Analysis of Attacks Against the Security of Keyless-Entry Systems for Vehicles and Suggestions for Improved Designs

Ansaf Ibrahem Alrabady and Syed Masud Mahmud, *Member, IEEE*

***Abstract*—Remote control of vehicle functions using a handheld electronic device became a popular feature for vehicles. Such functions include, but are not limited to, locking, unlocking, remote start, window closures, and activation of an alarm. As consumers enjoy the remote access and become more comfortable with the remote functions, original equipment manufacturers (OEMs) have started looking for new features to simplify and reduce the user interface for vehicle access. These new features will provide users with an additional level of comfort without requiring them to touch or press any button on any remote devices to gain access to the vehicle. While this extra level of comfort is a desirable feature, it introduces several security threats against the vehicle's keyless-entry system. This paper describes a number of attacks against the security of keyless-entry systems of vehicles and also presents analyzes of several attacks and compares the vulnerability of the system under different attacks. At the end, some suggestions for improved design are proposed.**

***Index Terms*—Dictionary attack, keyless entry, passive-entry vehicles, rolling code, scan attack, vehicle security.**

I. Introduction

IN A CONVENTIONAL remote keyless-entry (RKE) system, a user interface is necessary to gain access to the vehicle. In this type of system, the user carries a handheld electronic device called the fob. The user presses a button on the fob in order to lock or unlock the vehicle. This action by the user initiates the transmission of a code from the fob. If the vehicle detects it as a valid code, then the vehicle locks or unlocks the doors.

The user can enjoy a higher level of comfort if an interface between the user and the fob, such as pressing a button, is eliminated. In 1993, a passive keyless-entry system for Corvette [1], which required no interface between the user and the fob. The system automatically unlocks or locks the vehicle when the user, carrying the fob, approaches or moves away from the vehicle, respectively. This system is similar to a conventional RKE system with a motion sensor built into the fob. The motion sensor triggers the fob to transmit an authorization code to the vehicle when the user starts to move [2], [3]. If the vehicle receives a valid code, it unlocks the doors. However, if the vehicle stops receiving a valid code within a certain time, it automatically locks the doors.

The aforementioned system has some design flaws, such as the following.

- An intruder can easily break the security of the system by grabbing the code transmitted from the fob and then playing it back near the vehicle while the vehicle is unattended by its authorized users.
- Since the fob keeps transmitting continuously while the user is in motion, power consumption of a fob's battery becomes an issue.

Even though Lectron's system provides the user with a higher level of comfort to enter into the vehicle, it still requires the driver to use the key for starting the engine. To provide the user with an additional level of comfort, Mercedes S-Class has introduced a different type of passive keyless system [4]–[6]. In this system, the user carries a customer-identification device (CID), which is like a credit card or a fob. When a person tries to open the vehicle's doors or trunk by pulling a door handle or to start the engine by pressing a button inside the vehicle, the vehicle sends an interrogation message. If an authorized CID is present within the vehicle's operating range, the CID responds with a valid code. After that, the vehicle performs the necessary operation.

While the main objective of the passive keyless-entry system is to provide the user with a higher level of convenience, the system must be designed in such a way that it should meet or exceed the current level of RKE security. One of the most technical challenges in designing a secure system is the communication protocol between the CID and the vehicle. The protocol has to meet the communication timing imposed by the system requirements. A fast protocol is important to ensure that the vehicle will unlock before the door handle reaches its full travel or a mechanical jam occurs. Other challenges in designing the protocol include, but are not limited to, the support of multiple CIDs for the same vehicle; synchronization between the CID and the vehicle; programming a new CID if the previous CID is lost; and, most importantly, the vehicle's security.

On the one hand, it is important to recognize that there are criminal organizations that can build sophisticated equipment to attack passive keyless vehicle systems. On the other hand, a highly secure system might be too expensive for automotive applications. For these reasons, analyzing different security threats against the system is crucial to meet the overall system requirements and design tradeoffs.

Manuscript received July 4, 2002; revised April 3, 2003, January 24, 2004, and May 21, 2004. The review of this paper was coordinated by Dr. K. Martin.

A. I. Alrabady was with Wayne State University, Detroit, MI 48202 USA (e-mail: ansafalrabady@aol.com).

S. M. Mahmud is with the Department of Electrical and Computer Engineering, Wayne State University, Detroit, MI 48202 USA (e-mail: smahmud@eng.wayne.edu).

Digital Object Identifier 10.1109/TVT.2004.838829

The rest of this paper is organized as follows. Section II shows an overview of different authentication techniques. Section III presents an overview of different attacks against the keyless-entry systems of vehicles and Section IV shows analyzes of different types of attacks. Section V presents some suggestions for improved designs and Section VI shows a summary of all the attacks, in terms of vulnerability of the vehicle system, efforts, and equipment needed from the intruder. Finally, Section VII presents the conclusion.

II. Overview of Different Authentication Techniques

There are several keyless vehicle-entry systems, such as a one-way RKE system, a two-way RKE system, and a passive keyless system. In a one-way RKE system, the user presses a button on his or her CID to initiate a communication. If the vehicle detects the CID's signal as a valid signal, then it performs the appropriate action. In a two-way RKE system, the vehicle sends a feedback signal to the CID to let the user know whether the action has been performed. In a passive keyless-entry system, the vehicle starts transmitting a low-frequency (LF) signal when the user pulls one of its door handles. The purpose of transmitting the LF signal is to wake up all CIDs, from a low-power mode, within the operating range of the vehicle. Once a CID wakes up from its sleep mode, it decodes the information received via the LF link. If the information is valid, then the CID responds with a security code. If the vehicle receives a valid code from the CID, it unlocks the doors.

Several techniques, such as fixed code, rolling code, and challenge-response techniques, can be used to transmit messages between the vehicle and the CID. The following sections show a brief description of these techniques.

A. Fixed Code Technique

In this technique, a predetermined fixed code is initially stored in a communication device. When a user action triggers this communication device, the device transmits its fixed code. If its intended receiver is present within its range, then the receiver tries to determine whether the code transmitted by the communication device is valid. If the code is valid, then the receiver performs its predefined operations. A similar technique for passive keyless-entry systems of vehicles is presented in [7]. In this technique, since the sender always transmits a fixed code, it introduces some security problems. An intruder can easily capture and record the code while the code is in transit from the sender to the intended receiver. Later on, the intruder can use the recorded code to gain unauthorized access to the receiver, say a vehicle.

B. Rolling Code Technique

In this technique, a device uses a different code for each transmission. This technique is widely used in the RKE and garage door opening systems [8], [9]. The rolling code technique maintains a sequence counter. The content of the sequence counter is the code to be transmitted when the device, say a fob, containing the sequence counter is triggered. Normally, the code is transmitted after encrypting it by using an encryption key. After each transmission, the content of the sequence counter is incremented. Fig. 1 shows a basic block diagram of a rolling code encoder.

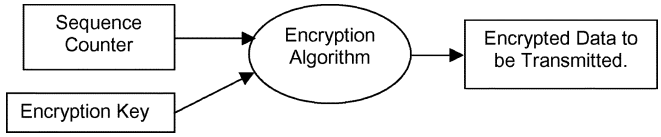

Fig. 1. Rolling code encoder.

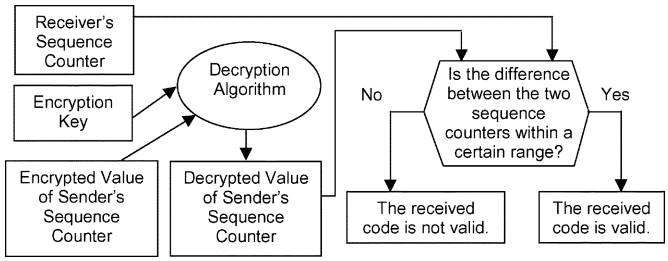

Fig. 2. Rolling code decoder.

The receiver, say a vehicle, also maintains a sequence counter in its memory. The receiver decrypts the encrypted message transmitted by the sender (a fob) to find the value of the sender's sequence counter. The receiver then compares the sender's sequence counter value with the value of its own sequence counter. If the difference between the two sequence counter values is within a certain predefined range, then the receiver validates the message from the sender and performs the required operation. The receiver also increments its own sequence counter after receiving a valid code. Fig. 2 shows a basic block diagram of a rolling code decoder.

C. Challenge–Response Technique

The challenge–response technique is widely used in immobilizer systems [10], [11]. It is also known as identify friend or foe (IFF) [12]. The challenge–response technique uses a bidirectional communication link. In this technique, both the verifier (say a vehicle) and the claimant (say a CID) share a secret encryption key. When the user pulls one of the door handles of the vehicle, the vehicle sends a random number, known as the random challenge, to the user's CID. The CID then encrypts the random challenge using an encryption key stored in it. After that, the CID sends the encrypted output to the vehicle. While the vehicle had been waiting for the response of the challenge, it also encrypted its own challenge using the same encryption key that is stored in the CID. After receiving the response from the CID, the vehicle compares it with its own calculated response. If both match, the vehicle recognizes the CID as a valid device and performs the necessary operation.

III. Overview of Attacks Against Keyless-Entry Systems for Vehicles

This section presents a discussion of different types of attacks against the keyless-entry systems for vehicles. The main security issues with such attacks are due to two main reasons. First, the intruder has unlimited access to the vehicle's door handle. Second, the intruder can solicit information from the owner's CID by generating LF signals near the owner. In the following sections, we present a brief description of the attacks that we have investigated.

A. Scan Attack

In the rolling code technique, which is used in RKE systems, the scan attack could be performed against the system by continuously transmitting different codes to the vehicle. The intruder keeps trying until one of the transmitted codes matches the one in the vehicle.

In the passive keyless-entry system, the scan attack against the system is little different. In this case, the intruder tries to gain access to the vehicle by pulling a door handle many times. Each time he sends a fixed code back to the vehicle. The intruder's main objective is to have the vehicle send a challenge that corresponds to the fixed code that he is sending. The scan attack is the simplest attack from the intruder's point of view, because the intruder does not need to know any other technical information about the system. Not all other attacks explained in this paper, are as simple as the scan attack. The probability of a successful scan attack depends on the number of bits in the random challenge, the random challenge-generation method, and the number of trials conducted by the intruder.

B. Playback Attack

The playback attack is also known as the code-grabbing attack [8]. In this type of attack, the intruder tries to record the transmitted message when the user initiates the communication. Later on, while the user is away, the intruder tries to gain access to the vehicle by playing back the recorded message. This type of attack is possible against a communication system in which the transmitted message does not change each time the system is triggered.

C. Two-Thief Attack

This is a widely known attack [13], [14] against the challenge–response technique used in the passive keyless vehicle system. In this attack, two thieves build an electronic bridge between the vehicle and CID. One thief stands near the vehicle and the second stands near the owner of the vehicle. The thief who stands near the vehicle pulls a door handle of the vehicle in order to receive the signal transmitted by the vehicle. This thief then sends the signal, after amplification, to the second thief, who stands near the owner. The second thief receives the signal from the first thief and sends it to the owner's CID. The second thief then receives the response from the CID and sends it to the first thief. The first thief then sends the signal to the vehicle. The vehicle then unlocks the doors. Thus, in this type of attack the thieves will always be successful as long as they have the right electronic equipment.

D. Challenge Forward Prediction Attack

In this attack, the intruder tries to predict the next challenge by observing the previous few challenges. The intruder can obtain the challenges by pulling a door handle several times. If the intruder has a method of predicting the next challenge, then the intruder can go near the owner of the vehicle and generate such a predicted challenge. He can then record the CID's response. After that, the intruder can go back to the vehicle and pull a door handle to trigger the system. In response, the intruder will play the message recorded from the CID. The intruder will be successful in his attack, provided that the vehicle generates exactly the same challenge that the intruder had predicted.

E. Dictionary Attack

In this attack, the intruder builds an electronic dictionary. Each entry in the dictionary consists of a valid (challenge–response) pair. The intruder can do this by simply generating a random challenge next to the vehicle's owner, who happened to carry the CID. The intruder then captures the CID's response and stores it in the dictionary with the corresponding random challenge. Once the intruder builds up his dictionary, he can go back to the vehicle and keep pulling the door handle, hoping that the vehicle would generate a challenge that is already stored in his dictionary.

IV. Analysis of Attacks Against Keyless-Entry Systems for Vehicles

In this section, we present analyses of different attacks and compare the vulnerability of the system from one attack versus another. We measured the vulnerability in terms of how easy or difficult it would be for an intruder to break the security of the vehicle. If it is possible for the intruders to break the security of the vehicle, then we measured the strength of an attack in terms of how long it would take an intruder to break the security. Our analyses will help the system designers to come up with a better design to protect the vehicle against different types of attacks.

Out of the five types of attacks explained in Section III, the two-thief and playback attacks are deterministic attacks and the other attacks are probabilistic attacks. For the probabilistic attacks, the success of the intruder depends on many factors, such as how long the random challenge is, how the challenge has been generated, how easy it is to collect a large set of challenges by pulling a door handle of the vehicle, and how easy it is to solicit information out of the CID.

A. Generation of a Random Challenge

One of the basic components of a random challenge is a random number. A random number can be classified as dependent, partially dependent, or independent of the previously generated numbers. In the one extreme case, the random number can be cyclic. This means that a random number that is generated this time will not be generated again until all numbers within the random number space are generated. On the other extreme case, the random number is independent of the previously generated number, i.e., the probability of getting the same random number in the next time is the same as the probability of getting any other random number from the random number space. We call such a random number the *noncyclic random* number.

We present a generic model, shown in Fig. 3, for generating a random number. Our model has been designed based on an encryption algorithm. We assume that the encryption algorithm is similar to the DES algorithm [15] with the following properties

The secrecy of the encryption is in the encryption key, not in the algorithm, because every device that will encrypt an item has its own unique encryption key. This means that even if the

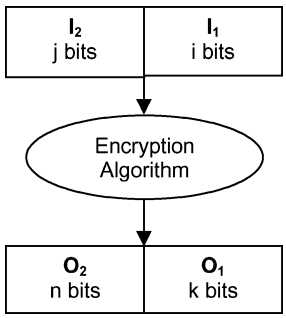

Fig. 3. Generation of a random number.

intruders know the encryption algorithm, the strength of the encrypted transmission will not be defeated, because the intruders cannot know the value of the encryption key.

The algorithm is one-to-one and reversible. This means that if plain texts P1 and P2 are, respectively, converted to cipher texts (encrypted texts) C1 and C2 using an encryption key K, then C1=C2 if and only if P1=P2 and *vice versa*. This also means that the number of input bits is equal to the number of output bits, but the key could be of any length.

Avalanche Effect: A one-bit change in the input will cause, on average, half the output bits to change using the same encryption key. In addition, a single-bit change in the encryption key will cause, on average, half the output bits to change using the same input. Moreover, we assume that each bit has a 50% chance to change if a single bit changes in the encryption key or the input.

The model presented in Fig. 3 shows an encryption algorithm that takes an input that has two blocks, I_1 (i bits) and I_2 (j bits). The output of the algorithm also has two blocks, O_1 (k bits) and O_2 (n bits). Due to the second property of the encryption algorithm, we can say that $i + j = k + n$.

The method that we used in this section assumes a sequence counter of i bits that is stored in a nonvolatile memory. The sequence counter is used as the input (I_1) to the encryption algorithm for the model shown in Fig. 3. The sequence counter value is incremented by one every time a call to the algorithm is made. For this method, we consider that the sequence counter is the only input (I_1) to the algorithm, i.e., $j = 0$. The other input (I_2) is not available. Since we are using an encryption algorithm, we expect that for each value of the i-bit sequence counter, there is a corresponding output that consists of i ($i = k + n$) bits. We use the lower k bits (O_1) to represent the random number. The other part of the output (O_2) is not used, but is available for randomization purposes, as explained later.

Let R_h be the value of the random challenge (available at O_1) when the sequence counter is equal to h. Then there exists an X such that $R_h = R_{h+X}$ for all $0 \leq h \leq 2^i$. If the only value of X that satisfies the previous condition is $X = 2^i$, then we say that the challenge is a random number with a maximum cycle. A random number with a maximum cycle does not repeat the sequence until all 2^i combinations are generated.

For one cycle of the sequence counter, there are $2^i = 2^{k+n}$ different numbers available at the output of the encryption algorithm shown in Fig. 3. For each value of O_1, there are 2^n combinations of O_2. Thus, every random number R ($0 \leq R \leq 2^k - 1$) appears 2^n times within one cycle of the sequence counter.

We have already defined a random number as a noncyclic random number if the probability of generating such a number remains the same no matter how many times this number has already been generated. Our model, shown in Fig. 3, will generate such a random number if n is a very large number.

For one cycle of the sequence counter, there are $2^i = 2^{k+n}$ different numbers available at the output of the encryption algorithm shown in Fig. 3. For each value of O_1, there are 2^n combinations of O_2. Thus, every random number R ($0 \leq R \leq 2^k - 1$) appears 2^n times within one cycle of the sequence counter.

We have already defined a random number as a noncyclic random number if the probability of generating such a number remains the same no matter how many times this number has already been generated. Our model, shown in Fig. 3, will generate such a random number if n is a very large number.

Lemma 1: A noncyclic random number can be generated if $n \to \infty$.

Proof: Let U be the number of random numbers already generated. Let L be the number of times a specific random number R is generated within the U random numbers. The probability that R would be generated again is given by

$$p = \frac{2^n - L}{2^i - U} = \frac{2^n - L}{2^{k+n} - U} = \frac{1 - \frac{L}{2^n}}{2^k - \frac{U}{2^n}}. \tag{1}$$

If $n \to \infty$, then $L/2^n \cong 0, U/2^n \cong 0$. Therefore, (1) reduces to

$$p \cong \frac{1}{2^k}. \tag{2}$$

Hence, if $n \to \infty$, then the probability of generating a random number R during the next trial is $1/2^k$, a constant value for a fixed value of k. This means that the probability of generating the number R again is independent of the fact, how many times the random number R has already been generated. We can consider the term n as the randomization factor because the value of n determines how random the numbers are going to be.

For a practical system, the value of n cannot be very large, because the cost of the system will be high for a very large value of n. If n is a very large number, then the system response will also be very slow, because the encryption algorithm will take too much time to do the encryption. However, doing our analyses with a noncyclic random number gives a theoretical limit on the results of our analyzes. The results of our analyses also show that we can design a system with a relatively low value of n and get a performance almost as good as that of a system with n equal to infinity, if we increase the size of the random challenge (O_1) by 1 bit.

B. Analysis of a Scan Attack

To measure the security of the system against the scan attack, we determine the probability of a successful attack after m trials by the intruder. At the first trial, the probability that the vehicle generates a challenge that corresponds to the intruder's fixed response is equal to $p_0 = 2^n/2^{k+n}$. If the intruder is not successful during the first trial, then the probability that the intruder will be successful during the second trial is $p_1 = 2^n/(2^{k+n} - 1)$. In general, if the intruder is not successful

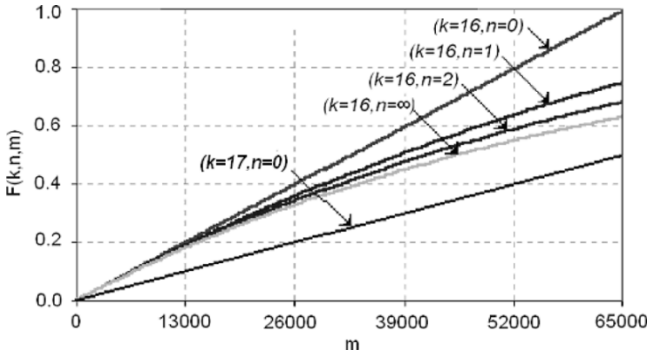

Fig. 4. Probability of a successful scan attack in m trials.

during the first jth trial, then the probability that the intruder will be successful during the $(j+1)$th trial is $p_j = 2^n/(2^{k+n} - j)$. If the intruder is not successful in all his trials, then the probability of a nonsuccessful attack, after trying m times, is given by

$$p(k,n,m) = \prod_{j=0}^{j=m-1} (1-p_j) = \prod_{j=0}^{j=m-1} \left(1 - \frac{2^n}{2^{k+n} - j}\right). \tag{3}$$

Let $F(k,n,m)$ be the probability of a successful attack within the first m trials for a system that uses k bits for the random challenge and n bits for the randomization factor. The value of $F(k,n,m)$ can be expressed as

$$F(k,n,m) = 1 - \prod_{j=0}^{j=m-1} \left(1 - \frac{2^n}{2^{k+n} - j}\right). \tag{4}$$

Note that $F(k,n,m)$ is the cumulative distribution function (cdf) of random variable m. It should be noted that (4) is valid only for $1 \leq m \leq 2^n(2^k - 1)$. If $m > 2^n(2^k - 1)$, then $F(k,n,m)$ assumes a value of 1. If $n \to \infty$, the challenge is a noncyclic random number. In this case, $F(k, n \to \infty, m)$ reduces to

$$F(k, n \to \infty, m) = 1 - \left(1 - \frac{1}{2^k}\right)^m. \tag{5}$$

If $n = 0$, the challenge is cyclic. In this case, the probability of a successful attack within the m trials can be simplified to

$$F(k,0,m) = \frac{m}{2^k}. \tag{6}$$

A plot of $F(k,n,m)$, for n =0,1,2, and ∞ and $k = 16$ is shown in Fig. 4. A plot of $F(k,n,m)$ for $n = 0$ and $k = 17$ is also shown in Fig. 4.

From Fig. 4, it is clear that, for a given value of k, say $k = 16$, there is not much difference in the value of $F(k,n,m)$ for $n = 2$ and $n = \infty$. So for a given value of k, the vulnerability of a system due to a scan attack for $n = 2$ will be very close to that for $n = \infty$.

An important security measure of the system is to find the average time needed by an intruder to have a successful attack. We will call this time as the *average attack time* (AAT). Let W be the number of times that a user can trigger a vehicle system per unit time. We assume the following system parameters to show the value of AAT for different cases:

- vehicle supports four different CIDs and each CID responds in an assigned time slot;
- vehicle can be triggered once every 200 ms;
- if the vehicle receives five consecutive unsuccessful invalid responses to the challenge from all four CIDs, the vehicle inhibits the system for 7 s.

In this case, W can be calculated as

$$W = \frac{4*5}{0.2*5 + 7} = 2.5 \ \frac{\text{trials}}{\text{s}}. \tag{7}$$

If the average number of trials for a successful attack is $E(k,n)$, then the AAT can be expressed as

$$\text{AAT} = \frac{E(k,n)}{W}. \tag{8}$$

To find $E(k,n)$, we need to calculate the probability distribution function (pdf) $f(k,n,m)$ of the random variable m as

$$f(k,n,m) = F(k,n,m) - F(k,n,m-1). \tag{9}$$

For $n = 0$

$$f(k,0,m) = \frac{1}{2^k}. \tag{10}$$

The average number of trials for $n = 0$ is given by

$$E(k,0) = \sum_{m=1}^{2^k} m*f(k,0,m) = 2^{k-1}. \tag{11}$$

Similar analysis can be done for $n \to \infty$. In this case, the average number of trials is given by

$$E(k, n \to \infty) = 2^k. \tag{12}$$

If $W = 2.5$ and the challenge is a 16-bit number, then, for a cyclic challenge, a scan attack will take approximately AAT =3.64 h. If the challenge is noncyclic, the AAT will be 7.28 h. In general, for $k = 16$ and $W = 2.5$, the value of AAT is in the range of 3.64–7.28 h, depending on the value of the randomization factor n. A higher n leads to a higher value of AAT. However, if we increase the value of k by 1, then $E(k+1,n)$ for $n = 0$ is equal to 2^k, which is same as $E(k,n)$ for $n \to \infty$. This means that

$$E(k+1,0) = E(k, n \to \infty). \tag{13}$$

Fig. 4 shows that, for $k = 16$, even a low value of n, say n =3 or 4, can be almost as good as the case where $n \to \infty$. From these results, it is clear that if the challenge is cyclic, then we need to transmit an extra challenge bit to have a comparable secure system to the one that uses a noncyclic random challenge. However, adding an extra bit in the challenge will slightly increase the CID's response time, because the CID will have to process one extra bit. This may also slightly reduce the CID's battery life. A higher value of n will not have any affect on the battery life of the CID. However, a higher value of n is not a

good choice to protect the system from another type of attack, as described in Section V.

In summary, we can say that we can increase the security of the system against the scan attack by incorporating one or more of the following features:

- decrease the number of times the vehicle can generate a challenge per unit time;
- increase the number of challenge bits;
- increase the randomization factor n.

Although these features will increase the security of the system against a scan attack, each has some disadvantages associated with it. For example, the first feature has some disadvantage from the system's reliability point of view. The second feature will increase the access time; hence, it will affect smooth operation. The second feature will also reduce the CID's battery life. The third feature will require more EEPROM space in the vehicle as the value of n increases.

C. Analysis of a Playback Attack

Such an attack can be easily performed against a system that employs a one-way communication, such as the communication mechanism used in the system that is designed based on a motion sensor. In this type of system, the intruder can easily collect the codes transmitted by the CID just by staying close to the owner of the vehicle. While the owner of the vehicle starts to move, the CID starts transmitting. The intruder can easily capture and record the code transmitted by the CID. The intruder can then play this recorded code after going near the intended vehicle.

The playback attack also is a powerful attack for a system that uses a two-way communication without using a challenge–response technique. For example, if only an LF signal is used to wake up the CID without generating a random number when a door handle is pulled, then the intruder's task could be as simple as building a device to generate an LF signal with a radio-frequency (RF) recorder. The intruder can generate the LF signal near the owner of the vehicle to solicit response from the CID. After that, the intruder can record the CID's response. The intruder can then go to the vehicle and pull a door handle for the vehicle to transmit an LF signal. The intruder can then respond to the vehicle's LF signal by playing the message recorded from the CID. Thus, the security of the vehicle system will be compromised if a simple two-way communication without using a challenge–response technique is used between the vehicle and CID.

The *playback* attack is not possible if the transmitted code, from both sides of the communication link, changes every time the system is triggered.

D. Analysis of a Two-Thief Attack

Section III mentioned that two thieves can implement an attack by building an electronic bridge between the vehicle and CID. The current keyless vehicle systems use an LF signal from the vehicle to the CID and an RF signal from the CID to the vehicle [13]. For this type of vehicle system, the two-thief attack is a deterministic attack, because the thieves will be able to break the security if they have the appropriate electronic devices. We proposed a solution for a multiple-thief attack problem against the passive keyless vehicle systems [17]. In our solution, a bidirectional RF communication link is used between the vehicle and the CID, in addition to the unidirectional LF communication link from the vehicle to the CID. To protect the system against attacks from more than two thieves, we proposed that the CID should send signals using two different power levels and the difference between the power levels must be greater than a threshold value. If the system is built as we proposed [17], then two or more thieves will not be able to break the security of the passive keyless vehicle systems.

E. Analysis of a Challenge Forward Prediction Attack

In this attack, the intruder tries to predict the next challenge by observing the previous few challenges. It is not an easy attack for the intruder to implement if the challenge has a good randomness property. The randomness property can be improved by increasing the values of k and n in the model shown in Fig. 3. If the values of k and n are large, then the intruder may also need to observe a large set of challenges in order to do some kind of predictions. If the vehicle system is properly designed, then the intruder can be prevented from collecting a large set of challenges in a short time. For example, if the vehicle system is designed in such a way that it would stop generating more challenges for a while if it did not receive valid responses for the previous few challenges, then the average number of challenges generated per unit time can be reduced. If we use the same design parameters that we used for the analysis of the scan attack, then the intruder will be able to collect only five challenges within 8 s. The main difference between the scan attack and this attack is that in the scan attack the intruder can stay near the vehicle as long as he wants and keep trying to become successful without requiring to find the owner with the CID. However, in the challenge forward prediction attack, the intruder has to find the owner with the CID to get a response for the predicted challenge. Therefore, in this type of attack the intruder cannot stay near the vehicle hours after hours for collecting the challenges. In order to protect the vehicle from this type of attack, the random challenge should be generated using a cryptographic generator so that the intruder cannot easily predict the next challenge based on a small set of previously captured challenges. We want to emphasize that the linear congruential method should not be used to generate random challenges, because these types of challenges can be predicted easily [16].

F. Analysis of a Dictionary Attack

In this attack, the intruder builds an electronic dictionary. Each entry in the dictionary consists of a valid (challenge–response) pair. The intruder can do that simply by generating a random challenge near the vehicle's owner, who happened to carry the CID. The intruder can then capture the CID's response and store it in the dictionary with the corresponding random challenge. Once the intruder builds his dictionary, he can go back to the vehicle and keep pulling the door handle, hoping that the vehicle would generate a challenge that is already stored in his dictionary. This method enables an intruder to implement a powerful attack against a keyless vehicle. To illustrate the threat of such an attack, we calculate the probability of a successful

attack. For simplicity of mathematics, we assume that the challenge generated by the vehicle is a noncyclic random number, i.e., $n \to \infty$ for the model shown in Fig. 3. By doing the analysis in a way that is similar to the scan attack, we can show that the probability of a successful attack within x trials (pulling the door handle x times) is

$$F(x) = 1 - \left(1 - \frac{D}{T}\right)^x \tag{14}$$

where, D is the size of the dictionary and $T = 2^k$ is the size of the challenge space. In fact, $F(x)$ is the cdf of the random variable x. After doing some mathematical calculations, one can easily show that the mean value of the random variable x is

$$E(x) = \frac{T}{D}. \tag{15}$$

Thus, the average number of trials for a successful dictionary attack is T/D. However, building the dictionary takes some time. If building each entry in the dictionary takes the same amount of time as to trigger the vehicle for sending a challenge, then the intruder would try to split the time between building the dictionary and triggering the vehicle in such a way that he can maximize the probability of a successful attack. Assume that each trial takes one time unit. Then, for a given dictionary size D, the average time the intruder needs to implement a successful dictionary attack is $E(x)+D$. Thus, the intruder would try to determine the value of D in such a way so that the term $E(x)+D$ becomes minimum. Using (15), we can write

$$E(x) + D = \frac{T}{D} + D. \tag{16}$$

By taking the derivative of (16) and equating to 0, we find that in order to minimize the intruder's time in implementing a successful attack, the dictionary size should be $D = \sqrt{T}$. For this case, $E(x) = T/D = \sqrt{T}$. Now, from (16) we get $E(x) + D = T/D + D = 2\sqrt{T}$. Since $T = 2^k$, the average time needed by the intruder to implement a successful dictionary attack is $2\sqrt{T} = 2^{(k/2)+1}$. If the vehicle's challenge is noncyclic, i.e., if $n \to \infty$, then from (12) we find that the average number of trials that an intruder will need to have a successful scan attack is 2^k. Hence, the intruder can significantly reduce the average number of trials for a successful attack if he tries to implement a dictionary attack as opposed to the scan attack. The intruder can reduce the time by a factor of

$$\frac{\text{Average} - \text{Trials} - \text{For} - \text{Scan} - \text{Attack}}{\text{Average} - \text{Trials} - \text{For} - \text{Dictionary} - \text{Attack}} = \frac{2^k}{2^{k/2+1}} = 2^{(k/2)-1}. \tag{17}$$

However, the price that the intruder has to pay for a dictionary attack is that he has to have more hardware devices, such as a transceiver and a storage device to build the dictionary. For a scan attack, the intruder has to have only a device to transmit a fixed code. Now, the question is how realistic it is for an intruder to build a dictionary of size $\sqrt{T} = 2^{k/2}$. The answer depends on the value of k. If $k = 16$, then the dictionary has to have 256 entries. Building a dictionary of size 256 may be possible for the intruder. However, if $k = 32$, then the dictionary has to have 65 536 entries. For all practical purposes, it would be difficult to build such a large dictionary.

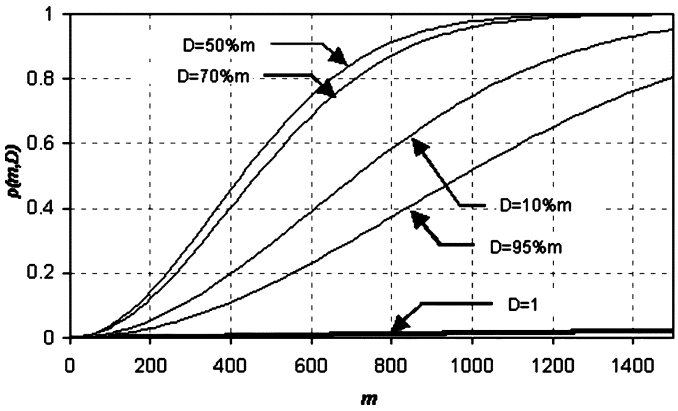

Fig. 5. Probability of a successful dictionary attack in m trials.

If the intruder does not have time to build a dictionary of size $\sqrt{T}$, then he may chose to build a smaller dictionary. Let us assume that altogether the intruder wants to go for m trials and that, out of these m trials, he will use D trials to build the dictionary and the remaining m-D trials to trigger the vehicle system by pulling a door handle. If the size of the dictionary is D and if the intruder pulls a door handle m-D times, then we can show that the probability of a successful attack is

$$p(m, D) = 1 - \left(1 - \frac{D}{C}\right)^{m-D}. \tag{18}$$

Fig. 5 shows the value of $p(m, D)$ versus m for different values of D. In the plot, D is represented as a percentage of m. The plot provides the following information regarding this kind of attack.

If $D = 1$, then this is like the scan attack discussed earlier. If D is greater than 1, then the intruder can increase the probability of success by implementing a dictionary attack.

The probability of a successful attack depends on the size of the dictionary and the number of trials conducted by the intruder.

The intruder would try to divide the m trials between building the dictionary using D trials and triggering the vehicle using m-D trials in such a way that $p(m, D)$ becomes maximum.

After doing some mathematical analysis, one can show that the value of $p(m, D)$ will be maximum if $D \cong m/2$. The Appendix shows the proof. Therefore, altogether if the intruder wants to spend m trials, then in order to have a maximum success rate in his attack, he has to spend $m/2$ trials to build the dictionary and the remaining $m/2$ trials to trigger the vehicle system.

V. Improved Protocol Design for Keyless-Entry Systems of Vehicles

It would be difficult to design an ideal theft-proof vehicle at a reasonable cost. It also is not desirable to build a very complex and expensive security system for keyless vehicles, because the intruder then may choose to get into the vehicle just by

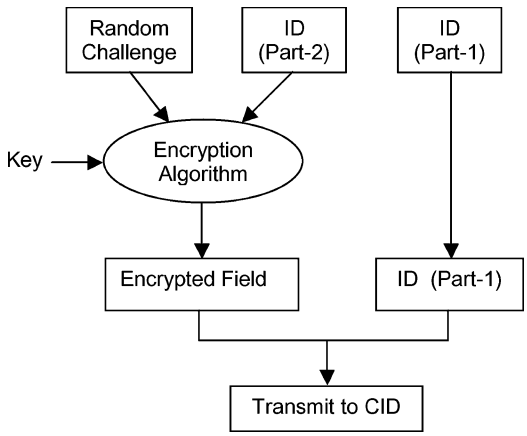

Fig. 6. Block diagram of the mechanism of the improved protocol.

breaking a window of the vehicle. In this section, we have proposed two simple solutions that can be implemented at a marginal cost. These simple solutions will significantly increase the odds against breaking the security of the keyless vehicle systems. It is obvious that a challenge–response technique gives better security than a rolling code technique. Thus, the simple suggestions that we are presenting here are for a system that uses a challenge–response technique.

A. First Suggestion for an Improved Protocol

Our first suggestion is made based on the idea that if the vehicle system detects that someone is pulling a door handle without sending a valid response, then the vehicle system should stop sending any more challenges for a while. This technique would prevent the intruder from implementing a successful scan attack in a short time. As a result, the odds against breaking the security of the vehicle using the scan attack will increase significantly. This technique will also prevent the intruder from soliciting many challenges out of the vehicle system in a given time. Thus, this technique will limit the intruder's ability to analyzing the challenges, do some kind of predictions, or figure out the encryption key implemented in the vehicle. As a result, it will be more difficult for an intruder to implement a successful challenge forward prediction attack or crypt-analysis attack. Discussion of the crypt-analysis attack is beyond the scope of this paper.

B. Second Suggestion for an Improved Protocol

In order to prevent the CID from responding to every challenge, the vehicle will send an identification (ID) with each challenge. The CID will first check if the ID matches with the one that is stored in its memory. If there is a match, then the CID will respond. Otherwise, the CID will not respond. To prevent an intruder from duplicating the ID from the vehicle's challenge, we can divide the ID into two parts: 1 and 2. Part1 of the ID will be sent in clear form (plain text), but part 2 will be sent in encrypted form along with the random challenge. Fig. 6 shows a block diagram of this technique. When the CID wakes up upon detecting the LF signal from the vehicle, it compares the clear part of the ID with the one that is stored in it. If there is a match, the CID will then decrypt the encrypted field. If the decrypted part of the ID matches the corresponding part stored in the CID, then the CID encrypts the challenge using a different key and sends it back to the vehicle. While the CID was computing the response, the vehicle was also calculating the expected response from the CID using the same encryption key used by the CID. When the vehicle receives the response from the CID, it compares the CID's response with the expected response. If all match, the vehicle then unlocks the doors.

C. Analysis of a Dictionary Attack With the Improved Protocol

For a system with an improved protocol, the intruder's job in building the dictionary is not as easy as it was for a system without an improved protocol. A CID without an improved protocol will respond to every challenge that the intruder would generate. However, a CID with an improved protocol will not respond to a challenge unless the challenge is from its own vehicle. Thus, in order to build a dictionary, first the intruder has to go to the vehicle to collect valid challenges by pulling a door handle a number of times. After that, the intruder can go close to the owner with the CID and play those challenges to collect responses. The intruder will save every response with the corresponding challenge to build his dictionary. The intruder will then go to the vehicle again to trigger the vehicle by pulling a door handle. The intruder will be pulling a door handle with the hope that one of the challenges from the vehicle would match a challenge that is already available in his dictionary. If there is a match, then the intruder will be successful in his dictionary attack.

This type of dictionary attack can be prevented if the random challenge, generated by the vehicle, is cyclic and the system is designed according to the suggestions presented in this section of this paper. If the bit-random challenge is cyclic, then a given challenge will not be generated again until all challenges are generated. Hence, if $= 16$, then a given challenge will repeat after generating 65 536 challenges. If the vehicle were designed using our first suggestion, in such a way that on an average the vehicle will not generate more than five challenges in every 8 s, then the vehicle would take 29.13 h to repeat a challenge. Thus, no matter how the intruder is going to build his dictionary, the total time (including building the dictionary) required by the intruder to implement a successful dictionary attack will be at least 29.13 h. Adding a few extra bits in the random challenge can significantly increase the time required to implement a successful attack. Hence, for all practical purposes, the intruder cannot be successful by implementing a dictionary attack.

VI. Summary of All Attacks

In this section, we have summarized all the attacks for the convenience of the readers. By looking at this summary, a reader can easily compare many features of different attacks such as the following:

- how vulnerable a system is going to be due to an attack;
- what type of devices an intruder needs in order to implement the attack;
- whether any mathematical analysis is needed by the intruder;
- how difficult the attack is going to be from the intruder's point of view.

The following list shows different types of tools that an intruder may need in order to implement the attacks.

TABLE I
TOOLS NEEDED FOR DIFFERENT TYPES OF ATTACKS

Type of Attacks	Tools Needed						
	Transmitter	Receiver	Recorder	Storage & Controller	Signal Analyzer	Mathematician	Others
Scan	Yes	No	No	No	No	No	No
Playback	Yes	Yes	Yes	No	No	No	No
Forward Prediction	Yes	Yes	Yes	No	Yes	Yes	No
Dictionary	Yes	Yes	Yes	Yes	Yes	No	No
Relay (*Two-Thief Attack*)	Yes	Yes	No	No	No	No	Yes

TABLE II
DIFFICULTY OF ATTACKS VERSUS TYPE OF TECHNIQUES USED IN KEYLESS-ENTRY SYSTEMS FOR VEHICLES

	Fixed Code	Rolling Code	Challenge-Response	Our Protocol
Scan	Hard	Hard	Very Hard	Extremely Hard
Playback	Easy	Hard	Very Hard	Extremely Hard
Forward Prediction	Easy	Hard	Very Hard	Extremely Hard
Dictionary	Easy	Medium	Hard	Extremely Hard
Relay (*Two-Thief Attack*)	Easy	Easy	Easy	Easy

A. List of Tools

- Transmitter: capability to transmit signals.
- Receiver: capability to receive signals.
- Recorder: capability to record a received signal.
- Signal analyzer: capability to understand the content of a received or recorded signal.
- Storage and Controller: capability to decode, store, compare, and control decoded signals.
- Mathematician: person with a strong mathematical background.
- Others: custom specific tools that are expensive to build.

Table I shows the list of tools needed by an intruder to implement different types of attacks. This table shows that forward prediction and dictionary attacks need more tools from the intruders than any other attacks.

Table II compares the difficulty of implementing different attacks versus the type of techniques used in keyless-entry systems for vehicles. The difficulty of implementing different attacks is shown in a scale that contains five values such as easy, medium, hard, very hard and extremely hard. Table II shows that the relay attack is the only attack that the intruders can easily implement against the keyless-entry system of vehicles regardless of the type of technique used to authenticate the CID by the vehicle. This table shows that the fixed code technique is easy to break using all types of attacks except the scan attack. The rolling code technique is harder to break compared to the fixed code technique using all types of attacks except the relay attack. Other than the relay attack, the dictionary attack is the next vulnerable attack against a system that uses the rolling code technique to authenticate the CID. The challenge–response technique is the next robust technique after the fixed and rolling code techniques. Table II also shows that, if the system is designed by incorporating our suggestions, then it will be extremely hard for the intruders to break the security of the system using all types of attacks except the relay attack.

Two or more intruders are necessary to implement a relay attack. In this type of attack, the intruders try to build an electronic bridge between the vehicle and the CID. In [17], we provided a solution for the well-known two-thief relay attack problem. In the same paper, we also provided a solution for an attack, which can be implemented by three thieves. To prevent the relay attack by three thieves, the CID has to transmit its messages using two different power levels and the difference between the two power levels must be higher than a threshold value. From our work [17], it is clear that if a system is protected from the three-thief attack, then it is also protected from any relay attack that can be implemented by more than three thieves. Thus, if the solutions presented in [17] and the suggestions proposed in this paper are used to design a system, then breaking the security of the system by the thieves will be extremely hard, if not impossible.

VII. CONCLUSION

This paper described various types of security attacks against keyless-entry systems of vehicles and compared the attacks in terms of the vulnerability of the system, level of difficulty to implement the attacks, and equipment needed for the attacks. This paper will help those people who have started working on or are going to work toward the design of keyless-entry systems for vehicles. It will provide the designers with a tutorial type of materials and will provide designers with the understanding of the complexity of different attacks; it also will provide the designers with some ideas of how to make the passive vehicles more secure. This paper is self-contained; thus, it will directly benefit many people in terms of saving the time and effort that would be required from them to collect the information presented in this paper by reading many published papers.

APPENDIX

Lemma A1: Assume that the size of the total challenge space is T. If an intruder wants to use a total of m trials ($m \ll T$) to build a dictionary of size D, and then trigger the vehicle using m-D trials, then the probability of a successful attack $p(m, D)$ will be maximum if $D \cong m/2$.

Proof: The probability of a successful dictionary attack can be expressed as

$$p(m, D) = 1 - \left(\frac{T - D}{T}\right)^{m-D}. \tag{19}$$

The value of $p(D)$ will be maximum if the value of $(T - D/T)^{m-D}$ is minimum.

Let

$$y = \left(\frac{T - D}{T}\right)^{m-D}. \tag{20}$$

We want to find a value of D such that $dy/dD = 0$. By taking the natural logarithm of both sides of (20), we get

$$\ln(y) = (m - D)\ln\left(\frac{T - D}{T}\right). \tag{21}$$

Differentiating both sides of (21), we get

$$\frac{dy}{dD}\left(\frac{1}{y}\right) = -\ln\left(\frac{T - D}{T}\right) + \frac{m - D}{D - T}. \tag{22}$$

Then

$$\begin{aligned}\frac{dy}{dD} &= \left[-\ln\left(\frac{T - D}{T}\right) + \frac{m - D}{D - T}\right] y \\ &= \left[-\ln\left(\frac{T - D}{T}\right) + \frac{m - D}{D - T}\right]\left(\frac{T - D}{T}\right)^{m-D}. \end{aligned} \tag{23}$$

Equating $dy/dD = 0$ leads to

$$\ln\left(\frac{T - D}{T}\right) = \frac{m - D}{D - T}. \tag{24}$$

By expanding the left side of (24) around $D = 0$ into its Taylor series we get

$$\ln\left(\frac{T-D}{T}\right) = -\frac{D}{T} - \frac{1}{2}\left(\frac{D}{T}\right)^2 - \frac{1}{3}\left(\frac{D}{T}\right)^3 - \frac{1}{4}\left(\frac{D}{T}\right)^4 - \cdots. \tag{25}$$

Since $m \ll T$, we can write $D \ll T$. Hence, the second, third, etc. terms of (25) can be ignored. As a result, (25) reduces to

$$\ln\left(\frac{T - D}{T}\right) \cong \frac{-D}{T}. \tag{26}$$

Now, using (24) and (26), we get

$$\frac{-D}{T} = \frac{m - D}{D - T}. \tag{27}$$

Solving for D, we can write

$$D = T \pm \sqrt{T^2 - Tm}. \tag{28}$$

The root $D = T + \sqrt{T^2 - Tm}$ violates the assumption $D \ll T$. Thus, we do not accept this root as a solution. The other root $D = T - \sqrt{T^2 - Tm}$ can be expanded into its Taylor series as

$$D = T - \left(T - \frac{m}{2} - \frac{1}{8}\left(\frac{m}{T}\right)^2 - \frac{1}{16}\left(\frac{m}{T}\right)^3 - \cdots\right). \tag{29}$$

Since $m \ll T$, the second, third, etc. terms can be ignored. Thus, we get

$$D \cong \frac{m}{2}. \tag{30}$$

Hence, Lemma A1 is proved.

REFERENCES

[1] D. Smith, "Passive keyless entry, latest from Lectron," in *Ward's Auto World*. Overland Park, KS: Intertec, 1993, p. 111.

[2] T. Waraksa, K. Farley, R. Kiefer, D. Douglas, and L. Gilbert, "Passive keyless entry system," U.S. Patent 4 942 393, Jul. 1990.

[3] ——, "Passive keyless entry system," U.S. Patent 5 319 364, Jun. 1994.

[4] W. Diem, "Smart card opens the door," *AutoTechnol.*, pp. 32–33, 2001.

[5] E. Mayne, "Genetic re-engineering," in *Ward's AutoWorld*. Overland Park, KS: Intertec, 2001, pp. 34–35.

[6] A. Wielgat, "What's the frequency? suppliers seek new applications for RF technology," in *Automotive Industries*. Tuscaloosa, AL: Randall, 2001.

[7] K. Nakano and M. Takeuchi, "Automotive keyless entry system incorporating portable radio self-identification code signal transmitter," U.S. Patent 4 794 268, Dec. 1988.

[8] K. Marneweck, *An Introduction to Keeloq Code Hopping*. Chandler, AZ: TB003 Applicat. Notes, Microchip Technol., Inc., 1996.

[9] "Microchip Inc., Data sheet for HCS300," in *KeeLoq Code Hopping Encoder*. Chandler, AZ: Microchip Technol., Inc., 2000.

[10] J. Gordon, U. Kaiser, and T. Sabetti, "A low cost transponder for high security vehicle immobilizers," in *Proc. ISATA'96*, Florence, Italy, 1996, 96AE001.

[11] J. Gordon, *Designing Codes for Vehicle Remote Security Systems*. Herfordshire: Concept Laboratories Ltd. and Police Science Develop. Branch, 1994, ch. U.K., pp. 1–22.

[12] "Microchip Inc., data sheet for HCS412," in *KeeLoq Code Hopping Encoder and Transponder*. Chandler, AZ: Microchip Technol., Inc., 2000.

[13] D. Juzswik, "Evolving automotive access systems," in *Proc. 4th Int. Conf. Vehicle Electronic System*, Coventry, U.K., Jun. 2001, pp. 8.2.1–8.2.7.

[14] S. Schmitz, J. Kruppa, P. Crowhurst, T. Oexle, and W. Ulke, "New door closure concept," *SAE Automot. Eng. Int.*, vol. 108, no. 9, pp. 118–120, Sep. 2000.

[15] B. Schneier, *Applied Cryptography*. New York: Wiley, 1994.

[16] H. Krawczyk, "How to predict congruential generators," in *Advances in Cryptology-CRYPTO 89*. New York: Springer-Verlag, 1990, vol. 435, Lecture Notes Comp. Sci., pp. 138–153.

[17] A. I. Alrabady and S. M. Mahmud, "Some attacks against vehicles' passive entry security systems and their solutions," *IEEE Trans. Veh. Technol.*, vol. 52, no. 2, pp. 431–439, Mar. 2003.

Ansaf Ibrahem Alrabady received the B.S. degree in electrical and computer engineering from Jordan University of Science and Technology (JUST), Jordan, in 1990 and the M.S. and Ph.D. degrees in computer engineering from Wayne State University (WSU), Detroit, MI, in 1992 and 2002, respectively.

He has published several papers and holds several patents in automotive electronics related products. His main research interests are related to vehicle security, communication protocols, and access control.

Dr. Alrabady received the Automotive Hall of Fame Young Leadership and Excellence Award for his contributions to the automotive industry in 2001.

Syed Masud Mahmud (S'82–M'84) received the Ph.D. degree in electrical engineering from the University of Washington, Seattle.

Since 1988, he has been with Wayne State University, Detroit, MI, where he currently is an Associate Professor in the Electrical and Computer Engineering Department. Over the last 15 years, he has been working in the areas of hierarchical multiprocessors, hierarchical networks, performance analysis of computer systems, digital signal processing, embedded systems, invehicle networking, performance analysis of networking protocols, secure wireless communications, and simulation techniques. He has supervised a number of projects from Ford Motor Company and other local companies. He has published approximately 70 peer-reviewed journal and conference proceeding papers.

Dr. Mahmud received the President's Teaching Excellence Award from Wayne State University in 2002. He also received several other teaching excellence awards within the college of engineering. He has served as a technical reviewer for many conferences, journals, and funding agencies. He has been listed in *Who's Who in Science and Engineering, Empowering Executives and Professionals* and many others.