ISSN: 0975-833X

Available online at http://www.journalcra.com

International Journal of Current Research
Vol. 8, Issue, 03, pp.27456-27459, March, 2016

INTERNATIONAL JOURNAL OF CURRENT RESEARCH

RESEARCH ARTICLE

USE OF CRYPTOGRAPHY IN WIRELESS NETWORK TO PREVENT JAMMING ATTACKS

***Yogesh Sawant, Jainisha Panchal and Prof. Uday Rote**

Mumbai University, Information Technology, K.J.S.I.E.I.T, Mumbai, India

ARTICLE INFO

Article History:
Received 20th December, 2015
Received in revised form
28th January, 2016
Accepted 20th February, 2016
Published online 16th March, 2016

Key words:

Attacks,
Jamming,
Cryptography,
Wireless Network.

ABSTRACT

In a wireless network, when the adversary is being part of the network, they are well known about the protocol being used and other network secrets. A transceiver is enough to get the key and decrypt the message. Hence, simple cryptographic mechanism is not enough to protect the message. Moreover, jamming can be easily performed by modifying the packet header. At the message level permutation and padding are used to protect the message and at the communication level puzzle is used to hide the key. A puzzle solver module in the client system can solve the puzzle and get the key. Attacks are of various types that effect confidentiality and integrity of wireless network and in this paper we are discussing about Jamming attacks. Jamming can stop or disrupt wireless transmission. It is interference, noise or collision at the receiver end. Jamming may happen unintentionally by network load or intentionally in form of attack. No specific hardware is used for executing it, it can be easily implemented by listening to the open medium and broadcasting in the frequency band same as network. If it is executed successfully it gives significant advantages to the attacker at very low cost. That is the reason why it is effective

Citation: Yogesh Sawant, Jainisha Panchal and Prof. Uday Rote, 2016. "Use of cryptography in wireless network to prevent jamming attacks", *International Journal of Current Research,* 8, (03), 27456-27459.

INTRODUCTION

The open nature of the wireless medium leaves it vulnerable to intentional interference attacks, typically referred to as jamming. This intentional interference with wireless transmissions can be used as a launch pad for mounting Denial-of-Service attacks on wireless networks. Typically, jamming has been addressed under an external threat model. However, adversaries with internal knowledge of protocol specifications and network secrets can launch low-effort jamming attacks that are difficult to detect and counter. In a wireless network, when an adversary is outside the network (external hacker), their presence is easy to detect. The external adversary normally uses the inter packet timing information as a key to detect the protocol being used. High effort is spent to classify the packet. Also the presence of high energy signal for a long duration is easy to detect. But, when the adversary is being part of the network, they are well known about the protocol being used and other network secrets. Low effort jamming attack can be easily performed. Even though cryptographic mechanisms are used, a half-duplex transceiver is enough to compromise and get the key. Even, special Cryptanalysis hardware is being used to decrypt the message.

****Corresponding author: Yogesh Sawant,***
Mumbai University, Information Technology, K.J.S.I.E.I.T, Mumbai, India.

So we need some other mechanism to protect our data. We are going to apply permutation and padding to protect our message. The jamming is easily achieved by simply modifying the packet header, when the syntax and semantics of the protocol is well known. At the message level our message should be protected from such jamming attacks that usually lead to Denial of Service Attack using Permutation (Randomization of message). A Cryptographic puzzle is going to be used to protect the key during communication.

Existing System

Normally, jamming attacks are considered as external threat. Jamming is performed by continuous or random transmission of high – power signal. The continuous presence of high power signal is easy to detect. Even when the adversary is being part of the network, several methods already proposed each with its own disadvantage.

Encryption / Decryption

Usual method to protect the message is to encrypt the message based on a key and decrypting the message at the receiver. Since the wireless medium is having open nature, a transceiver is enough to get the key and decrypt the message [Brown et al., 2006].

(ii) Dynamic channel allocation according to a cryptographic function. Instead of mapping the control channels to static locations (in terms of timeslot, frequency), it randomly maps them according to a cryptographic function. Such a mapping is unpredictable for an external attacker since it does not have the shared secret within the system. Any internal attacker will know the locations of the control channels and easy hack the message [Chan et al., 2007].

Random key distribution for channel allocation

The use of random key distribution to hide the location of control channels in frequency and/or time. Any internal attacker will know the locations of the control channels and easy hack the message.

Types of Jammers

Jammers are of four models. They are [IRACST, 2013]

- Constant jammer
- Reactive jammer
- Deceptive jammer
- Random jammer

- Constant Jammer: In this model, jammer continuously emits RF signals and it transmits random bits of data to channel. It does not follow any MAC layer etiquette. Being constant to the transfer it does not wait for channel to become an idle.
- Deceptive Jammer: In this model, jammer constantly injects series packets to the channel without any gap between subsequent transmissions. It also broadcasts fabricated messages and reply old ones. Jammer will pass preambles out to the network and just check the preamble and remain silent.
- Random Jammer: In this model, jammer alternates between period of continuous jamming and inactivity. After jamming for t1 units of time, it stops emitting radio signals and enter into sleep mode. The jammer after sleeping for t2 units of timewakes up and resumes jamming. Both time t1 and t2 is either random or fixed.
- Reactive Jammer: In this model, jammer will stay quite when the channel is idle. As soon as it senses activity on channel, it starts transmitting signal. In order to sense the channel jammer is ON and should not consume energy. To mitigate jamming attacks many hiding schemes were used. These are

• Strong hiding commitment scheme
• Cryptographic puzzle base scheme
• All-or-nothing transmission

Proposed System

When the adversary is being part of the network that is aware of network secretes and the implementation details network protocols, low effort jamming can be easily performed. They usually target at the messages of high importance like Routing messages like Route Request/ Reply which may lead to Denial of Service, TCP Acknowledgements that requires retransmission of packets, which may lead to reduction in throughput etc. The jamming is performed by packet classification. We have to prevent packet classification.

Related Work

Protecting the Message

Let us take our message to be transmitted as m. The Sender has packet m for the Receiver. Before committing the message m to the receiver the following functions are performed.

$$C = Ek (\Pi (m)) \quad (1)$$

Where Π is the Permutation function that randomizes the message. E is the encryption function which encrypts the permuted message based on the key k. For encryption we can use encryption algorithm like AES.

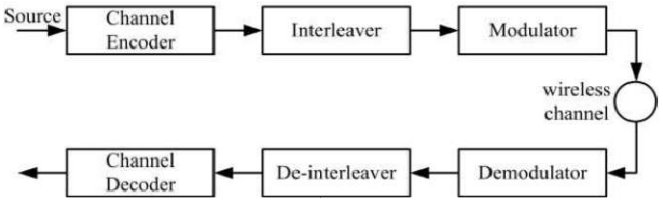

Fig. 1. Block Diagram

Permutation

The message is going to be split into a number of plaintext blocks depending on the size of the message. Each and every field of the message or packet is randomized. (ie), character of the field is divided to each plaintext blocks starting from the last block, that is in the reverse order. The permutation distributes the critical fields which are used for packet classification across multiple plaintext blocks which are then converted into cipher text blocks.

Padding

Later modulation is performed by adding extra bits depending on the length of the message. To increase the size of the message, padding of some random characters is done to the encrypted message as in Fig 1. It is represented as

$$C \parallel pad (C) \quad (2)$$

At the receiver the reverse process should be carried out to get the original message. Even though the adversary gets the key, without applying the reverse of padding and permutation we cannot get the original message back.

Message Recovery

To reconstruct these fields all the cipher text blocks must be received; demodulation of padded characters should be carried out; decryption using the received key and then reverse of permutation is applied to the plain text to get the original message. In order to recover the message, the following function has to be performed.

$$M = \Pi\text{-}1(Dk(C)) \quad (3)$$

At first, the message is decrypted using key k. Then reverse of Permutation is applied.

Protecting the Key

Usually jamming attack is performed by modifying the packet header. The source and/ or destination address are modified so that the packet won't reach the actual recipient. Any random modification of the packet header leads to denial of service attack. Our packet is already randomized. To protect the key here we are going to develop a puzzle which involves some sequence of Mathematical calculations based on a random number generated

Sender SReceiver R

Generate: k, Tp.

Compute:

C= Ek(□(m))

P= puzzle (k,Tp) $\xrightarrow{(C,P)}$ k'=solve(p)

Compute:

m'=□$^{-1}$(Dk(C))

Let the puzzle P. The sender generates puzzle P = puzzle (), which is puzzle generator function. The key is going to be sent in the same packet as that of the message m. The key is tied with the Puzzle. The Message generated at level 1 is going to be sent along with the decryption key k as a single packet as shown in Figure 2 (C,P)

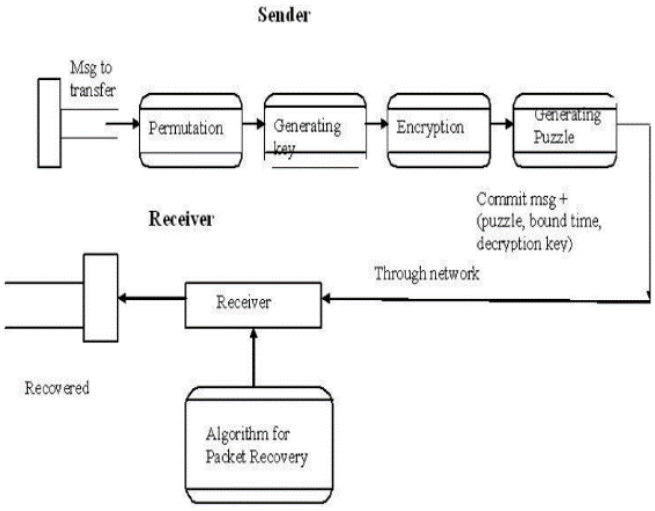

Fig. 2. Data Flow Diagram But the key is hidden with the puzzle and time to solve the puzzle Tp

P = puzzle (k, Tp)

(4) Where Tp is the time to solve the puzzle. The time to solve the puzzle P was chosen small so that a client could not solve the puzzle within Tp. Key Recovery The receiver has to solve the puzzle within the time Tp to get the key k. Usually the time Tp will be chosen such that the puzzle could not be solved within the time Tp by a untrusted network client. Puzzle Solver Module When the client could not solve the puzzle within the time Tp, again it will lead to Denial of Service attack; which merely wastes the resources (time and processing power) of the client.

To overcome this problem, we have developed a Puzzle Solver Module (PSM). It is a software module which is based on the puzzle generator module. It uses the reverse algorithm of puzzle developer and easily solves the puzzle within the short duration. The time the PSM takes to solve the puzzle is usually less than the time Tp. Hence the client system which was installed with PSM can easily solve the puzzle and get the key to decrypt the message.

Conclusion

Even though the adversary is trying to hack the packet by doing cryptanalysis the key k is given to the puzzle P which prevents any receiver from recovering the key for at least time Tp. The Tp was chosen so that the transmission will be completed before the puzzle is solved. At a trusted client, a puzzle solver module solves the puzzle within the stipulated time period without much wastage of resources. The authenticated recipient can recover the key in the time period which is less than Tp. The Puzzle generation can be implemented without the wastage of resource. When comparing with the cost of security it is negligible.

REFERENCES

Alejandro Proan˜o and LoukasLazos,"Packet-Hiding Methods for Preventing Selective Jamming Attacks", IEEE Transactions on Dependable and Secure Computing, Vol. 9, No. 1, January/February 2012

Brown, T.X., James, J.E. and Sethi, A. 2006. "Jamming and Sensing of Encrypted Wireless Ad Hoc Networks," Proc. ACM Int'l Symp. Mobile Ad Hoc Networking and Computing (MobiHoc), pp. 120-130.

Chan, A., Liu, X., Noubir, G. and Thapa, B. 2007. "Control Channel Jamming: Resilience and Identification of Traitors," Proc. IEEE Int'l Symp. Information Theory (ISIT).

Dempsey, T., Sahin, G., Morton, Y. and Hopper, C. 2009. "Intelligent Sensing and Classification in Ad Hoc Networks: A Case Study," IEEE Aerospace and Electronic Systems Magazine, vol. 24, no. 8, pp. 23-30, Aug.

Greenstein, B., Mccoy, D., Pang, J., Kohno, T., Seshan, S. and Wetherall, D. 2008. "Improving Wireless Privacy with an Identifier-Free Link Layer Protocol," Proc. Int'l Conf. Mobile Systems, Applications, and Services (MobiSys).

IEEE, 2007. IEEE 802.11 Standard, http://standards.ieee.org/getieee802/download/802.11-2007.pdf.

IRACST – 2013. International Journal of Computer Science and Information Technology & Security (IJCSITS), ISSN: 2249-9555 Vol. 3, No.2, April.

Juels, A. and Brainard, J. 1999. "Client Puzzles: A Cryptographic Countermeasure against Connection Depletion Attacks," Proc. Network and Distributed System Security Symp. (NDSS), pp. 151-165.

Law, Y.W. Palaniswami, M., Hoesel, L.V., Doumen, J., Hartel, P. and Havinga, P. 2009. "Energy-Efficient Link-Layer Jamming Attacks against WSN MAC Protocols," ACM Trans. Sensor Networks, vol. 5, no. 1, pp. 1-38.

Lazos, L., Liu, S. and Krunz, M. 2009. "Mitigating Control-Channel Jamming Attacks in Multi-Channel Ad Hoc Networks," Proc. Second ACM Conf. Wireless Network Security, pp. 169-180.

Lin, G. and Noubir, G. 2004. "On Link Layer Denial of Service in Data Wireless LANs," Wireless Comm. and Mobile Computing, vol. 5, no. 3, pp. 273-284, May.

Liu, X., Noubir, G. and Sundaram, R. 2007. "Spread: Foiling Smart Jammers Using Multi-Layer Agility," Proc. IEEE INFOCOM, pp. 2536-2540.

******