ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

# Combining Cryptographic Technique to Avoid Attacks in Wireless Networks

**I.Chinna Rao**
**M.Tech CSE,**
**Sri Sivani College of Engineering,**
**Chilakapalem.**

**G. Rajendra Kumar**
**Professor,**
**Sri Sivani College of Engineering,**
**Chilakapalem.**

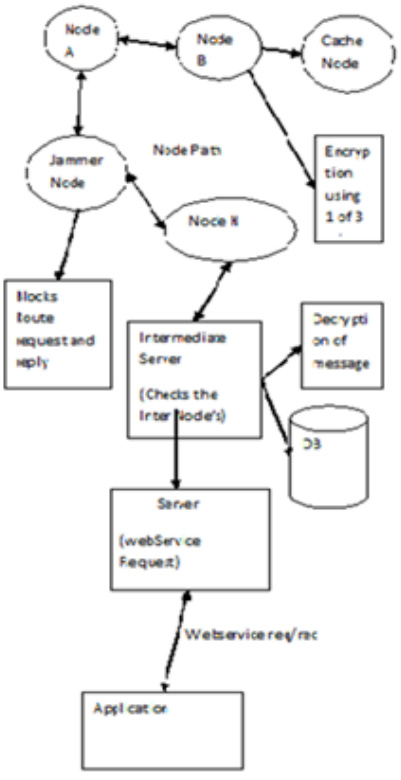
## ABSTRACT:

The Open Nature of wireless medium leaves an intentional interference attack, typically referred to as jamming. This intentional interference with wireless transmission launch pad for mounting Denial-Of-Service attack on wireless networks. Typically, jamming has been addresses under an external threat model. However, adversaries with internal knowledge of protocol specification and network secrets can launch low-effort jamming attacks that are difficult to detect and counter. In this work we address the problem of jamming attacks and adversary is active for short period of time, selectively targeting the messages of high importance. We show that the selective jamming attacks can be launched by performing real-time packet classification at the physical layer. To mitigate these attacks, we develop three schemes that prevent real time packet classification by combining cryptographic primitives with physical-layer attributes. They are Strong Hiding Commitment Schemes (SHCS), Cryptographic Puzzles Hiding Schemes (CPHS), and All- Or-Nothing Transformation Hiding Schemes (AONTSHS). Random key distribution methods are done along with three schemes to give more secured packet transmission in wireless networks.

## INTRODUCTION:

To show that selective jamming attacks can be launched by performing real time packet classification at the physical layer. To mitigate these attacks develop a schemes that prevent real-time packet classification by combining cryptographic primitives with physical layer attributes. To address the problem of jamming under an internal threat model and consider a sophisticated adversary who is aware of network secrets and the implementation details of network protocols at any layer in the network stack. The adversary exploits his internal knowledge for launching selective jamming attacks in which specific messages of high importance are targeted. For example, a jammer can target route-request/route-reply messages at the routing layer to prevent route discovery, or target TCP acknowledgments in a TCP session to severely degrade the throughput of an end-to-end flow. The jammer may decode the first few bits of a packet for recovering useful packet identifiers such as packet type, source and destination address. After classification, the adversary must induce a sufficient number of bit errors so that the packet cannot be recovered at the receiver.

## SYSTEM ARCHITECTURE:



ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

## EXISTING SYSTEM:

Conventional ant-jamming techniques extensively on spread-spectrum 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. Potential disclosure of secrets due to node compromise neutralizes the gains of SS. 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.

## DISADVANTAGES OF EXISTING SYSTEM:

Under this model, jamming strategies include the continuous or random transmission of high power interference signals. However, adopting an "always-on" strategy has several disadvantages. First, the adversary has to expend a significant amount of energy to jam frequency bands of interest. Second, the continuous presence of unusually high interference levels makes this type of attacks easy to detect.

## PROPOSED SYSTEM:

In this paper, we address the problem of jamming under an internal threat model. We consider a sophisticated adversary who is aware of network secrets and the implementation details of network protocols at any layer in the network stack. The adversary exploits his internal knowledge for launching selective jamming attacks in which specific messages of "high importance" are targeted. For example, a jammer can target route-request/route-reply messages at the routing layer to prevent route discovery, or target TCP acknowledgments in a TCP session to severely degrade the throughput of an end-to end flow.

## ADVANTAGES OF PROPOSED SYSTEM:

Evaluated the impact of selective jamming attacks on network protocols such as TCP and routing and show that a selective jammer can significantly impact performance with very low effort and developed three schemes that transform a selective jammer to a random one by preventing real-time packet classification. Schemes combine cryptographic primitives such as commitment schemes, cryptographic puzzles, and all-or-nothing transformations with physical layer characteristics and analyzed the security of our schemes and quantified their computational and communication overhead. With these schemes a random key distribution has been implemented to more secure the packet transmission in the wireless networks.

## IMPLEMENTATION MODULES:

- ✓ Real Time Packet Classification
- ✓ A Strong Hiding Commitment Scheme
- ✓ Cryptographic Puzzle Hiding Scheme
- ✓ Hiding based on All-Or-Nothing Transformations
- ✓ MD5 Algorithm:

### 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, de-interleaved and decoded to recover the original packet m. Nodes A and B communicate via a wireless link. 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.

### A Strong Hiding Commitment Scheme:

A strong hiding commitment scheme (SHCS), which is based on symmetric cryptography. Assume that the sender has a packet for Receiver. First, S constructs commit( message ) the commitment function is an off-

ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

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 computes.

### 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. 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 in 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 Transformations:

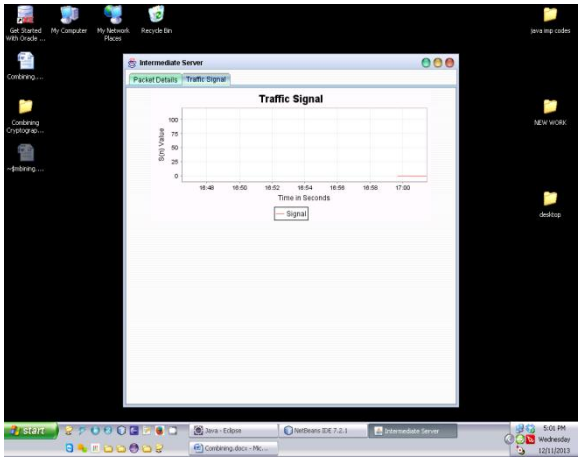
The packets are pre-processed by an AONT before transmission but remain unencrypted. The jammer cannot perform packet classification until all pseudo-messages corresponding to the original packet have been received and the inverse transformation has been applied. Packet m is partitioned to a set of x input blocks m = {m1, m2, m3….}, which serve as an input to an The set of pseudo-messages m = {m1, m2, m3,…..} is transmitted over the wireless medium.

### MD5 Algorithm:

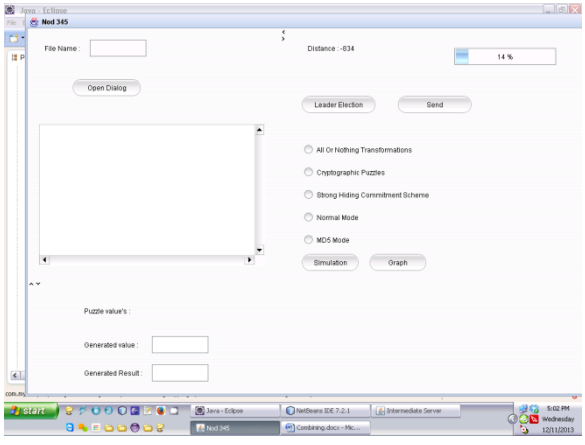
When a password is encrypted by a hash algorithm the resultant is called hashed password. This type of transmission is always a subject of interception by the hackers. These hashed passwords are passed through the Internet as a data packet. TCP header is a most common part of the data packet. In a TCP header there are six reserved bits which remains always unused. In this paper we propose a new approach to enhance the security of hashed passwords by using the six reserved bits of a TCP header. Here we encrypt the hashed password by a random key using simple mathematical function. The information needed to decrypt the encrypted hashed password is carried by the six bits of TCP header.

### SCREEN SHOTS:

**Inter Mediate Server:** To communicate between Client to Server one medium will work called Inermediate Server.

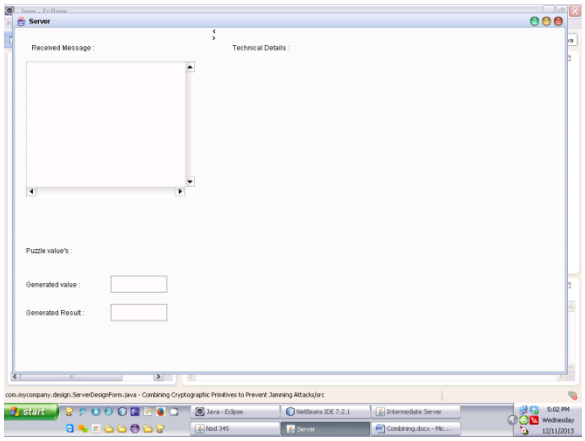



**Node Design:** Before Designing of code some attribute will be work called Field Attribute, So Node Design is used to know about who is Administrator and who is Student, So we have to design first Node.




**Server:** A computer or computer program which manages access to a centralized resource or service in a network.

ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal




## CONCLUSION:

In this paper the problem of selective jamming attacks in wireless networks has been addressed and 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. Showed that the jammer can classify transmitted packets in real time by decoding the first few symbols of an ongoing transmission. Evaluated the impact of selective jamming attacks on network protocols such as TCP and routing and show that a selective jammer can significantly impact performance with very low effort and developed three schemes that transform a selective jammer to a random one by preventing real-time packet classification. Schemes combine cryptographic primitives such as commitment schemes, cryptographic puzzles, and all-or-nothing transformations with physical layer characteristics and analyzed the security of our schemes and quantified their computational and communication overhead. With these schemes a random key distribution has been implemented to more secure the packet transmission in the wireless networks.

## REFERENCES:

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

M. Cagalj, S. Capkun, and J.-P.Hubaux, "Wormhole-Based Anti- Jamming Techniquesin Sensor Networks," IEEE Trans. MobileComputing, vol. 6, no. 1, pp. 100-114, Jan.2007.

A. Chan, X. Liu, G. Noubir, and B. Thapa, "Control Channel Jamming: Resilience a n d I d e n t i f i c a t i o n of Traitors," Proc. IEEE Int'l Symp. Information Theory (ISIT), 2007.

W. Xu, W. Trappe and Y. Zhang, "Anti- Jamming Timing Channels for Wireless Networks," Proc. ACM Co n f . Wireless Network Security (WiSec), pp. 203-213, 2008.

R. Rivest, "All-or-Nothing Encryption and the Package Trans- form," P roc . Int'l Workshop Fast Software Encryption, pp. 210-218,1997.

R. Rivest, A. Shamir, a n d D . Wagner, "TimeLock Pu z z l e s and Timed-Release Crypto," technical report, Massachusetts Inst. of Technology, 1996.

P. Tague, M. Li, and R. Poovendran, "Mitigation of Control Channel Jamming under Node Capture Attacks," IEEE Trans.
Mobile Computing, vol. 8, no. 9, pp. 1221-1234, Sept. 2009.

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