Validation Logic through Turn around Time for Collusion Attack In Wireless Sensor Environment

[1]Christy Grace M A, [2]Jebasheela A,
[1]PG Student, [2]Assistant Professor
[1]Computer Science And Engineering
[1]DMI College Of Engineering,Chennai,India

***Abstract* - The wireless sensor environment is used for performing secure communication between the sender and the receiver through wireless medium over long distance. The wireless medium should be kept highly secure, because if there is any leakage in information or informations could be hacked by any unauthorized person then the system could become corrupted. For proper communication the users have to authenticate himself with the other user he is going to communicate. After authentication, the actual messages are encrypted using the encryption algorithm. The user at the other end can view this message by decrypting it. Usually the text is encrypted and decrypted. But in this paper we use a technique called METAR. This technique is used for communication in wireless environment which helps to transfer details about cloud base height, temperature, latitude and its longitude of aircraft which helps in safe landing of aircraft.**

***Key Terms* - METAR, nounce, EDNLib , cipher block rivest algorithm, prover , verifier**

I.Introduction:

The wireless sensor environment is implemented using the vehicular adhoc network technology. The wireless environment helps the users to communicate each other by sending and receiving messages. The first process to be done is authentication. The sender takes the initiative to perform authentication.

Sender first sends an nounce using a one-way function , the receiver receives the nounce and sends another nounce to the sender as a reply. The nounce is nothing but the pseudo random number. The sender calculates the time taken for sending and receiving messages between them. The distance is also measured between user's [2]. Frequency of nounce exchanging is calculated using the below given formula,

Min (Tnounce)=$\frac{dv+2dr}{vt}$

vt- The speed of sending nounce between user's
dr– Transmission range
dv– Distance between the sender and receiver

Sender confirms authentication by obtaining quick response from the receiver. Finally authentication is done successfully [5]. Then the sender starts sending message to the receiver. The messages cannot be sent directly to the receiver. Because the messages can be easily hacked while transferring from one place to another. So the only solution to prevent hacking is encrypting the messages. The encryption can be performed using any of the encryption algorithms.

A technique called METAR is used. The METAR is a technique where the aero plane information is recorded manually by the user. The information such as source port from which the aircraft is belonged to, prescribed maximum altimeter(to which level of the sky it could fly),day of month(day in which the aircraft was started to use),start time(the time at which the aircraft is started to take off),temperature(maximum temperature at which aircraft travel),calculates the wind direction, calculates the gusting(pressure of the wind),calculates the knots(speed of the wind),calculates cloud visibility(the clarity of the cloud is found so that the aircraft could penetrate into it while passing through it).

The data sets are created for each type of aircraft and recorded. Then the data sets are invoked. After invoking, the aero plane signals are generated for the information which is recorded by the user. The encryption and decryption is differentiated and shown as existing and proposed methodology. In the existing methodology, the sender takes the first signal which is generated in aero signal generator is taken as the input from the wireless sensors. Then it is analyzed to know from which system the input has obtained. The information like MAC address of the system and the time at which user sent this message. Then finally the original aero-signal is encrypted using the cipher block rivest algorithm which replaces the signals with the special characters [10]. This replacement of special characters could be done by importing EDNLib function. The EDNLib function is already predefined with the aero plane information and the aero plane signals which has the corresponding encrypted text and decrypted text to be replaced randomly.

The receiver obtains this encrypted text. Extracts the MAC address and the timing from the encrypted text and convert it into original text using the cipher block rivest algorithm. The time is already fixed by the sender. Within the fixed time it has to be obtained by the receiver. The algorithm replaces the encrypted special characters with the original text by using the EDNLib function as it is already predefined. Finally the receiver gets the corresponding aero-signal of the aero plane sent by the sender location [11].

II. Encryption and Decryption Technique:

The purpose of using algorithm here is for encryption and decryption of text. But in this project we don't encrypt or decrypt a text, instead we encrypt and decrypt an aero-signal generated by an aero plane system. The specialty of this algorithm is to replace the aero-signals with some special characters. The could be done by using the EDNLib function. This function helps to replace the original text with some special characters by recognizing the input given, that is nothing but the manually recorded aero plane information. Already the aero plane information's are available in the EDNLib. If the manually recorded information is found in EDNLib it helps to generate aero plane signals for manually given input. The EDNLib also has the corresponding aero-signals for each aero plane information. For each aero-signal there is an encrypted text available in the EDNLib. If the manually given information matches the EDNLib, they fetch the corresponding encrypted text for that particular aero-signal.

A. Signal Encryption :

The sender takes the first signal which is generated in aero signal generator is taken as the input from the wireless sensors. Then it is analyzed to know from which system the input has obtained. The information like MAC address of the system and the time at which user sent this message. Then finally the original aero-signal is encrypted using the cipher block rivest algorithm which replaces the signals with the special characters. This replacement of special characters could be done by importing EDNLib function.

i) The rivest cipher engine is implemented
ii) The encryption key is generated in the rivest cipher engine
iii) Generated key string is validated.
iv) The aero-signal is encrypted by replacing the content available EDNLib.
v) The encrypted aero-signal is inserted.

B.Signal Decryption :

In the decryption process the receiver obtains this encrypted text. Extracts the MAC address and the timing from the encrypted text and convert it into original text using the cipher block rivest algorithm. The time is already fixed by the sender. Within the fixed time it has to be obtained by the receiver. The algorithm replaces the encrypted special characters with the original text by using the EDNLib function as it is already predefined. Finally the receiver gets the corresponding aero-signal of the aero plane sent by the sender location.

i) The string decrypt is performed in this step.
ii) The decryption is performed by replacing content available in EDNLib.
iii) New rivest cipher engine is created.
iv) Encryption key of encrypted string is obtained.
v) Using the replacing content and key the aero-signal is decrypted.
vi) In the receiver side time index is also decrypted along with MAC address of the sender.
vii) The time index includes system date, time such as hour,minute,second and millisecond. Everything is combined together using string merger and displayed together.

The encrypted string is taken to decrypt. It is replaced with the original characters using the EDNLib function. Then time index is obtained. It validates the time and MAC address sent by the sender. The timing is validated based on the moment, hour, minute, second and milli second. Each information is obtained individually from the system and merged together to be displayed to the receiver.

C. METAR Technique:

The METAR technique is processed by the sequence of steps given below:

1. Aero vehicular data construction
2. Encrypted code sent
3. Key response
4. Wireless response information
5. User validation and identification
6. Performance track

1. Aero vehicular data construction:

METAR is constructed to analyze the Weather report and cloud base height of air plane. These details or information is passed between verifier and Prover. METAR is Meteorological elements observed at an Airport at a specific time. Specific intervals between prover and verifier is also analyzed. Weather conditions, changes in surface wind these changes are passed as a information from prover to verifier in air force department. Prover verify the information of verifier using techniques involved in System.

2. Encrypted code sent:

Meteorological elements is encrypted by using cipher block Rivest algorithm. This encrypted text is more robust and secure when compared to other features involved in system. After Encryption, a verified text is sent to the other end user.

3.Key response:

Using cipher block Rivest algorithm an encrypted text is generated based on the source. The MAC content is extracted at the verifier side to approve the sender. And the content is decrypted on the receiver location.

4. Wireless response information:

If the user is valid the on extracting the MAC address, the receiver fixes the time for communication. This content is encrypted and given as response to sender.

5. User validation and identification:

The user validation and identification is performed in three steps.
i)validate the authentication information given by the user.
ii)extract the MAC address to validate the request origin.
iii)fix consecutive time for communication.

6. Performance track:

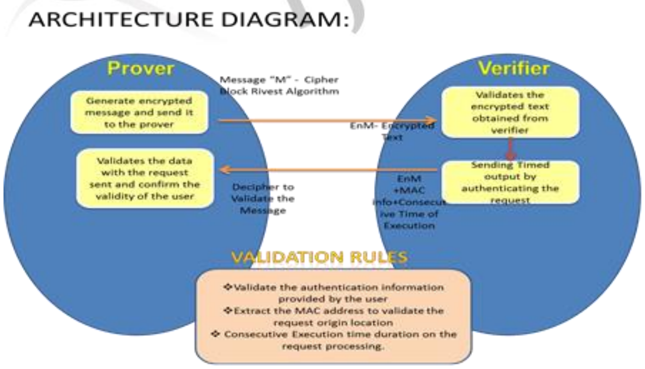
The performance is tracked based on how quick the information is sent between the users based on the fixed consecutive time duration.

III. Security Analysis:

The security analysis mainly focuses on the secrecy logic to extract the MAC address of the system and fix the consecutive time intervals for sending the messages to the receiver [4]. In the sender location the MAC address of the sender is recorded along with the time, sender fixes the encrypted text to be delivered to the receiver is recorded. After all these process gets over the encrypted aero-signal is forwarded to the receiver. In the receiver location receiver obtains the encrypted aero-signal, checks whether it's a valid MAC address to know whether sender is a valid user. If the receiver fails to receive the encrypted text within the fixed time then the text becomes invalid and could not be opened further. Then the encrypted aero-signal has to be sent again from the sender location. The consecutive time interval and MAC address is calculated in order to maintain secrecy. The unauthorized user also may try to send irrelevant content to the receiver. As the MAC address is extracted during authentication the frequent messages sent from a particular system is taken as it is obtained from an authenticated user. If the message is obtained from an irrelevant MAC address it is being omitted or not considered. This logic is being implemented using the technique called METAR. The METAR is a technique used to communicate secret information in an aircraft to discuss about the landing of aircraft; diversion of paths, in case of any failure's in aircraft how it could be handled and weather conditions etc. These information's are shared between an pilot and the commanding officer from the airport. As the distance communication could be performed only through the wireless system, this technique is being implemented. The authentication process is done so that it could be done in a highly secure manner. An hijacker could try to extract the aero-signals in between or send any irrelevant information and confuse the commander or the pilot. To avoid this only we use the validation rules to check the consistency of the authentication step.

IV. Performance Evaluation:

The performance is being evaluated by measuring its accuracy authenticating the users and forwarding the encrypted messages within the fixed time intervals. The architecture of the system is given below and it explains the performance of the METAR technique used.


ARCHITECTURE DIAGRAM:
Prover
Verifier
Generate encrypted message and send it to the prover
Message "M" - Cipher Block Rivest Algorithm
EnM- Encrypted Text
Validates the encrypted text obtained from verifier
Validates the data with the request sent and confirm the validity of the user
Decipher to Validate the Message
EnM +MAC info+Consecutive Time of Execution
Sending Timed output by authenticating the request
VALIDATION RULES
❖Validate the authentication information provided by the user
❖Extract the MAC address to validate the request origin location
❖ Consecutive Execution time duration on the request processing.

The performance evaluation checks how quick the generated. The messages are received by the receiver after checking all the security constraints. The prover encrypts the message using the cipher block rivest algorithm. The encryption process is performed using the EDNLib function which has predefined information about the aero-signals. When an corresponding information of an aircraft is recognized, it starts generating aero-signals for that particular aircraft for communication. The first generated signal is encrypted. As the EDNLib function has predefined information it synchronizes the aero-signal generated by the aircraft and replaces corresponding encrypted information for the generated aero-signal. Then the encrypted aero-signal is forwarded to the verifier. The verifier checks the obtained encrypted message by validating it. The validation process takes place in three steps. First receiver checks the authentication information provided by the prover. Further the receiver extracts the MAC address to validate the request origin location. This is done to ensure that the messages are obtained from a valid user. Finally receiver checks the consecutive time duration on request processing. This is done to ensure how quick the communication is preceded by sending and receiving messages between the prover and verifier. The unauthorized user could be avoided if proper authentication information is not provided. As the verifier could extract the MAC address if the unauthorized person try to interfere in-between by sending irrelevant messages unauthorized person could be rejected on identifying his MAC address. And if suppose the verifier was not conscious about extracting his MAC address unauthorized person could be identified by the final process that is the consecutive time duration on request processing. The unauthorized person does not know about the time intervals fixed by both the prover and verifier. Unauthorized person may send messages to the users in time duration which he decides. So the prover and verifier could identify the unauthorized user if they get any messages during out of the fixed consecutive timing.

After validation the verifier fixes time intervals for sending and receiving the message. The encrypted message has verifier's MAC information and consecutive time fixed for communication. This encrypted message is forwarded to the prover. The prover obtains this encrypted message and decrypts it to know the consecutive timings for communicating with the verifier.

V. RESULT:

The validation process is performed for accuracy in authentication. The aero-signals are generated and encrypted by using the EDNLib function which helps to replace the original aero-signals with some irrelevant predefined content. The communication is further performed through signals

The information like the landing of aircraft, weather conditions, direction change due to bad weather etc could be performed. The further implementation is to be done with an hardware kit. This hardware kit demonstrates how the information is passed between the prover and the verifier. The information of the user is identified by sensing the RFID tags. This RFID tag consists of the information about the aircraft. Before the information were given manually. But now the information is given by sensing the RFID tags. Then the aero-signals are generated for the detected information using the tags. They are further encrypted using the cipher block rivest algorithm and forwarded to the verifier. Verifier validates the prover authentication information, extracts the MAC address and fixes the consecutive time intervals for the prover to send messages only in that fixed time to maintain

Secrecy. The prover gets this information and sends message to the verifier only during the specified timing. Thus the unauthorized person's interference could be avoided and the information could be passed between the prover and the verifier securely.

VI. Conclusion:

The validation logic is performed with validation rules in order to maintain authentication. The secrecy is maintained by performing validation rules. The encryption and decryption of signals is also considered as important factor in maintaining secrecy. The uniqueness is maintained by identifying the aero signals by detecting the RFID tags. The sensed aero signal is then encrypted using the predefined function using EDNLib. The EDNLib replaces the original content and sent to the receiver. The receiver obtains this encrypted message and validates to extract the MAC address of sender and decrypts it, if it is from a valid user. Finally fixes consecutive timing for exchanging messages encrypts it and send it to the sender. Then sender decrypts the message to know the consecutive timing and send the corresponding messages within the fixed timing. This system maintains secrecy and improves the performance and efficiency.

References:

[1]P. Papadimitratos, A. Kung, J.P. Hubaux, and F. Kargl, "Privacy and Identity Management for Vehicular Communication Systems: A Position Paper," Proc. Workshop Standards for Privacy in User- Centric Identity Management, July 2006.

[2]K. Sampigethaya, L. Huang, M. Li, R. Poovendran, K. Matsuura, and K. Sezaki, "CARAVAN: Providing Location Privacy for VANET," Proc. Embedded Security in Cars (ESCAR) Conf., Nov. 2005.

[3]A. Wasef, Y. Jiang, and X. Shen, "DCS: An Efficient Distributed Certificate Service Scheme for Vehicular Networks," IEEE Trans. Vehicular Technology, vol. 59, no. 2 pp. 533-549, Feb. 2010.

[4]M. Raya and J.-P. Hubaux, "Securing Vehicular Ad Hoc Networks," J. Computer Security, vol. 15, no. 1, pp. 39-68, 2007.

[5]Y. Sun, R. Lu, X. Lin, X. Shen, and J. Su, "An Efficient Pseudonymous Authentication Scheme with Strong Privacy Preservation for Vehicular Communications," IEEE Trans. Vehicular Technology, vol. 59, no. 7, pp. 3589-3603, Sept. 2010.

[6]J.P. Hubaux, "The Security and Privacy of Smart Vehicles," IEEE Security and Privacy, vol. 2, no. 3, pp. 49-55, May/June 2004.

[7]A. Studer, E. Shi, F. Bai, and A. Perrig, "TACKing Together Efficient Authentication, Revocation, and Privacy in VANETs," Proc. IEEE CS Sixth Ann. Conf. Sensor, Mesh and Ad Hoc Comm. And Networks (SECON '09), pp. 1-9, 2009.

[8]L. Eschenauer and V.D. Gligor, "A Key-Management Scheme for Distributed Sensor Networks," Proc. ACM Conf. Computer and Comm. Security, pp. 41-47, 2002.

[9]D. Johnson, A. Menezes, and S. Vanstone, "The Elliptic Curve Digital Signature Algorithm (ECDSA)," Int'l J. Information Security, vol. 1, no. 1, pp. 36-63, 2001.

[10]C. Zhang, R. Lu, X. Lin, P.-H. Ho, and X. Shen, "An Efficient Identity-Based Batch Verification Scheme for Vehicular Sensor Networks," Proc. IEEE INFOCOM, pp. 246-250, 2008.