Security of Wireless Networks in Intelligent Vehicle Systems

Syed M. Mahmud and Shobhit Shanker
Electrical and Computer Engg. Dept.
Wayne State University
Detroit, MI 48202

Email: smahmud@eng.wayne.edu
Phone: (313) 577-3855

Webpage: http://www.ece.eng.wayne.edu/~smahmud

Outline of the Presentation

- Why wireless communications ?
- Applications of wireless communications in Intelligent Vehicles.
- Problems with wireless communications.
- Our solution for an in-vehicle wireless network.

Why wireless communications ?

- Because, no cables or wires are necessary.
- It's the only way, two vehicles can talk to each other when they are moving.
- Occupants of a vehicle can easily access internet through wireless enabled Laptops and PDAs from anywhere within the vehicle.
- The driver of a vehicle can easily make phone calls and control other items inside a vehicle, through a ***wireless enabled headset*** and ***voice activated devices***.

Applications of wireless communications in Intelligent Vehicles.

1. **Personal Wireless Networks within a vehicle.** ***(Internet access, fax service, phone calls using Bluetooth enabled headsets, etc.)***
2. **Inter-Vehicle Wireless Networks for exchanging Vehicles' dynamic information.** ***(Speed, acceleration, position, direction, etc.)***
3. **Wireless Networks for accessing information from the infrastructure of intelligent highways and freeways.** ***(Road condition, lane detection, speed limit, local information about hotel/motel, weather, etc.)***

Need For Inter-Vehicle Wireless Communication Links

- To exchange vehicles' dynamic information, which is necessary in order to build *Collision Warning*, *Collision Avoidance* and *Cooperative Driving* systems

No Wireless System Will Work Properly Unless it is Secured

- If a wireless system is not secured, then it is vulnerable to many types of attacks from the hackers, such as:
  - ***Eavesdropping***: Someone could record a sensitive conversation, or intercept classified information.
  - ***Tampering***: Information in transit is changed or replaced and then sent to the recipient.
  - ***Impersonation***: Information passes to a person who poses as the intended recipient.

Why Do We Need Security for Intelligent Vehicle Networks ?

- To protect personal information, such as fax, computer files, credit card numbers, etc.
- To protect inter-vehicle messages from tampering by hackers.

A Bluetooth Enabled Vehicle

- General Motor Corporation introduced a Wireless Personal Area Network (WPAN) in its 2003 Saab 9-3 model car using the Bluetooth technology.
- In future, other companies may come up with similar networks for a vehicle.
- But, the security of a Bluetooth system is very weak.
- Thus, we tried to come up with a technique to protect the WPAN of a vehicle.

Contribution of Our Paper

- **The main contribution of our paper is the development of a security technique for the *Wireless Personal Area Network* (WPAN) within a vehicle.**

BLUETOOTH SECURITY

- **Four different entities are used for maintaining security at the Bluetooth Link Layer: a *public address* which is unique for each Bluetooth device , *two secret keys*, and a *random number* which is different for each new transaction.**

Entity	Size
BD_ADDR	48 bits
Private user key, authentication	128 bits
Private user key, encryption configurable length (byte-wise)	8-128 bits
RAND	128 bits

48-Bit Bluetooth Address

- The Bluetooth device address (BD_ADDR) is a 48-bit number which is unique for each Bluetooth unit.
- The Bluetooth addresses are publicly known, and can be obtained automatically, via an inquiry process by a Bluetooth Unit.

Authentication Key and Encryption Key

- The secret keys are derived during initialization and are further never disclosed.
- The *encryption key* is derived from the *authentication key* during the authentication process.
- Each time encryption is activated, a new encryption key is generated.
- The authentication key will be more static- once established, the particular application running on the Bluetooth device decides when, or if, to change it.

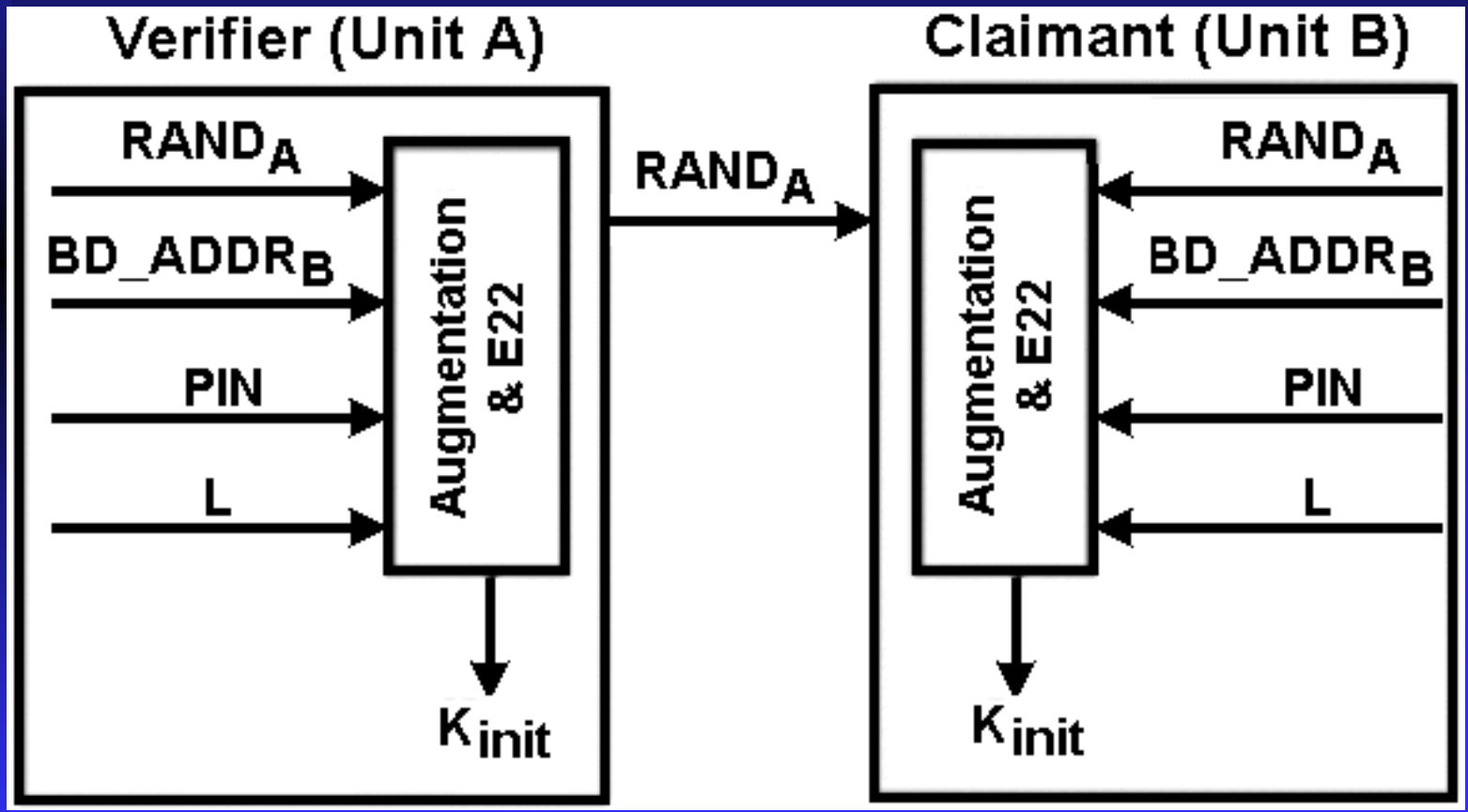
Link Key

- The authentication key is also known as the ***Link Key***.
- In order to accommodate for different types of applications, four types of link keys have been defined:
  - the combination key K_{AB}
  - the unit key K_A
  - the temporary key K_{master}
  - the initialization key K_{init}

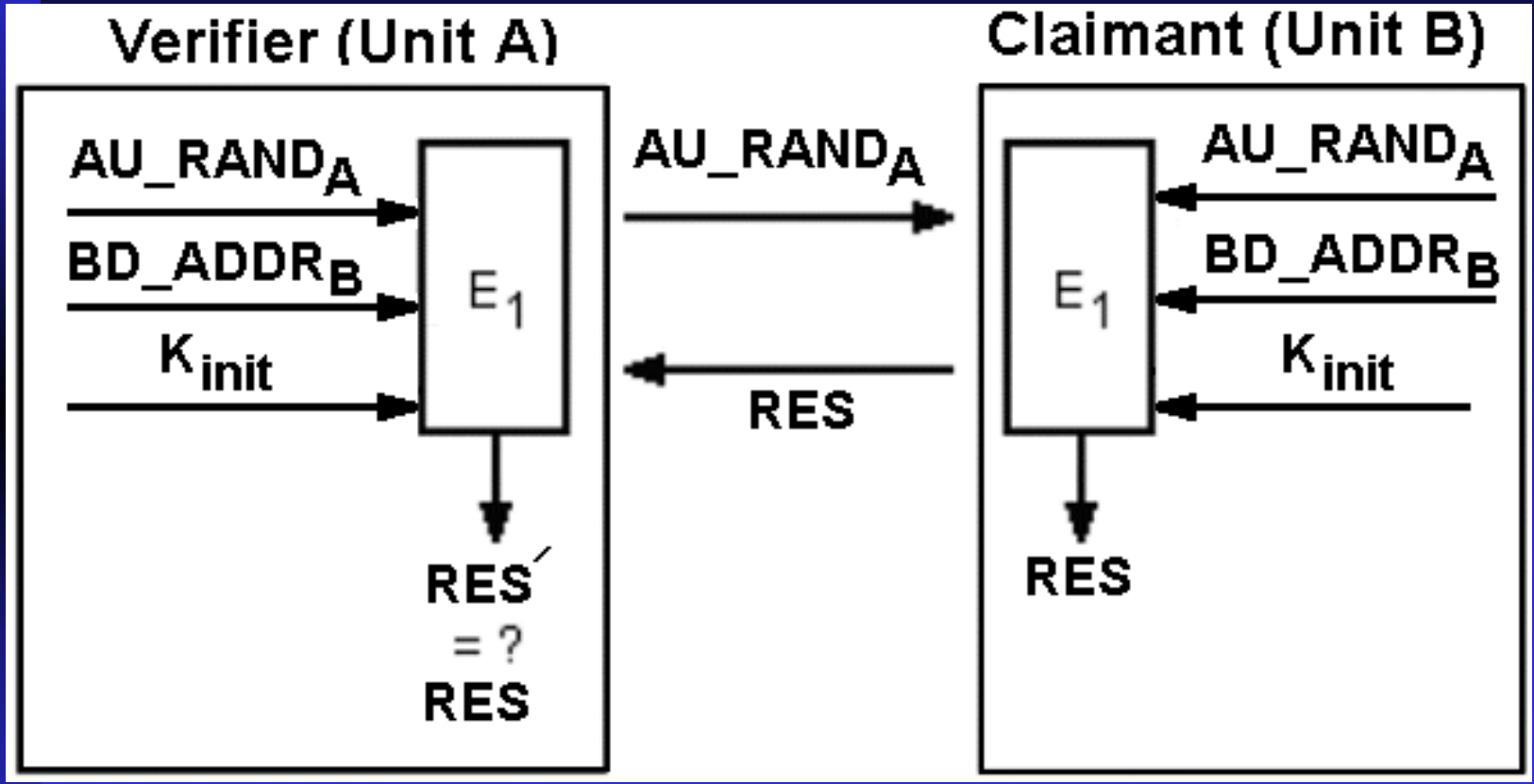
Initialization Key

- The initialization key, K_{init}, is used as the *link key* during the initialization process when no combination or unit keys have been defined and exchanged yet or when a link key has been lost.
- It is derived from four entities: the Bluetooth address BD_ADDR_B of the claimant unit, a PIN code, the length of the PIN (L), and a random number $RAND_A$ issued (and created) by the verifier

Generation of the Initialization Key when Unit B wants to establish a connection with Unit A



Unit A is Authenticating Unit B



The PIN is the Cause of Security Problems in a Bluetooth System

- The PIN is a 4-digit number (0000 – 9999).
- For two Bluetooth devices to form an ad-hoc network (automatically), the PINs of the two devices must be same.
- In 50% of the devices it is always 0000, so that they can automatically form an ad-hoc network when they come close to each other.

The Problem with a 4-Digit PIN

- Since the PIN is a 4-digit number, the hackers may be able to get it using a *Brute Force* attack.
- If a user is required to manually enter a PIN, every time the user is going to use a Bluetooth device for a certain application, then it won't be convenient for the user if the PIN is very long.
- As a result, the security threat still remains in Bluetooth devices.

How to Build a Secured In-Vehicle Wireless Network ?

1. Make the PIN a *very large number* so that it can't be easily obtained through a *Brute Force* attack.
2. Make the PIN *transparent* to the user so that the user doesn't have to remember it.
3. *Change* the PIN from time to time so that it can't be obtained by analyzing data recorded over a period of several communication sessions.

How to Build a Secured In-Vehicle Wireless Network (contd.) ?

4. Use different PINs for different in-vehicle devices (e.g. laptop, PDA, cell phone, etc.) so that PINs of other devices can't be obtained from a stolen device.
5. Don't allow two in-vehicle devices to start a communication without being authenticated by a *Gate-Way* device.
6. Register all devices (to be used in the vehicle) to the Gate-Way device, so that the Gate-Way device can know who is allowed to participate in a secured communication.

How to Build a Secured In-Vehicle Wireless Network (contd.) ?

7. The user should be able to *remove* a stolen device from the list of registered devices, maintained in the Gate-Way device.

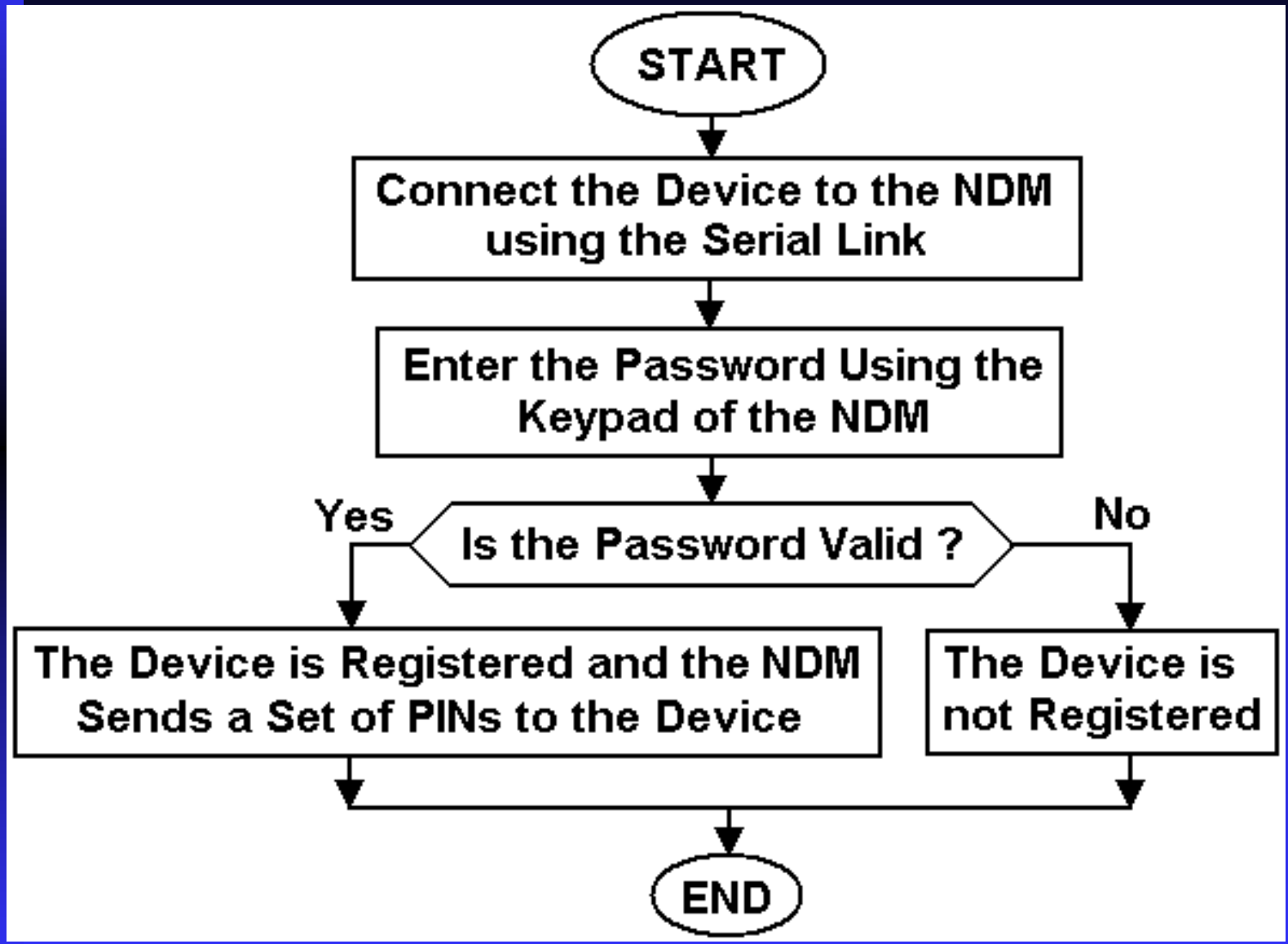
Our Solution for an In-Vehicle Wireless Network

- We proposed to have a device, called the *Network Device Monitor* (NDM).
- The NDM is the Gate-Way device.
- The NDM can be installed in the dashboard of the vehicle.
- The NDM should be equipped with a keypad or another type of interface in order to enter a password by the users of the vehicle.

Our Solution for an In-Vehicle Wireless Network (contd.)

- The NDM and each Bluetooth device, to be used in the vehicle, should have either a wired or infrared serial link interface.
- Every device, to be used in the vehicle, must be registered to the NDM via the serial link and a password protected user interface (e.g. a keypad).
- The device will be registered only once during its life time.

Registering a Device



The Set of PINs

- The NDM also keeps the set of PINs that was sent to a device during the registration process.
- Let the set of PINs be PIN_1, PIN_2, . . . PIN_k. Where, k >= 1.
- The following figure shows the contents of NDM's and Device1's memory (for k=2) after Device1 is registered.

NDM's Memory		
DEVICE	PIN_1	PIN_2
Device1	24..4	31..0
Device2		
Device3		
Device4		

Device1's Mem.	
PIN_1	PIN_2
24..4	31..0

Memory of NDM and Four Devices

- The following figure shows the memory contents of the NDM and four devices after the devices are registered.

NDM's Memory		
DEVICE	PIN_1	PIN_2
Device1	24..4	31..0
Device2	30..5	41..9
Device3	44..6	37..5
Device4	53..5	41..8

Device1's Mem.	
PIN_1	PIN_2
24..4	31..0

Device2's Mem.	
PIN_1	PIN_2
30..5	41..9

Device3's Mem.	
PIN_1	PIN_2
44..6	37..5

Device4's Mem.	
PIN_1	PIN_2
53..5	41..8

Authenticating a Device by the NDM

- Every time a device wants to participate in a secured in-vehicle communication, first the device must be authenticated by the NDM.
- If it is the i^{th} session of the device after it received the last set of PINs from the NDM, then the device and the NDM will use PIN_i for the authentication process.

An Example of Authenticating Device1 by the NDM for the First Time

PIN 24..4 is used when Device1 participates for the first time.

NDM's Memory		
DEVICE	PIN_1	PIN_2
Device1	~~24..4~~	31..0
Device2	30..5	41..9
Device3	44..6	37..5
Device4	53..5	41..8

Device1's Mem.	
PIN_1	PIN_2
~~24..4~~	31..0

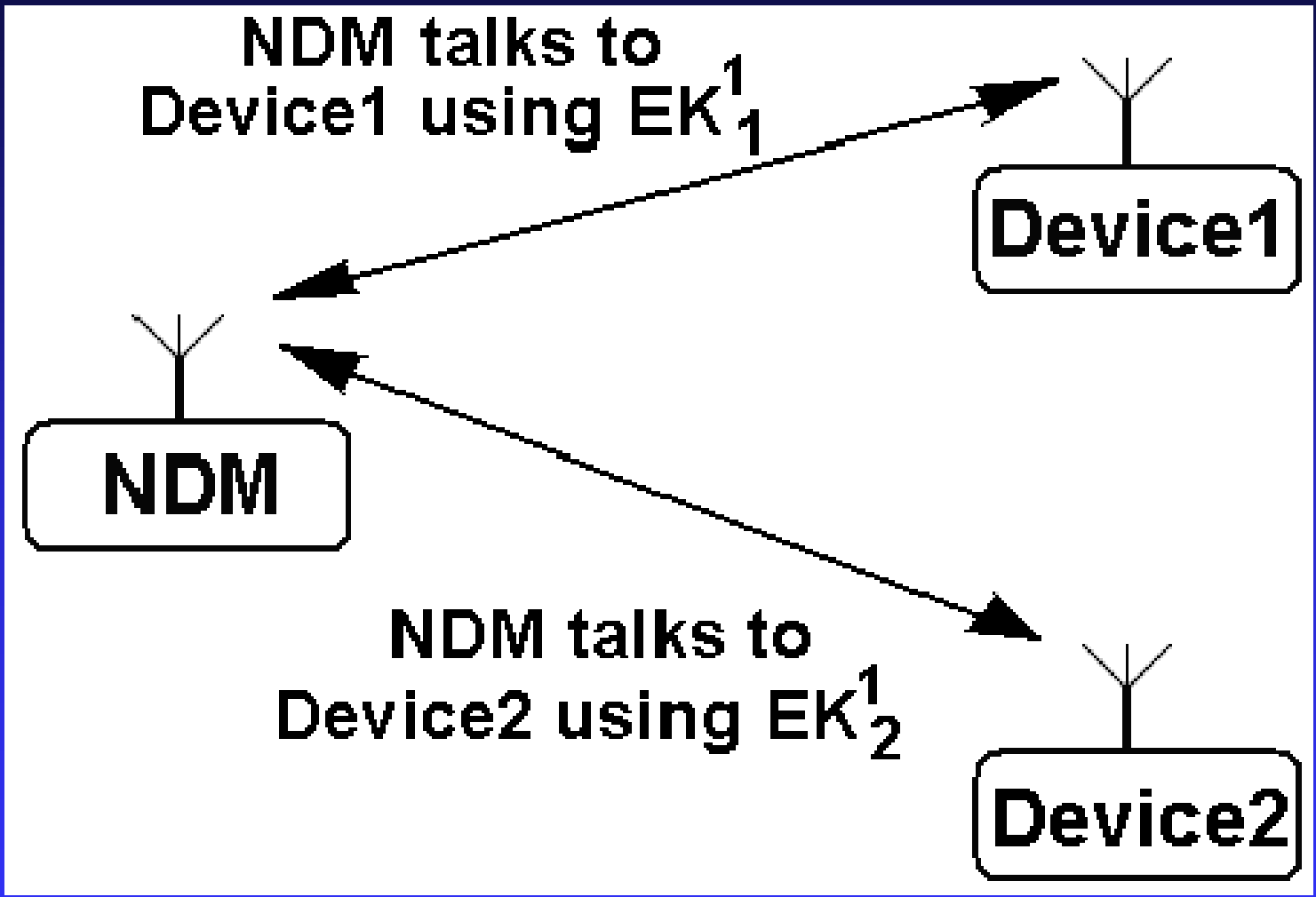
Encryption Key for Device1 and the NDM

- Both the NDM and Device1 will use the first PIN (24..4) to generate an *Encryption Key* **(EK^1_1)** using the Bluetooth algorithms.
- This Encryption Key will then be used by the NDM and Device1 to exchange all messages between them.
- Syntax of an Encryption Key : **Ek^i_n** (n = device number, i = session number).

Communication Between the NDM and Device2

- If Device2 also wants to start a communication, the NDM and Device 2 will use the first PIN **(30..5)** of Device2 in exactly the same way as the NDM and Device1 did.
- The NDM and Device2 will generate another Encryption Key **(EK^1_2),** based on the PIN 30..5, to securely transfer messages between them.

Communication Between the NDM and two devices



Forming a Secured Network

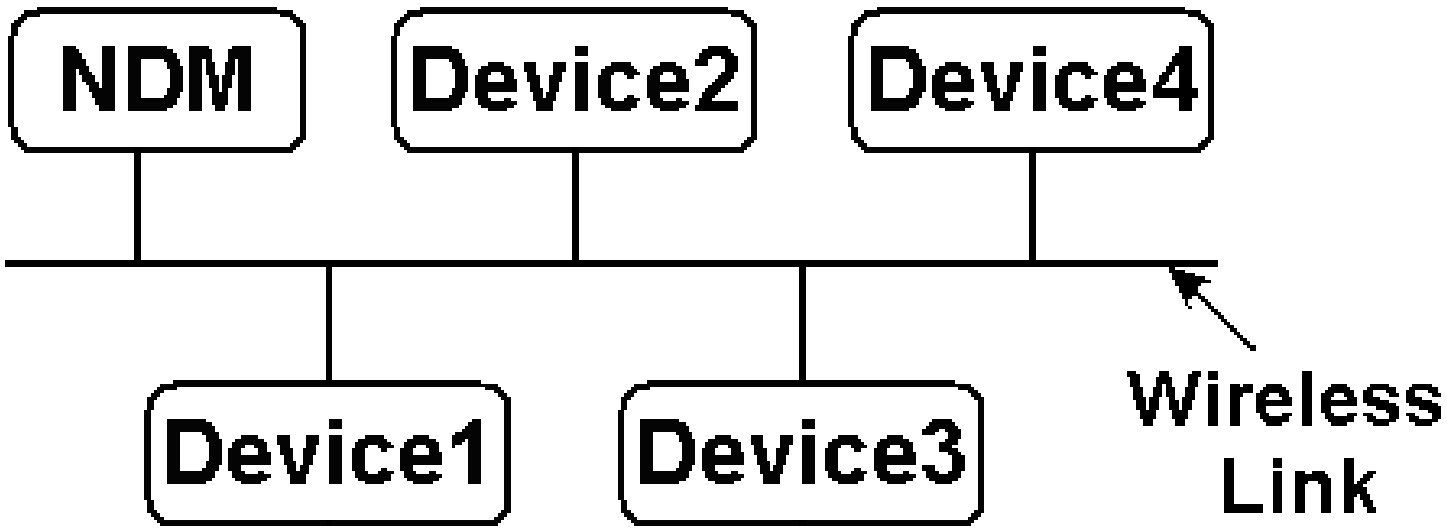
- When the NDM talks to Device1 using the encryption key EK^1_1, no other devices can understand that conversion.
- Similarly, when the NDM talks to Device2 using the encryption key EK^1_2, no other devices can understand that conversion.
- If all devices and the NDM want to form a *Secured Network*, then another encryption key, called the *Session Key*, is necessary.

Session Key

- The session key will be created by the NDM.
- This session key will then be sent to all the devices using the encryption keys of the corresponding devices.
- For example, the session key will be sent to Device1 after encrypting it using EK^1_1.
- Similarly, the session key will be sent to Device2 after encrypting it using EK^1_2.
- Once all the devices received the session key, they can talk among themselves by encrypting messages using the session key.

A Secured Wireless Network

The NDM and all the devices exchange messages among themselves using the SESSION KEY



The Life of a Session Key

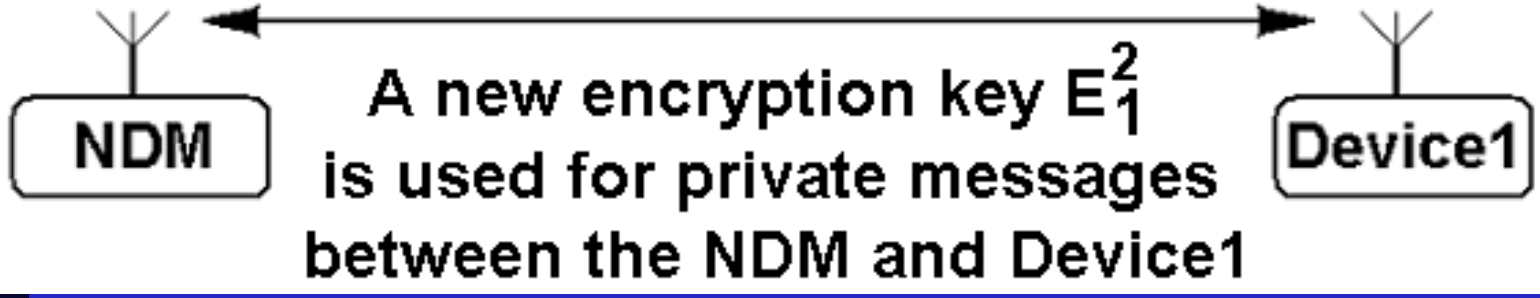
- The maximum length of the life of a session key is the length of the current session.
- However, the NDM may decide to change the session key from time to time if the length of the session is too long.
- A new session key will be distributed to all active devices using the devices own encryption keys.
- Every new session will always start with a new session key.

Leaving and Reentering a Secured Network

- A device can leave a secured network at any time.
- If the device wants to come back and join another session of the network at a later time, then the device must be authenticated by the NDM again.
- This time, the device will be authenticated using the second PIN of the device.
- The NDM and the device will use a new encryption key, derived from the second PIN, to talk to each other.

Device1 Comes Back and Participates for the Second Time in a New Session

PIN 31..0 is used when Device1 participates for the second time



NDM's Memory		
DEVICE	PIN_1	PIN_2
Device1	~~24..4~~	~~31..0~~
Device2	~~30..5~~	41..9
Device3	~~44..6~~	37..5
Device4	~~53..5~~	41..8

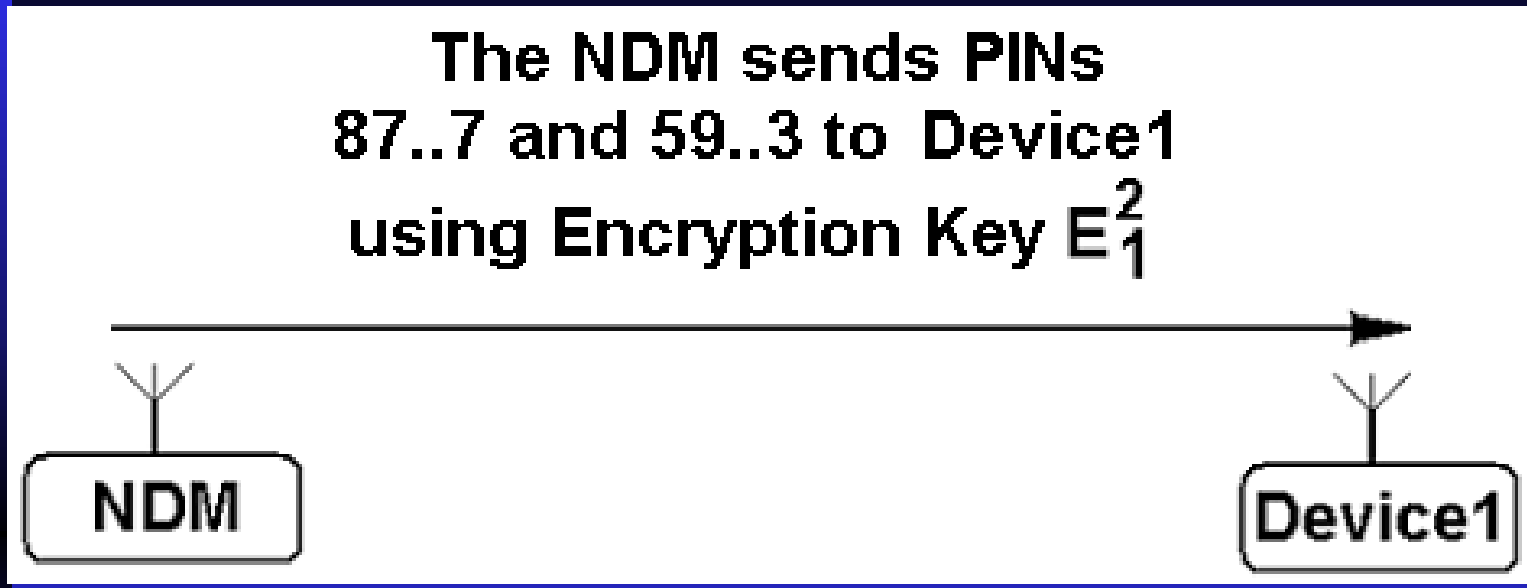
Device1's Mem.	
PIN_1	PIN_2
~~24..4~~	~~31..0~~

Device1 Needs Another Set of PINs

- Both PINs of Device1 have been used.
- Thus, Device1 needs another set of PINs to come back and join a future session.
- During the second session of Device1, the NDM will send another set of two PINs (k=2) to Device1.
- There after, the NDM will send a set of two PINs after every 2 (k=2) sessions.

Device1's Mem.	
PIN_1	PIN_2
~~24..4~~	~~31..0~~

Transmission of a New Set of PINs



NDM's Memory		
DEVICE	PIN_1	PIN_2
Device1	87..7	59..3
Device2	~~30..5~~	41..9
Device3	~~44..6~~	37..5
Device4	~~53..5~~	41..8

Device1's Mem.	
PIN_1	PIN_2
87..7	59..3

Disadvantages of Our Technique

- The NDM must have enough memory to keep all the PINs of all the devices.
- In a standard Bluetooth device, the previously used Link Key is used for successive authentications, but in our technique a new link key is generated using a new PIN for every new session. This may take little bit extra time to get connected to the NDM.
- If the NDM becomes faulty, then no device will be able to communicate with any other devices.
- The built-in algorithms of Bluetooth devices may need to be changed (slightly) in order to implement our technique.
- The above disadvantages are the price that we have to pay in order to obtain security.

Advantages of Our Technique

- Since the PINs of a device are known only to the NDM and the device itself, it is very secured.
- Since the PIN is very long, it is not vulnerable to the *Brute Force* attack.
- Since the PIN is secured, the encryption key (generated based on the PIN) of a device is also secured.
- The Session Key is sent in encrypted form.
- Thus, unlike the *Diffie-Hellman* key exchange algorithm, the exchange of our session key is not vulnerable to the *Man-in-the-Middle* attack.
- Since the system is not complicated, compared to the standard Bluetooth devices, it can be implemented at a low cost.

Future Work

- Currently, we are developing techniques to implement secured inter-vehicle wireless links.
- Secured inter-vehicle wireless links are necessary to develop *collision warning*, *collision avoidance* and *cooperative driving* systems.
- Hopefully, next year we will be able to present our work related to inter-vehicle networks.

ANY QUESTIONS ?