Packet-Hiding Methods for Preventing Selective Jamming Attacks using Swarm Intelligence Techniques

M. Rameshkumar¹, Dr. S. Sakthivel²

¹Asst. Professor/ Computer Science & Engineering, Jayalakshmi Institute of Technology, Thoppur, Tamilnadu
²Professor / Information Technology, Sona College of Technology, Salem, Tamil Nadu

Abstract—This paper aims to explore on Packet-Hiding Methods for Preventing Selective Jamming Attacks using Swarm intelligence techniques. This core concept explains the different hiding methods and its jamming attacks using swarm intelligence system. The open nature of the wireless medium leaves it vulnerable to intentional interference attacks, typically referred to as jamming. This system will help in real time network security system for identifying the different attacks while using the internet. Through internet, the different packets are to be used for transferring the data from one place to another using packet with a key. When the data packet is transferred, the security concern also needs to take into consideration. The research gap of this paper is to fulfill most secured way of transferring data by using swarm intelligence techniques.

I. INTRODUCTION

The selective jamming attacks can be launched by performing real time packet classification at the physical layer. To mitigate these attacks develop a scheme that prevent real-time packet classification by combining cryptographic primitives with physical layer attributes. The Swarm intelligence algorithm is proficient enough to adapt change in network topology and traffic. The sender and receiver change channels in order to stay away from the jammer, in channel hoping techniques. The Swarm intelligence techniques forward either unicast or broadcast at each node depending on the availability of the channel information for end of channel.

II. EXISTING SYSTEM

Conventional anti-jamming techniques rely extensively on spread-spectrum (SS) communications or some form of jamming evasion (e.g., slow frequency hopping, or spatial retreats). SS techniques provide bit-level protection by spreading bits according to a secret pseudo-noise (PN) code, known only to the communicating parties. These methods can only protect wireless transmissions under the external threat model.

III. DISADVANTAGES OF EXISTING SYSTEM

The system does not solves the real time classification and not prevent the packet at the time of attackers. Broadcast communications are particularly Vulnerable under an internal threat model because all intended receivers must be aware of the secrets used to protect transmissions. Hence, the compromise of a single receiver is sufficient to reveal relevant cryptographic information.

IV. PROPOSED SYSTEM

An intuitive solution to selective jamming would be the encryption of transmitted packets (including headers) with a static key. However, the broadcast communications, this static decryption key must be known to all intended receivers and hence, is susceptible to compromise. Moreover, even if the encryption key of a hiding scheme were to remain secret, the static portions of a transmitted packet could potentially lead to packet classification.

Advantages Of Proposed System

The combination of cryptographic primitives with physical layer attributes for preventing real-time packet classification and neutralizing the inside knowledge of the attacker.

The swarm intelligence techniques which updates the sensor details more effectively and successfully.

V. PACKET-HIDING METHODS

- Real Time Packet Classification
- A Strong Hiding Commitment Scheme
- Cryptographic Puzzle Hiding Scheme
- Hiding based on All-Or-Nothing Transformation

Real Time Packet Classification

At the physical layer, a packet m is encoded interleaved, and modulated before it is transmitted over the wireless channel. At the receiver, the signal is demodulated, deinterleaved and decoded to recover the original packet m.
Nodes A and B communicate via a wireless link's 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 classifies m by receiving only the first few bytes of m. J then corrupts m beyond recovery by interfering with its reception at B. We address the problem of preventing the jamming node from classifying m in real time, thus mitigating J's ability to perform selective jamming.

A Strong Hiding Commitment Scheme

A strong hiding commitment scheme (SHCS), which is based on symmetric cryptograph. Assume that the sender has a packet for receiver. First, S constructs commit (message) the commitment function is an off-the-shelf symmetric encryption algorithm is a publicly known permutation, and K is a randomly selected key of some desired key length S (the length of K is a security parameter). Upon reception of d, any receiver R computers.

Cryptographic Puzzle Hiding Scheme

A sender S has a packet m for transmission. The sender selects a random key k, of a desired length. S generates a puzzle (key, time), where puzzle() denotes the puzzle generator function, and tp denotes the time required for the solution of the puzzle.

The parameter is measured in units of time, and it is directly dependent on the assumed computational capability of the adversary, denoted by N and measured on computational operations per second.

After generating the puzzle P, the sender broadcasts(C, P). At the receiver side any receiver R solves the received puzzle to recover key and then computes.

Hiding based on All-Or-Nothing Transformation

The Packets are pre-processed by an AONT before transmission but remain unencrypted. The jammer cannot perform packet classification until all pseudo-messages corresponding to the original packet have been received and the inverse transformation has been applied.

Swarm Intelligence

An artificial intelligence (AI) technique based on the collective behavior in decentralized, self-organized systems.

- No centralized control structures
- Based on group behavior found in nature

Swarm intelligence (SI) is an artificial intelligence technique based around the study of collective behavior in decentralized, self-organized systems. Introduced by Beni & Wang in 1989.

VI. TWO COMMON SI ALGORITHMS

- Ant Colony Optimization (ACO)
- Particle Swarm Optimization

ACO algorithm techniques can be used in a number of applications like controlling unmanned vehicles, control nanobots within the body for the purpose of killing cancer tumors. Swarm intelligence has also been applied for data mining. Meta-Heuristic algorithms have been applied to three areas of software engineering: test data generation, module construction and cost/effort prediction. But these algorithms can be applied to many other operations in software engineering and much research should be done in this field.

Optimization using SI

Swarms have the ability to solve problems Ant Colony Optimization (ACO), a meta-heuristic ACO can be used to solve hard problems like TSP, Quadratic Assignment Problem (QAP)
Design SI Systems

The 3 step process

1. Identification of analogies: in swarm biology and IT systems
2. Understanding: computer modelling of realistic swarm biology and engineering
3. Model simplification and tuning for IT applications

Ant foraging
Cooperative search by pheromone trails

Example for SI
An In-depth Look at Real Ant Behaviour

The Path Thickens!
The New Shortest Path

Ant foraging
Cooperative search by pheromone trails
VII. CONCLUSION

Packet hiding method is used to prevent the selective jamming attacks. This will improve the detection of a jammer quickly with less complication. The existing system not prevents the real time packet classification. The Swarm intelligence algorithm is proficient enough to adapt changes in network topology and traffic.

The combination of cryptographic primitives with physical layer attributes for preventing real-time packet classification and neutralizing the inside knowledge of the attackers.

REFERENCES

[15] www.adaptiveview.com/articles/ipsop1
[16] “Particle Swarm Optimization” http://www.swarmintelligence.org