Autonomous Encoding of Packets in Wireless Sensor Network

Patole Uttam R¹, Sunil Gupta²
¹M.Tech (CSE) S.V. C.S&H.E Alwar, Rajasthan
²M.Tech (CSE) Associate Prof. S.V. C.S&H.E Alwar, Rajasthan

Abstract—The jamming attacks nothing but in open nature of wireless medium. They leave vulnerable to intentional interference attack. The launched pad used for mounting denial of service attack in wireless network intentionally interferes with wireless transmission. In this work the problem of selective jamming attacks in wireless network is addressed. In these attack adversary is remain active for a short period time and which is target selective massage of high importance. The target present here in two case studies as a selective attack on TCP and attack on routing which is advantageous of selective jamming in terms of network performance degradation.

We show that the selective jamming attacks can be mounted by easy real time packet classification in physical layer. To achieve this attack to implementing three schemes that avoids real time packet classification with combination of cryptographic primitives in physical layer. We analyze the security for our method and computational over head.

Keywords—Selective jamming, denial of service, packet classification, cryptography.

I. INTRODUCTION

The problem of jamming under an internal threat model is addressed. Consider a sophisticated adversary who has knowledge about network secrets and the details of implementation in network protocol at any layer in network stack. The adversary uses his internal knowledge for implementing selective jamming attacks where the message has high importance are targeted. Example, A jammer may target route request/ reply message at the routing layers. To avoid discovery of route or target of TCP identification in TCP session, degrade overall throughput of end to end flow. The jammer has ability to identify first few bits of a packet. It can be packet identifiers like packet type, source and destination address useful in recovery of packets. When the classification done by them, there is sufficient number of bit errors due to this packet cannot be recovered at receiver side.

II. EXISTING SYSTEM

The conventional system uses the techniques which are depends on spread spectrum (SS) communication or in the form of evasion of jamming. In Spread Spectrum technique the security provides using bit level which distributes bits according to secrets pseudo wise (PN) code, which are known to only communication parties. These techniques only useful in external threat model for wireless communication.

Disadvantages of Existing System:
1) In broadcast communication the possibility that it can vulnerable under an internal threat model because all users have known the secrets which is used for transmission.
2) Due to open nature of wireless transmission may vulnerable to intentional interference attacks called as jamming.
3) Anybody with the transceiver can watch the wireless communication, adding its own messages or may congest the network.
4) So single user is sufficient to take cryptographic information.

III. PROPOSED SYSTEM

The solution for existing system over a selective jamming is the transmitted packets have encryption (including headers) with a static key. In broadcast communication this static key for decryption which is known to all intended receivers, due to this it is susceptible to compromise. The hiding scheme have encryption key which is remain secret, the static portion of transmitted packets may lead to classification of packet.

Advantages of proposed system
1) It is easy to implement than other scheme by using internal knowledge of network protocol and basics of cryptography extracts from compromised node.

2) Here we detects that the selective jamming may lead to Denial of service attacks with very low possibility.
3) It gives very strong security properties.
IV. MODULES DESCRIPTION

Real time packet classification:

In the physical layer, the wireless channel have a packet m is encoded, interleaved and modulated before it can be transmitted. After it reaching to receiver it is demodulated, de-interleaved and decoded to achieve the original packet m. The communication range of both A and B. When the packet m is transmitted by A to B, J has ability to classify it with only first few bytes of m. Then J corrupts m before reception at B by interfering it.

Strong Hiding Commitment Scheme:

The strong hiding commitment scheme (SHCS) is based on the symmetric cryptography. Assumption is that the sender gives packet to receiver. The sender S builds commit message, the committer function is an off the shelf symmetric encryption algorithm is publicly known permutation and randomly selected key K having length S (the length k is security parameter). After reception of d the receiver R computes cryptographic puzzle hiding scheme.

The sender S has packet m for transmission. The random key k is selected by sender of some specific length. Sender S generates puzzle (key, time) where puzzle () indicates puzzle generator function and tp denotes gives required time for puzzle solution. The parameter is counted in units of time and which is directly dependent on capability for solving of adversary indicates by N and count using computation operations per second.

Puzzle P is generated, the sender broadcasts (c,p). At receiver end receiver R solves desired puzzle to recover key and computes it.

Hiding Transformation on All- or Nothing Based:

In AONT scheme packets are preprocessed before transmission but it is unencrypted. The packet classification cannot perform by jammer up to all pseudo massage corresponding to the original packet have been received and transformation is applied by inverse.

The UDDI is semantically categorised where we combine ontology’s with established hierarchical clustering method, the service description vector building process. In service description vector for each term, a corresponding concept is located in the respective ontology. If match occur this concept is added in description vector. The remaining additional concepts are added and irrelevant terms are deleted on the basis of semantic relationship. An easy way to comply with the conference paper formatting requirements is to use this document as a template and simply type your text into it.

REFERENCES