc.) is granted only if the validation is successful. In VANET, position information can be used to enhance access control. Users are allowed to access data only in a specified region, and users outside the specified region cannot access the data. As an example, Figure 6 shows a location-based access control region which is the shaded square. The sender vehicle *a* sends a message to vehicles in this region. Vehicles outside this region, e.g. *b*, cannot read this message. Only vehicle *c* can read this message. The method to implement the location-based access control is based on GPS coordinates. In Figure 6, vehicle *a* specified a region which is described by two GPS coordinates $P_0(x_0, y_0)$ and $P_1(x_1, y_1)$. When a vehicle located at $P_2(x_2, y_2)$, receives an access-controlled message, it checks

$$\begin{cases} x_0 \geq x_2 \geq x_1 \\ y_0 \geq y_2 \geq y_1 \end{cases}$$

If the position of vehicle P_2 passes the check, it is granted access rights, otherwise access is denied.

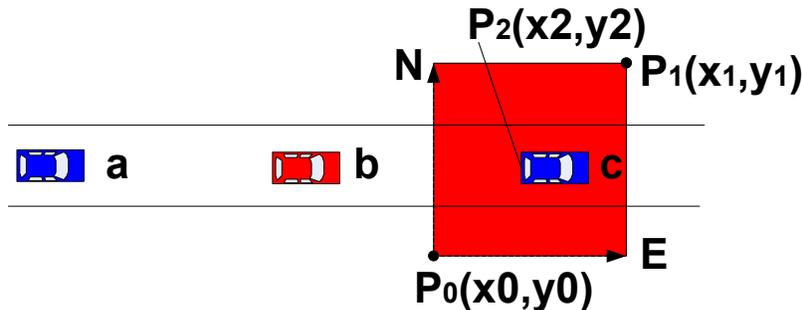


Fig. 6. Illustrating an access control region.

VI. SECURITY ANALYSIS

The proposed methods can prevent most position attacks in VANET. We now show how each type of attack is addressed by our scheme:

- Fabrication attacks: the location integrity model has three schemes to filter out fabricated location information: active, passive and general location integrity schemes in the simple to realistic scenarios (vehicles with radar, vehicles without radar, and mixture of the two types of vehicles).
- Alteration attacks: the location confidentiality model can prevent location information from being modified by unauthorized vehicles.

- Packet dropping: the location availability model can detect malicious packet dropping and establish a reliable routing path that avoids intentional packet dropping.
- Replaying: the location integrity model can validate the correctness of location information at the specified time and vehicle ID.

VII. CONCLUDING REMARKS

In this work, we have presented a number of location security mechanisms specifically designed for vehicular networks. The proposed mechanisms range from the use of on-board radar and GPS devices to simpler methods that rely on information fusion. We have also discussed ways to enhance the availability of location information by selecting and maintaining stable routing paths. Location confidentiality is also preserved by encryption/decryption and access control mechanisms based on geographical information. The three security aspects of location information meet the requirements of the CIA model. Privacy is a major concern in VANET. Since privacy is often linked with location information, the proposed location security mechanisms can be extended to protect privacy in VANET. This is an exciting area for future work.

REFERENCES

- [1] L. Volonino and S. R. Robinson, *Principles and Practice of Information Security*. Pearson Education, 2003.
- [2] M. Horton and C. Mudge, *HackNotes Network Security Portable Reference*. New York, NY, USA: McGraw-Hill, Inc., 2003.
- [3] C. Harsch, A. Festag, and P. Papadimitratos, "Secure position-based routing for VANETs," *Vehicular Technology Conference, 2007. VTC-2007 Fall. 2007 IEEE 66th*, pp. 26–30, 30 2007-Oct. 3 2007.
- [4] N. Sastry, U. Shankar, and D. Wagner, "Secure verification of location claims," in *WiSe '03: Proceedings of the 2nd ACM workshop on Wireless security*. New York, NY, USA: ACM, 2003, pp. 1–10.
- [5] A. Vora and M. Nesterenko, "Secure location verification using radio broadcast," *IEEE Trans. Dependable Secur. Comput.*, vol. 3, no. 4, pp. 377–385, 2006.
- [6] E. Ekici, S. Vural, J. McNair, and D. Al-Abri, "Secure probabilistic location verification in randomly deployed wireless sensor networks," *Ad Hoc Netw.*, vol. 6, no. 2, pp. 195–209, 2008.
- [7] G. Yan, S. Olariu, and M. C. Weigle, "Providing VANET security through active position detection," *Computer Communications: Special Issue on Mobility Protocols for ITS/VANET*, vol. 31, no. 12, p. 2883C2897, 2008.
- [8] M. Raya, P. Papadimitratos, I. Aad, D. Jungels, and J. P. Hubaux, "Eviction of misbehaving and faulty nodes in vehicular networks," *IEEE Journal on Selected Areas in Communications*, vol. 25, no. 8, pp. 1557–1568, Oct. 2007.
- [9] G. Yan, "Ph.D dissertation: Proving location security in VANET," Computer Science Department, Old Dominion University, 2009.
- [10] C. Huang, Y. Chuang, D. Yang, I. Chen, Y. Chen, and K. Hu, "A mobility-aware link enhancement mechanism for vehicular ad hoc networks," *EURASIP J. Wirel. Commun. Netw.*, vol. 8, no. 3, pp. 1–10, 2008.
- [11] C. Maihofer and R. Eberhardt, "Geocast in vehicular environments: caching and transmission range control for improved efficiency," in *Proceedings of IEEE Intelligent Vehicles Symposium*, Parma, Italy, Jun 2004, p. 951956.
- [12] I. W. H. Ho, K. K. Leung, J. W. Polak, and R. Mangharam, "Node connectivity in vehicular ad hoc networks with structured mobility," in *LCN '07: Proceedings of the 32nd IEEE Conference on Local Computer Networks*, Washington, DC, USA, 2007, pp. 635–642.
- [13] L. Scott and D. E. Denning, "Location based encryption technique and some of its applications," in *Proceedings of Institute of Navigation National Technical Meeting 2003*, Anaheim, CA, January 22-24, 2003 2003, pp. 734–740.
- [14] G. Yan and S. Olariu, "An efficient geographic location-based security mechanism for vehicular adhoc networks," in *Proceedings of the IEEE International Symposium on Trust, Security and Privacy for Pervasive Applications (TSP-09)*, Macau, China, Oct 2009.

AUTHORS

Gongjun Yan received his MS in Computer Science from University of Electronics Science and Technology of China. Currently, he is a Ph.D candidate in Computer Science at Old Dominion University. His main research areas include wireless security and Intelligent Transportation Systems. In the area of security Gongjun is mostly interested in location security, confidentiality, and availability (the so-called CIA model).

Professor Olariu received his BSc, MSc and PhD all in Computer Science from McGill University in Montreal. Over the years Prof. Olariu has held many different roles and responsibilities as a member of numerous organizations and teams. Much of his experience has been with the design and implementation of robust protocols for wireless networks and in particular sensor networks and their applications. Professor Olariu is applying mathematical modeling and analytical frameworks to the resolution of problems ranging from securing communications, to predicting the behavior of complex systems, to evaluating performance of wireless networks.

Dr. Weigle is an Assistant Professor in the Department of Computer Science at Old Dominion University. She received her Ph.D. from the University of North Carolina in 2003. Her current research interests are in vehicular networks, wireless and mobile networks, Internet congestion control, network protocol evaluation, and network simulation. Dr. Weigle is a member of IEEE, ACM, ACM SIGCOMM, and ACM SIGMOBILE.