Secure Protocol for Ad Hoc Transportation System

Johnson P Thomas, Vinay Abburi
Department of Computer Science,
Oklahoma State University, USA
jpt@cs.okstate.edu

Mathew Thomas
IBM Global Solutions,
USA

Ajith Abraham
Machine Intelligence Research Labs
Czech Republic

Abstract—**We define an ad hoc transportation system as one that has no infrastructure such as roads (and lanes), traffic lights etc. We assume that in such a system the vehicle are autonomic and can guide and direct themselves without a human driver. In this paper we investigate how a safe distance can be maintained between vehicles. A vehicle which has been compromised by an adversary can cause serious chaos and accidents in such a network (a denial of service type of attack). A simple key management scheme is then introduced to ensure secure communications between the components of the system.**

Keywords–collision avoidance, cyber-physical systems, secure communications

I. INTRODUCTION

In this paper we consider an ad hoc transportation system as a cyber physical system. We define an ad hoc transportation system as one that has no infrastructure such as roads (and lanes), traffic lights etc. Such systems may be set up and shut down quickly as needed. For example rather than build a road on a beach, an ad hoc transportation system may be set up at short notice. Such a system may also be needed in disaster areas where the infrastructure has been destroyed. Other possible application areas include under-sea and planetary transportation systems. We assume that in such a system the vehicles are autonomic and can guide and direct themselves without a human driver. In this paper we look at one particular aspect of such a system. We investigate how a safe distance can be maintained between vehicles. If the distance is below a critical point, then brakes must be applied to slow down the vehicles. This requires determining the direction and distance between vehicles. A vehicle which has been compromised by an adversary can cause serious chaos including accidents in such a network. For example, if false information is sent to neighboring vehicles, a crash may occur causing chaos and a type of Denial of Service attack in a transportation system. We propose an approach to detect malicious vehicles. A simple key management scheme is introduced to ensure safe communications between the components of the system.

Since there is no fixed transportation or other infrastructure, in our model, portable anchors can be installed in the transportation system at any point. These anchors provide the basis for determining direction and distance. We assume that vehicles are not trustworthy and therefore secure communication is only between vehicles and anchors. Insecure communication is possible between vehicles. Furthermore we assume that GPS may not be available. For example under-sea transportation systems may not have access to GPS. We consider a simplified scenario in this preliminary work.

In our approach anchors are not resource constrained and possess sufficient hardware and software to do their job. However we assume that vehicles are fully automated (no human driver), but simple and resource constrained. Any sensors and processors on these vehicles will therefore be very constrained. These may be robotic vehicles, lego type of vehicles or such vehicles designed to carry out a specific task rather than a generic kind of automobile that we commonly associate with. Such constraints also limit the use of GPS or other location detection devices. The model for the physical part of the system is first defined. Based on this underlying model, the algorithmic (or cyber) part is outlined. This is extended to make it secure.

A considerable amount of work has been done in automated transportation systems. A survey of the design and control of automated guided vehicle systems is given in [1]. Xu et. al [2] use laser scanners to avoid collisions. In our case we assume that the vehicles are not equipped with such sophisticated equipment. Determining distance and direction using simple resources is a difficult problem. Wang et al [3] propose a coordinate based system for direction based localization in wireless sensor networks. In their approach, static sensors are made aware of the direction of the sink by communicating with neighboring sensors. Some work has been done in secure vehicular communications. Many of them used certification authorities such as in [4]. Secure routing protocols for vehicles have been proposed in [5]. Authentication is vehicular networks is addressed in [6]. Our approach is different from the above works as we assume vehicles are not equipped with complex equipment, are mobile, and require not just distance, but also directional information in a secure manner. We do not assume a third party certification authority or secure inter-vehicle communications via authentication or secure routing as our approach assumes that vehicles are resource constrained and fully automated.

II. Physical Model

The physical model is briefly described here. A pair of interacting vehicles may be described by the following equations:

$$\begin{aligned} \frac{dx_A}{dt} &= a_{AA}x_A + a_{AB}x_B \\ \frac{dx_B}{dt} &= a_{BA}x_A + a_{BB}x_B \end{aligned} \qquad (1)$$

where x_A and x_B are the speeds of a pair of vehicles A and B and $x = \{x_A, x_B\}$ is the speed vector. If the speed x_A of vehicle A goes down, while the speed of vehicle B x_B is a constant, the positivity of a_{BA} will cause the rate $\frac{dx_B}{dt}$ to decrease. That is, in the automated system vehicle B will slow down or decelerate. This will cause the speed of vehicle B, x_B to decrease. A similar argument can be used to show that the positivity of a_{AB}; a_{BA} means that an increase in the speed (acceleration) of x_A implies an increase of x_B and vice-versa. The elements a_{ij} specifies quantitatively the relationship among pairs of vehicles represented by the states $\{x_i, x_j\}$ The modeling of the physical system is essential and approaches for modeling systems such as in [7] may be applied.

The physical model is as described by eq. (1). To implement this model requires hardware and software that will achieve the effects described by (1). Eq (1) states that if one vehicle slows down, then the other one has to. This equation does not capture the directional and distance relationship between vehicles. This will be discussed in a future paper. There is only a need to slow down if they are both traveling in the same direction and are close to each other.

III. Implementation of Physical System

From an implementation perspective, the physical system of eq. (1) can only be realized if directional and distance information is available. The proposed approach to derive direction and distance is briefly outlined first.

A. Model

Each vehicle is equipped with a microsecond precision clock and a sound (ultra sound - US) network interface: R is the range of the US technology. s=342m/s is the speed of sound. Two vehicles A and B are in physical proximity of each other if they can communicate directly using US, i.e $AB < R$. AB is the distance between vehicles A and B.

Each vehicle also has three simple sensors, one at the front, one in the middle and one at the rear. Anchors are placed in different places within the region of interest. These anchors carry a number of directional transmitters to beam directional signals (Fig. 1). Such transmitters have been proposed for a number of applications such as in [8]. Fig. 1 shows directional beams with an angle α. The anchor beams the direction code at regular intervals. This is to avoid interference between the signals sent out by different anchors. Anchors whose signals do not interfere with each other transmit at the same time. In Fig. 1 anchor 1 transmits in one time period, whereas anchor 2 transmits at the next time period. Each beam transmits directional information specified by a code. The first beam has a code 000. The code is incremental. Sensors in the vehicle detect the directional beams. The beam angle is the same for all beams on all anchors and is known to each vehicle before it enters the transportation system. For this paper we assume that each vehicle is aware of the ‘lane’ is in. This is an imaginary lane as there is no infrastructure. The term ‘lane’ in this paper is simply an indication of the distance from the anchor. A simple neighbor discovery protocol can be used by a vehicle to determine the lane it is in.

For example, the front sensor of vehicle A reports directional codes 100 (Fig. 1). It can be shown that under certain conditions, the number of directional codes detected by a vehicle that is further from the anchor will be less than the number of number of directional codes detected by a vehicle that is closer to the anchor. Let the set of codes received by a vehicle i be $codes_i$. For example, $codes_A$ = {011,100}.

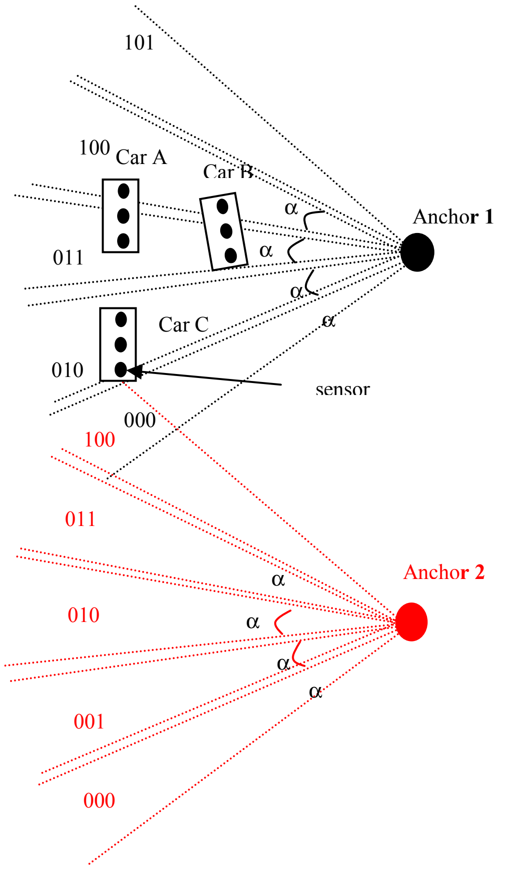

Figure 1: Beam Structure

Property 1: Given the set of direction codes, *codes$_i$* detected by a vehicle i then, $\#codes_A < \#codes_B$ where vehicle A is further from the anchor than B by at least distance d and $codes_A \cap codes_B \neq \emptyset$.

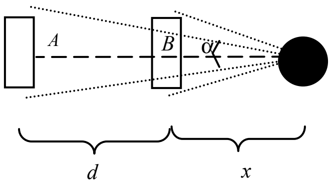

Figure 2: Distance Measurement

# is the cardinality of the set.

Proof: The range of the beam will be wider the further away it is from the anchor. Let $n_A = \#codes_A$ number of codes detected by a vehicle A (this requires at least n sensors) and let $n_B = \#codes_B$ number of codes detected by a vehicle B.

To a very close approximation we can say, for the car B with length l closest to the anchor: $l = x(n_B + 1)\tan\left(\frac{\alpha}{2}\right)$ (see Figure 2). Therefore

$$x = \frac{l/2}{\tan\left(\frac{n_B\alpha}{2}\right)} \qquad (2)$$

For a car A also of length l closest that has another car B between it and anchor $l = (n_A + 1)(x + d)\tan\left(\frac{\alpha}{2}\right)$

Therefore

$$d = \frac{l/2}{\tan\left(\frac{n_A\alpha}{2}\right)} - x \qquad (3)$$

Therefore from eq.(2) and eq.(3) we can conclude that $n_A > n_B$, that is, $\#codes_A < \#codes_B$

Property 2: A vehicles that is north will have a higher directional code than one that is relatively south.

For example a vehicle receiving directional code 100 is in front of a vehicle receiving code 000 assuming they are traveling in a northerly direction.

Theorem 1: Collision between two vehicles A and B is prevented if $codes_A \cap codes_B = \emptyset$ or $n_A \geq \delta n_B$.

Proof: From property 1, even if there is partial overlap in the codes, the horizontal distance is large enough to prevent collision. δ is some collision constant which defines the minimum distance for collision avoidance. However if the vehicles are close horizontally (that is $n_A < \delta n_B$), then the vertical distance must be large enough, that is, $codes_A \cap codes_B = \emptyset$.

B. Protocol

The anchor beams the direction code at regular intervals as outlined above. A vehicle on getting the beam from the anchor broadcasts the car or vehicle identification number (*Car_id*), and the directional beam code received from the anchor.

Anchor: Directional Beam ⟨*D_code* ⟩ where *D_code* is the directional code.
Vehicle: Broadcast ⟨*D_code, Car_id*⟩

Any vehicle that receives a signal from another vehicle has to decide whether to slow down or not. Distance alone is not a sufficient indicator. For example, although a vehicle may be physically close to a vehicle in the next 'lane', there may be no need to brake. On the other hand, a communication from a vehicle that is physically close and directly in front requires brakes to be applied. Both distance and direction therefore need to be determined.

An approximate measure of distance can be obtained by measuring the directional gap between the vehicles that transmits an anchor signal and one that receives one. This gap is measured by the signal received on the middle sensor. The difference in the codes received by the two vehicles gives the directional gap. Based on the angle α and the directional gap, it can be determined that each directional code is c units of distance. The approximate distance can therefore be calculated (see property 1). For example, in Fig. 3, car *A* of length *l* gives the distance *l* of the code 010 where car *A* is currently located.

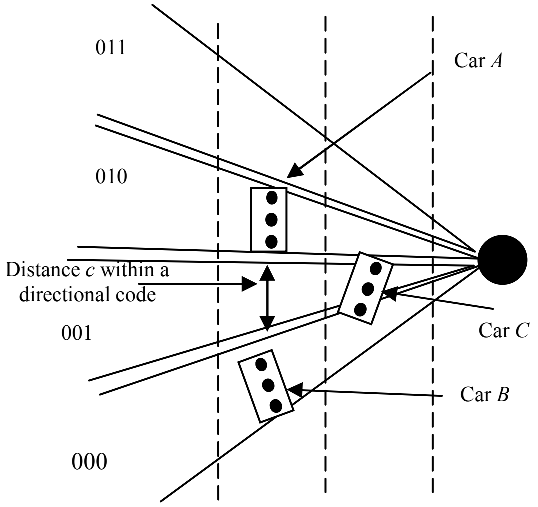

Figure 3: Calculating Distance

Direction is obtained by using properties 1 and 2. From property 1, one can determine if the vehicles are in different 'lanes' (or the horizontal distance between them). In other words, if distance *d* from eq. (3) is above a pre-determined threshold, the vehicles are in different 'lanes. If they are in different 'lanes', braking is not required. If they are in the same 'lane', then from property 2, by examining the directional codes one can determine whether a neighboring vehicle in the same lane is in front or behind and the distance between them. If the distance is too close, then braking is applied. For example, in Figure 3, from property 1, vehicle *A* is in the same 'lane' as vehicle *B*, but in a different 'lane' to car *C*. Since car *B* is in the same 'lane' as car *A*, property 1 can be used to determine if braking is required.

A major advantage of this approach is that it is robust and not dependent upon the direction the vehicle is traveling. For example in Figure 3 all three cars are facing in different directions, but the protocol will still take care of avoiding a collision.

IV. Secure Direction Discovery

A vehicle may act maliciously in such an environment. For example, a rogue vehicle may wish to cause an accident (note that the vehicles are all fully automated with no human driver), and thereby disrupt the transportation system, at least locally. This is a form of denial of service attack. This can be achieved by the rogue vehicle transmitting false codes, such that vehicles which are very close to colliding with the rogue vehicle believe the rogue vehicle to be physically far away and therefore do not brake. Anchors are not resource constrained and are therefore very secure. All anchors have the same public/private key. Hence any new vehicle that enters the transportation system is given the public key of anchors for anchor-vehicle communication. Vehicles enter and leave the transportation network dynamically. Ideally there should be secure communications between vehicles. However, to implement a key management system for secure communication between vehicles requires trusted third parties and other complex security mechanisms. Given the ad hoc nature of the systems and the simplicity of the vehicles, implementing a key management system to communicate securely between vehicles is therefore not practical. The proposed security protocol is outlined next.

A. Secure Protocol

The proposed protocol consists of three phases.

Phase I: *Key establishment*. At regular intervals a vehicle transmits a request REQ message. This is a broadcast signal that is picked up by any nearby anchors.

$\mathrm{Car_i} \underset{broadcast}{\longrightarrow}$ Anchor: $\langle \mathrm{REQ}, E_{pub,anc}\{N, K_i, MAC_{car\_id}\{.\}\}\rangle$

$E_{pub,anc}$ – public key of anchor
N – nonce to determine freshness of message
K_i – symmetric key to be used in communication between vehicle i and anchor
$MAC_{car\_id}\{.\}$ – Message Authentication code to ensure REQ message has not been tampered with.

The REQ message sends a symmetric key to the anchor that will be used in future communication between the vehicle and the anchor. The message is encrypted using the public key of the anchor. If the nonce is fresh and the message authentication code is verified, the anchor sends a reply message REP confirming the key establishment. A position pos indicating the position of the anchor is also sent to the car.

Anchor $\longrightarrow$ Car: $\langle \mathrm{REP}, K_i\{K_i, pos, t_{anc}, MAC_{anc}\{.\}\}\rangle$

t_{anc} is the time value at the anchor for the vehicle to synchronize its clock with the clock of the anchor. The car clock takes its value to be the value of $t_{anc} + t_d$ where t_d is transmission delay. Calculating a fairly accurate value for td is simple because based on the code based calculations described in section III.1 and the position pos of the anchor, the approximate distance value can be obtained. Given the approximate distance of the vehicle from the anchor, t_d can be determined.

Phase II: *Direction information from anchor*

Anchor $\underset{broadcast}{\longrightarrow}$ Car: $\langle K_1\{code,\ t_{anc}\},\ K_2\{code,\ t_{anc}\}, \ldots,\ K_k\{code,\ t_{anc}\}\rangle$

The anchor broadcasts the direction code and time of transmission at the anchor. This duet is encrypted with the symmetric key established in phase I and transmitted to all *k* vehicles. Using the *pos* field from phase I, each car decrypts the message and records the following information:

$\mathrm{Car_i}: \langle\ code,\ t_{anc},\ t_{rec}\rangle$
where t_{rec} is the time of reception of the message.

Phase III: *Neighbor Information*
Each vehicle transmits its information to other cars within range.

$\mathrm{Car_i} \underset{broadcast}{\longrightarrow}$ Car : $\langle \mathrm{INFO}, code_i, t_{anc}\rangle$

Here $code_i$ is the set of codes Cari received from the anchor. t_{anc} is the value of the anchor clock when this message was received. INFO may contain other information such as Car id or other such optional information. This message is not encrypted since vehicles do not establish keys between themselves. The message contains the codes and timestamp received from anchor. This information is used to detect if a potential collision is possible

B. Analysis

We assume that communications with the anchor is secure. The most vulnerable part of the scheme is the inter-vehicle communication in phase three where communication between vehicles is not secured and a car may send the wrong code or the wrong timestamps with malicious intent. For example, if the code suggests the car is on the side, when it is in fact in the front, this may cause a crash as the vehicle will not slow down. On the other hand, if the vehicle is on the side, whereas the code indicates it is in front, the car may slow down unnecessarily. We only consider this part of the security scheme. A more substantial analysis will be performed in a subsequent paper.

Assume a compromised or malicious car A sends a code indicating that it is in a different lane, when in fact it is directly in front of vehicle B, thereby likely to cause an accident. The clocks are all synchronized in phase I. The attacker detection algorithm is summarized below:

In phase II:

$\text{Anchor} \underset{broadcast}{\longrightarrow} \text{Car}: \langle K_1\{code, t_{anc}\}, K_2\{code, t_{anc}\},\ldots, K_n\{code, t_{anc}\}\rangle$

In phase III:

$\text{Car}_A \underset{broadcast}{\longrightarrow} \{codes_A, t_{anc}\}$

At car *B*:

```
Car_B:  Let B-Anchor_B be Car_B-Anchor distance calculated using
        codes_B  /*as in section 3.1*/
  if $time_B \leq t_{anc} + k$, then        /* $time_B$ - clock at B, $k$ is some
                                  constant indicating max time to transmit
                                  between vehicles*/
  {
    Calculate Anchor-Car_A distance using codes sent by A /* see
    property 1*/
    Calculate Anchor-Car_B distance using codes sent by Anchor
    Calculate Car_A- Car_B distance    /*cosine rule */
    B-Anchor_A = Car_B - Anchor distance
    If $\text{B-Anchor}_B - m \geq \text{B-Anchor}_A \geq \text{B-Anchor}_B + m$ then
        /*m is error range  constant */
        Attacker-detected
  }
```

In outline, vehicle *B* checks whether the distance between itself and the anchor can be verified. *B* can calculate the distance from the anchor based on the codes $codes_B$ it receives directly from the anchor. It then verifies whether this distance matches the distance it calculates using the codes $codes_A$ received from vehicle *A*. The synchronized clock signal ensures that signals are current. Car *A* therefore cannot send false codes, for example, a code indicating that it is far away when it reality it may be about to collide with *B*. The synchronization also ensures that the vehicles cannot send false timestamps. However, car *A* may be able to manipulate the code to some extent, depending on factors such as the beam angle (see next section).

Similarly it can be shown that even if the messages between vehicles are intercepted by other vehicles and replayed, the receiver is able to detect foul play. Hence even though the link between vehicles *A* and *B* is not secured, any foul or malicious activity has a high probability of being detected.

V. Simulation Results

A C program was written to validate the proposed approach. The simulation assumed 2 vehicles and a single anchor with a range of 25 units. A vehicle had length 3 units and carried 3 sensors. Due to the small area studied, the probability of a collision was high. Both cars traveled at different varying speeds which ranged from 0 units/time unit to 1.4 units/time unit.

A. *Success rate of proposed approach*

A possible collision was signaled if the cars came with 2 units of each other. The simulation results show that the proposed scheme is very 'safe' as false negatives never occur, that is, a potential collision or 'true collision' will always be detected. This is very important as the consequences of a true potential collision scenario not being flagged could have serious consequences. However, the false positives vary depending on the angle α of the anchor beams. The number of false positives vary between 9%-15% when α is between 2.5^o and 30^o, but it doubles to 30% or more when α is more than 15^o. False positives indicate the proportion of potential collisions that are flagged by the system, but are not within collision range.

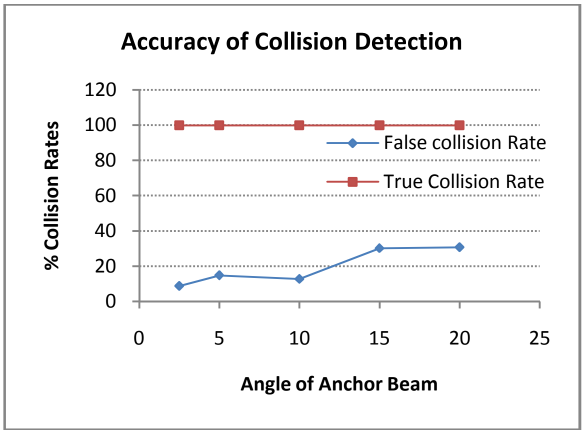

Figure 4: Accuracy of Proposed Scheme

B. *Detecting Malicious Attackers*

Malicious attackers sending false directional codes were also simulated. In the simulations, cars got closer to each other with each move. In Figure 5, the y-axis shows the percentage moves when the attacker is detected. It can be seen that at small angles of the anchor beam, such attackers are detected at all moves. Hence attackers are detected quickly. However, at larger angles, the attacker is detected only in a few of the last moves and for angle 40^o the attacker is never detected. Detection is therefore slower at larger angles and it is also possible at the larger angles for the attacker to not be detected sending false codes, which may result in a collision. That is, the codes are false and the car receiving the codes is not able to identify them as fake codes.

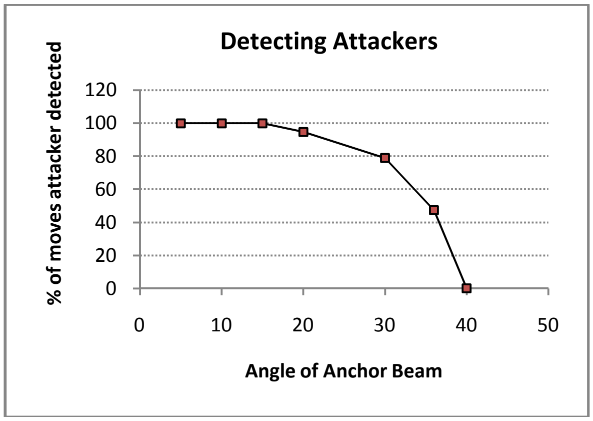

Figure 5: Detecting Malicious Attackers

VI. Conclusions

In this paper we have introduced the concept of an ad hoc transportation system. The first step in modeling the system is to describe the physical component. The corresponding cyber component is described and a secure protocol for the cyber component is outlined. The proposed model is able to detect all potential collisions, although false positives are generated. The secure protocol is able to quickly detect attackers when the angle of the anchor beams is small. As the vehicles are assumed to be resource constrained, trigonometric function values can be stored as look-up tables which minimizes resource usage. Ongoing work is investigating approaches to reduce the number of false positive collisions. A substantial security analysis is also being undertaken and both of these works will be reported in a subsequent paper. The work is also being extended to cater for wider areas and vehicles of different sizes. Cars where anchor signals cannot reach resulting in multi-hop communications is also being studied. A simpler approach would be a system where each anchor sends signals in a straight line, but this would need many more anchors.

References

[1] F A Iris, "Survey of research in the design and control of automated guided vehicle systems," European Journal of Operational Research, vol. 170, no. 3, pp. 677-709, May 2006.

[2] Hendrik Van Brussel, Marnix Nuttin, Ronny Moreas Fuyi Xu, "Concepts for dynamic obstacle avoidance and their extended application in underground navigation," Robotics and Autonomous Systems, vol. 42, no. 1, pp. 1-15, January 2003.

[3] K P Shih, C Y Chang S S Wang, "Distributed Direction-based Localization in Wireless Sensor Networks ," Computer Communications, vol. 30, pp. Pages 1424-1439, 2007.

[4] B. Aslam, F. Alserhani, I.U. Awan and J. Mellor M. Akhlaq, "Empowered Certification Authority in VANETs ," in Proc. International Conference on Advanced Information Networking and Applications Workshops, May 2009, pp. 181-186.

[5] J. Bernsen and D. Manivannan, "Unicast Routing Protocols for Vehicular Ad Hoc Networks: A Critical Comparison and Classification," Pervasive and Mobile Computing, vol. 5, no. 1, pp. 1-18, February 2009.

[6] A. Groll and C. Ruland, "Secure and authentic communication on existing in-vehicle networks," in Proc. IEEE Intelligent Vehicles Symposium, June 2009, pp. 1093-1097.

[7] D D Siljak, Large-Scale Dynamic Systems: Stability and Structure.: North-Holland, 1978.

[8] "In-Body device having a Multi-Directional Transmitter," http://www.faqs.org/patents/app/20100022836.