Volume : 2 | Issue : 11 | Nov 2013 • ISSN No 2277 - 8160

Research Paper Engineering

Packet Hiding Method for Providing Security Over Jamming Attacks in Wireless Network

S. M. Keerthana Master Of Engineering, Dept.Of ECE, Parisutham Institute Of Technology And Science, Thanjavur, India.

D. Parameshwari Assistant Professor,Dept.Of ECE, Parisutham Institute Of Technology And Science, Thanjavur, India.

ABSTRACT

In the wireless networks the wireless medium leaves it vulnerable to premeditated meddling attacks, typically referred to as jamming. This premeditated meddling used in wireless transmission for Denial-of-Service on wireless networks. Fundamentally jamming has been addressed under external threat model. We proposed the problem of internal threat model. In the internal threat model the jammer with awareness of protocols and network secrets can perform low-effort jamming attacks. These attacks are difficult to discover and counter. In this paper, we propose the badly-behaviours of selective jamming attacks and also the jammer is active only for a short period of time and selectively targeting messages of high importance. We show that selective jamming attacks can be launched by performing real-time packet classification at the physical layer. To mitigate these attacks, we develop four schemes that prevent real-time packet classification by linking encrypting methods with physical-layer attributes.

KEYWORDS : DES, Cryptographic, Jamming attack

1. INTRODUCTION:

The wireless network means gives the continuous accessibility of wireless medium to communicate the participating nodes. The wireless network can be classified into two methods open network and closed network. Open network can easily defined by the internet, there are multiples of computers and devices can be connected through various protocols and connection methods. In this paper open network referred as external threat model. Closed network can easily define by organisations, there is single protocol and single connection method is used. In this paper closed network referred as internal threat model. In conventional model the jamming attacks are considered only on external threat model. In external threat model jammer is not part of the network. In the proposed paper jammer is part of internal threat model with the knowledge of network protocols and secrets at the layer level. The jammer abuses his internal knowledge for initiation of selectively jamming attacks in which particular messages of "high importance" are targeted. For example, a jammer can aim TCP acknowledgments in a TCP session to reduce the amount of data transmission on end-to-end flow. The jammer must have the skill to implement the "classify-then-jam" strategy before the end of transmission.

2. PROBLEM STATEMENT AND ASSUMPTIONS

2.1. Problem Statement

Fig.1

J (Jammer)

(A and B Sender and Receiver respectively)

The Fig.1 shows Node A as sender and B as receiver interconnect through a wireless medium. Within the communication range of both A and B there is a jamming node J. When A transmits a packet m to B, node J categorises m by getting only the first few bytes of m. The jammer node J spoils m outside retrieval by meddling with its response at B. We discourse the difficulty of preventing the blocking node from categorizing m in real time, thus moderating J's capability to achieve selective blocking. Our goal is to transform a selective jammer to a random one. Note that in the present work, we do not address packet classification methods based on protocol semantics.

2.2. System and proposed model

2.2.1. Network model:

The network means, it is a group of nodes connected through wire or wireless. Here we propose our strategy in wireless network. The nodes can connect directly when they are inside communication range. If the nodes outside the communication it will be connected indirectly through many hops. Transmissions can be each encrypted or unencrypted.

2.2.2. Communication Model:

In the wireless network transmission Packets are transmitted at a rate of R bauds. Each PHY-layer symbol corresponds to q bits. Every symbol carries q data bits, where α/β is the rate of the PHY-layer encoder. The encoder output is divided into symbols by the inter-leaver. Here, the transmission bit rate is equal to qR bps. Spread spectrum techniques such as frequency hopping spread spectrum or direct sequence spread spectrum may be used at the PHY layer to protect wireless transmissions from jamming. Spread spectrum provides protection to interference to some extent. The PHY layer header contains information about the length of the frame, and the transmission rate. The MAC header defines the MAC protocol version, the sender and receiver addresses, sequence numbers and additional fields. The MAC header is charted by the frame body that usually contains an ARP packet or an IP datagram. In conclusion, the MAC frame is protected by a cyclic redundancy check (CRC) code. At the PHY layer, a trailer may be attached for synchronizing the sender and receiver.

2.2.3. Proposed Model:

We assume that the jammer can be placed at any part of network medium and can jam messages at any part of the network. The jammer can function in full-duplex mode, thus being able to receive and transmit concurrently. For analysis purposes, we assume that the jammer can pro-actively jam a number of bits just below the ECC capability early in the transmission. He can then decide to irrecoverably corrupt a transmitted packet by jamming the last symbol. In reality, it has been demonstrated that selective jamming can be achieved with far less resources. A jammer equipped with a single half-duplex transceiver is sufficient to classify and jam transmitted packets. However, our model captures a more potent jammer that can be effective even at high transmission speeds. The jammer is assumed to be computationally and storage bounded, although he can be far superior to normal nodes. In particular, he can be equipped with special purpose hardware for performing cryptanalysis or any other required computation. Solving well-known hard cryptographic problems is assumed to be time-consuming. For the purposes of analysis, given a cipher text, the most efficient method for deriving the corresponding plaintext is assumed.

3. Methodologies

3.1. REAL TIME PACKET CLASSIFICATION

In the Real time packet classification, we define how the jammer can classify packets in real time; previously the packet communication is finished. Once a packet is classified, the jammer can choose to jam it

depending on his plan. Consider the communication system depicted in Fig. 2. At sender side the PHY layer, a packet m is encoded, interleaved, and modulated before it is transmitted on the wireless medium. At the receiver side, it is demodulated, de-interleaved, and decoded, to recover the original packet m.

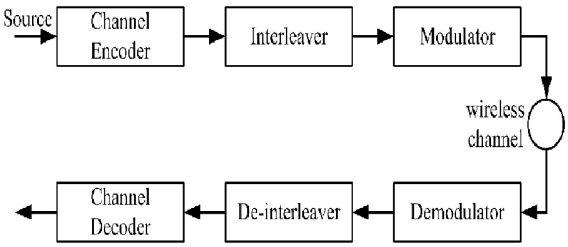

Fig. 2 A generic communication system diagram. [1]

The jammer's ability in classifying a packet m depends on the implementation.

3.1.1. Channel Encoder

The channel encoder encodes the original data with necessary bits through this process the original data packets are expanded. By this expansion the channel errors are rectified. For example, a α/β-block code could protect m from up to e errors per block. Alternatively, a α/β-rate convolutional encoder with a constraint length of L_{max}, and a free distance of e bits provides similar protection. For our purposes, we assume that the rate of the encoder is α/β.

3.1.2. Inter-leaver

In the inter-leaver output of channel encoder is given as input, and it change the original encoded data into symbols. Symbol means inter-leaver divide original data packet into individual packs. Through this implementation burst errors are omitted. The de-inter-leaver is simply doing the reverse process.

3.1.3. Modulator

Using modulation technique the output of inter-leaver is modulated for the desired transmission medium. In the modulation process digital data is transmitted into analogy waveform. At last in digital modulation process, maps the received bit stream to symbols of length q. usually modulation techniques maybe OFDM, BPSK.

3.2. A Strong Hiding Commitment Scheme (SHCS)

In SHCS, we overcome that the problem of real-time packet classification can be drawn to the hiding property of commitment schemes, and propose a packet-hiding scheme based on commitments.

Through SHCS the original packets are permutated and encrypted with random symmetric key. We use DES to encrypt. After the permutation padding bits are added after this process it wills permutated once again. Undertake that the sender S has a packet m for receiver R. Beginning of transmission, S makes (C, d) = commit (m), where, C = Ek(π1(m)), d = k. π1 is a publicly known permutation, and k ∈ {0, 1} s is a randomly selected key of some desired key length s. The sender broadcasts (C||d). To fulfil the strong hiding property, the packet carrying d is formatted so that all bits of d are modulated in the last few PHY layer symbols of the packet. To recover original data any receiver must receive and decode the last symbols of the transmitted packet, thus preventing early discovery of d.

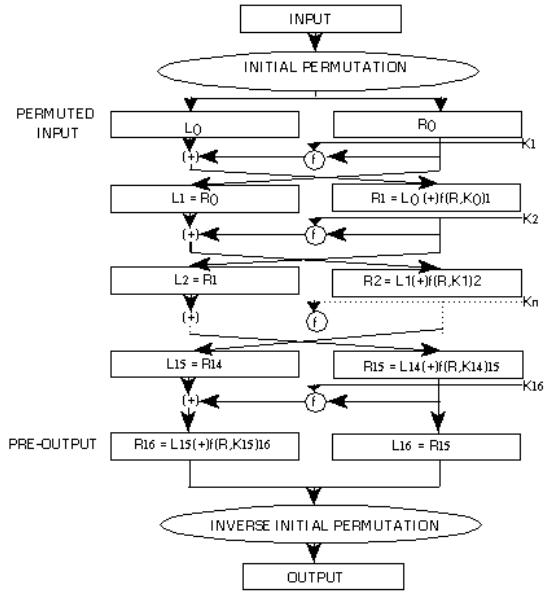

Fig. 3 Generic format of DES [11]

5. Classification

Methodology	Conventional	Proposed
Real time packet classification	The jammer on network and transport layers through AODV protocol.	The jammer on network and transport layers through TCP protocol.
SHCS	The Hiding Based on Commitments is used to protect the data.	In proposed SHCS used the protection based on symmetric key and also partially released.
CPHS	There is no CPHS is used.	The CPHS applied on TCP packets only based on time clock.
AONT	In AODV protocol, AONT is not used.	In TCP, the linear transformation is used.

In order to our model the jammer gets slow down and avoided. The TCP packets are transmitted safely between the sender and receiver.

4. CONCLUSION

We talked about the difficulties of selective jamming attacks in wireless network medium. We considered an internal adversary model in which the jammer is part of the network under attack, thus being aware of the protocol specifications and shared network secrets. We showed that the jammer can classify transmitted packets in real time by decoding the first few symbols of an on-going transmission. We evaluated the effectiveness of jamming attacks on wireless network protocol such as TCP. Our findings show that a selective jammer can significantly impact performance with very low effort. We developed three schemes that transform a selective jammer to a random one by preventing real-time packet classification. Our schemes combine cryptographic primitives such as commitment schemes, cryptographic puzzles, and all-or-nothing transformations (AONTs) with physical layer characteristics. We analysed the security of our schemes and quantified their computational and communication overhead.

REFERENCES

1. Alejandro Proano and Loukas Lazos, Packet-Hiding Methods for Preventing Selective Jamming Attacks, IEEE TRANSACTIONS ON DEPENDABLE AND SECURE COMPUTING ,VOL. 9, NO. 1, JAN-FEB 2012 | | 2. M.Gowsalya, V.Palanisamy, Detection and prevention of congestion attacks and packet loss using piggyback methods in wireless network, International Journal of Engineering Trends and Technology-olume3Issue3- 2012 | | 3. Kpele,Marios, Denial of Service Attacks in Wireless Networks: The case of Jammers, Communications Surveys & Tutorials, IEEE, Page(s): 245 - 257 | | 4. Mario Cagalj, Srdjan Capkun, and Jean-Pierre Hubaux, Wormhole-Based Antijamming Techniques in Sensor Networks, IEEE TRANSACTIONS ON MOBILE COMPUTING, VOL. 6, NO. 1, JANUARY 2007 | | 5. Timothy X Brown, Jesse E. James, Amitha Sethi, MobiHoc Proceedings of the 7th ACM Jamming and Sensing of Encrypted international symposium on Mobile ad hoc Wireless ad hoc networks, Networking and computing, Pages 120-130. | | 6. Agnes Chan, Xin Liu, Guevara Noubir, Bishal Thapa, Control Channel Jamming: Resilience and Identification of Traitors, Information Theory, 2007. ISIT 2007. IEEE International Symposium on, Page(s): 2496 - 2500 | | 7. Tae Dempsey, Gokhan Sahin, Y.T. (Jade) Morton, Chahira M. Hopper, Intelligent Sensing and Classification in Ad Hoc Networks: A Case Study, Aerospace and Electronic Systems Magazine, IEEE, Aug. 2009, Page(s): 23 - 30 | | 8. Loukas Lazos, Sisi Liu, and Marwan Krunz, Mitigating Control-Channel Jamming Attacks in | Multi-channel Ad Hoc Networks, Mobile Computing, IEEE Transactions on, Page(s): 1545 – 1558 |