iJRASET
International Journal For Research in
Applied Science and Engineering Technology

# INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

**Volume:** 2 **Issue:** III **Month of publication:** March 2014

**DOI:**

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

ISSN: 2321-9653

INTERNATIONAL JOURNAL FOR RESEARCH IN APPLIED SCIENCE AND ENGINEERING TECHNOLOGY (IJRASET)

# Packet Classification for Preventing Selective Jamming Attacks

Mr.P.Rajkumar, Mrs. J Lekha M.Sc, .M.Phil

*M.Phil* ***Scholar***

*Department of Computer Science*

*Sri Krishna Arts and Science College*

*Coimbatore, India.*

*Assistant Professor Department of Computer Science*

*Sri Krishna Arts and Science College*

*Coimbatore, India*

***Abstract* — The open nature of wireless medium in wireless network leaves it vulnerable to multiple security threats. In this project we investigate the feasibility of real-time packet classification for launching selective jamming attacks, by exploiting knowledge of network protocols and cryptographic primitives extracted from compromised nodes. Our findings indicate that selective jamming attacks lead to DoS with very low effort on behalf of the jammer. To mitigate such attacks, we develop three schemes that prevent classification of transmitted packets in real time. Our schemes rely on the joint consideration of cryptographic mechanisms with PHY-layer attributes. We analyze the security of our schemes and show that they achieve strong security properties, with minimal impact on the network performance.**

***Keywords: Packet Classification, Jamming Attacks, Wireless Network, Denial of Service***

## 1. INTRODUCTION

Wireless networks rely on the uninterrupted availability of the wireless medium to interconnect participating nodes. However, the open nature of this medium leaves it vulnerable to multiple security threats. Anyone with a transceiver can eavesdrop on wireless transmissions, inject spurious messages, or jam legitimate ones. While eavesdropping and message injection can be prevented using cryptographic methods, jamming attacks are much harder to counter. They have been shown to actualize severe Denial-of-Service (DoS) attacks against wireless networks. In the simplest form of jamming, the adversary interferes with the reception of messages by transmitting a continuous jamming signal, or several

Short jamming pulses.

ISSN: 2321-9653

INTERNATIONAL JOURNAL FOR RESEARCH IN APPLIED SCIENCE AND ENGINEERING TECHNOLOGY (IJRASET)

Typically, jamming attacks have been considered under an external threat model, in which the jammer is not part of the network. 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. Conventional antijamming 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 pseudonoise (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. 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. To launch selective jamming attacks, the adversary must be capable of implementing a "classify-then-jam" strategy before the completion of a wireless transmission.

Such strategy can be actualized either by classifying transmitted packets using protocol semantics or by decoding packets on the fly. In the latter method, 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. Selective jamming requires an intimate knowledge of the physical (PHY) layer, as well as of the specifics of upper layers.

In the proposed system here investigate the feasibility of real-time packet classification for launching selective jamming attacks, under an internal threat model. We show that such attacks are network protocols and cryptographic primitives extracted from compromised nodes. We investigate the impact of selective jamming on critical network functions. Our findings indicate that selective jamming attacks lead to DoS with very low effort on behalf of the jammer. To mitigate such attacks, we develop three schemes that prevent classification of transmitted packets in real time. Our schemes rely on the joint consideration of cryptographic mechanisms with PHY-layer attributes. We analyze the security of our schemes and show that they achieve strong security properties, with minimal impact on the network performance.

## 2. LITERATURE REVIEW

In this Chapter, references of previous research that utilized the concepts in Introduction are introduced. An overview of related literature is provided. In section 2.1, Jamming and Sensing of Encrypted Wireless Ad Hoc Networks are Explained. In Section 2.2, Foundations of Cryptography are presented. In Section 2.3 Anti-Jamming Timing Channels for Wireless Networks in Section 2.4, Randomized Differential DSSS: Jamming-Resistant Wireless Broadcast Communication is discussed. In Section 2.5 Client Puzzles: A Cryptographic Countermeasure against Connection Depletion Attacks is analyzed. Finally In Section 2.6 the Feasibility of Launching and Detecting Jamming Attacks in Wireless Networks

### *2.1, Jamming and Sensing of Encrypted Wireless Ad Hoc Networks*

*Author: T.X. Brown, J.E. James, and A. Sethi*

ISSN: 2321-9653

INTERNATIONAL JOURNAL FOR RESEARCH IN APPLIED SCIENCE AND ENGINEERING TECHNOLOGY (IJRASET)

This paper considers the problem of an attacker disrupting an encrypted victim wireless ad hoc network through jamming. Jamming is broken down into layers and this paper focuses on jamming at the Transport/Network layer. Jamming at this layer exploits AODV and TCP protocols and is shown to be very effective in simulated and real networks when it can sense victim packet types, but the encryption is assumed to mask the entire header and contents of the packet so that only packet size, timing, and sequence is available to the attacker for sensing. A sensor is developed that consists of four components. The first is a probabilistic model of the sizes and inter-packet timing of different packet types. The second is a historical method for detecting known protocol sequences that is used to develop the probabilistic models, the third is an active jamming mechanism to force the victim network to produce known sequences for the historical analyzer, and the fourth is the online classifier that makes packet type classification decisions. The method is tested on live data and found that for many packet types the classification is highly reliable. The relative roles of size, timing, and sequence are discussed along with the implications for making networks more secure.

*2.2 Anti-Jamming Timing Channels for Wireless Networks*

*Author: W. Xu, W. Trappe, and Y. Zhang*

Wireless communication is susceptible to radio interference, which prevents the reception of communications. Although evasion strategies have been proposed, such strategies are costly or ineffective against broadband jammers. In this, we explore an alternative to evasion strategies that involves the establishment of a timing channel that exists in spite of the presence of jamming. The timing channel is built using failed packet reception times. We first show that it is possible to detect failed packet events in spite of jamming. We then explore single sender and multi-sender timing channel constructions that may be used to build a low-rate overlay link-layer. We discuss implementation issues that we have overcome in constructing such jamming- resistant timing channel, and present the results of validation efforts using the MICA2 platform. Finally, we examine additional error correction and authentication mechanisms that may be used to cope with adversaries that both jam and seek to corrupt our timing channel.

*2.3 Randomized Differential DSSS: Jamming-Resistant Wireless Broadcast Communication*

*Author: Y. Liu, P. Ning, H. Dai, and A. Liu*

Jamming resistance is crucial for applications where reliable wireless communication is required. Spread spectrum techniques such as Frequency Hopping Spread Spectrum (FHSS) and Direct Sequence Spread Spectrum (DSSS) have been used as countermeasures against jamming attacks. Traditional anti-jamming techniques require that senders and receivers share a secret key in order to communicate with each other. However, such a requirement prevents these techniques from being effective for anti-jamming broadcast communication, where a jammer may learn the shared key from a compromised or malicious receiver and disrupt the reception at normal receivers.

In this paper, we propose a Randomized Differential DSSS (RD-DSSS) scheme to achieve anti-jamming broadcast communication without shared keys. RD-DSSS encodes each bit of data using the correlation of unpredictable spreading codes. Specifically, bit "0" is encoded using two different spreading codes, which have low correlation with each other, while bit "1" is encoded using two identical spreading codes, which have high correlation. To defeat reactive jamming attacks, RD-DSSS uses multiple spreading code sequences to spread each message and rearranges the spread output before transmitting it. Our theoretical analysis and simulation results show that RD-DSSS can effectively defeat jamming attacks for anti-jamming broadcast communication without shared keys.

*2.4 Client Puzzles: A Cryptographic Countermeasure against Connection Depletion Attacks*

*Author : A. Juels and J. Brainard*

ISSN: 2321-9653

INTERNATIONAL JOURNAL FOR RESEARCH IN APPLIED SCIENCE AND ENGINEERING TECHNOLOGY (IJRASET)

Denial-of-service (DoS) attack is one of the most malicious Internet based attacks. Introduction of cryptographic authentication protocols into Internet environment does not help alleviate the impact of denial-of-service attacks, but rather increases the vulnerability to the attack because of the heavy computation associated with cryptographic operation. Nevertheless, many Internet security protocols including SSL/TLS protocol do not consider this aspect. We consider this overlooked issue in authentication protocol design, and propose an effective countermeasure applicable to authentication protocols like SSL/TLS protocol which adopt public-key based encryption to authenticate the server to the client.

*2.5 The Feasibility of Launching and Detecting Jamming Attacks in Wireless Networks*

*Author: W. Xu, W. Trappe, Y. Zhang, and T. Wood*

Wireless networks are built upon a shared medium that makes it easy for adversaries to launch jamming-style at- tacks. These attacks can be easily accomplished by an ad versify emitting radio frequency signals that do not follow an underlying MAC protocol. Jamming attacks can severely interfere with the normal operation of wireless networks and, consequently, mechanisms are needed that can cope with jamming attacks. In this paper, we examine radio interference attacks from both sides of the issue: we study the problem of conducting radio interference attacks on wireless networks, and second we examine the critical issue of diagnosing the presence of jamming attacks. Specially, we propose four deferent jamming attack models that can be used by an adversary to disable the operation of a wireless network, and evaluate their effectiveness in terms of how each method affects the ability of a wireless node to send and receive packets. We then discuss deferent measurements that serve as the basis for detecting a jamming attack, and explore scenarios where each measurement by itself is not enough to reliably classify the presence of a jamming at- tack. In particular, we observe that signal strength and carrier sensing time are unable to conclusively detect the presence of a jammer. Further, we observe that although by using packet delivery ratio we may differentiate between congested and jammed scenarios, we are nonetheless unable to conclude whether poor link utility is due to jamming or the mobility of nodes. The fact that no single measurement is sufficient for reliably classifying the presence of a jammer is an important observation, and necessitates the development

Of enhanced detection schemes that can remove ambiguity when detecting a jammer. To address this need, we propose two enhanced detection protocols that employ consistency checking. The rst scheme employs signal strength measurements as a reactive consistency check for poor packet delivery ratios, while the second scheme employs location information to serve as the consistency check. Throughout our discussions, we examine the feasibility and effectiveness of jamming attacks and detection schemes using the MICA2 Mote platform.

Jamming-style DoS attacks on the physical and data link layer of wireless sensor networks (WSNs) have recently attracted attention. In particular, propose 4 generic jammer models, namely (1) the constant jammer, (2) the deceptive jammer, (3) the random jammer and (4) the reactive jammer. A constant jammer emits a constant noise; a deceptive jammer either fabricates or replays valid signals on the channel incessantly; a random jammer sleeps for a random time and jams for a random time; and lastly, a reactive jammer listens for activity on the channel, and in case of activity, immediately sends out a random signal to collide with the existing signal on the channel. According to the constant jammers, deceptive jammers and reactive jammers are effective jammers in that they can cause the packet delivery ratio to fall to zero or almost zero, if they are placed within a suitable distance from the victims. However these jammers are also *energy-inefficient*, meaning they would exhaust their energy sooner than their victims would when given comparable energy budgets. Although random jammers save energy by sleeping, they are less effective.

ISSN: 2321-9653

INTERNATIONAL JOURNAL FOR RESEARCH IN APPLIED SCIENCE AND ENGINEERING TECHNOLOGY (IJRASET)

## 3. SYSTEM ARCHITECTURE

A system architecture or systems architecture is the conceptual design that defines the structure and/or behavior of a system. An architecture description is a formal description of a system, organized in a way that supports reasoning about the structural properties of the system. It defines the system components or building blocks and provides a plan from which products can be procured, and systems developed, that will work together to implement the overall system.

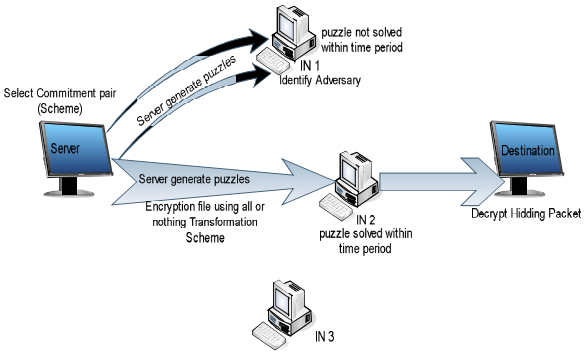



Fig 3.1 System Architecture

*Uml Diagram*

UML stands for Unified Modeling Language which is used in object oriented software engineering. Although typically used in software engineering it is a rich language that can be used to model an application structures, behavior and even business processes.

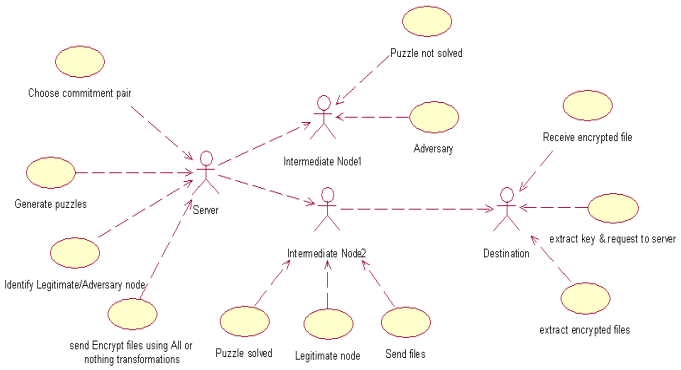



Fig 3.2 Uml Diagram

*Sequence Diagram*

A sequence diagram is a Unified Modeling Language (UML) diagram that illustrates the sequence of messages between objects in an interaction. A sequence diagram consists of a group of objects that are represented by lifelines, and the messages that they exchange over time during the interaction.

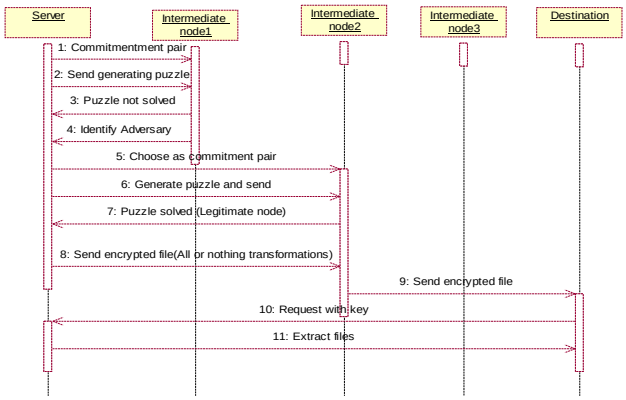



Fig 3.3 Sequence Diagram

ISSN: 2321-9653

INTERNATIONAL JOURNAL FOR RESEARCH IN APPLIED SCIENCE AND ENGINEERING TECHNOLOGY (IJRASET)

## 4. PROBLEM FORMULATION

The goal of system analysis is to determine where the problem is in an attempt to fix the system. This step involves breaking down the system in different pieces to analyze the situation, analyzing project goals, breaking down what needs to be created and attempting to engage users so that definite requirements can be defined.

The methods of systems analysis are necessary to the solution of the aforementioned problems primarily because in the process of making decisions, choices must be made under conditions of uncertainty that result from the presence of factors not subject to strict quantitative evaluation. The procedures and methods of systems analysis are aimed precisely at setting forth alternative variations of a solution to the problem, identifying the scale of uncertainty for each variation, and comparing variations according to particular efficiency criteria. Specialists in systems analysis only prepare or recommend variations of a solution; the decision-making remains within the jurisdiction of the appropriate official or agency.

System Analysis is used in every field where there is a work of developing something. Analysis can also be defined as a series of components that perform organic function together. --in computer world, in this stage a statement of the problem is formulated and a model is built by the analyst in encouraging real-world situation. This phase show the important properties associated with the situation. Actually, the analysis model is a concise, precise abstraction and agreement on how the desired system must be developed. You can say that, here the objective is to provide a model that can be understood and criticized by any application experts in the area whether the expert is a programmer or not.

### *4.1 Existing System*

WIRELESS networks rely on the uninterrupted availability of the wireless medium to interconnect participating nodes. However, the open nature of this medium leaves it vulnerable to multiple security threats. Anyone with a transceiver can eavesdrop on wireless transmissions, inject spurious messages, or jam legitimate ones. While eavesdrop and message injection can be prevented using cryptographic methods, jamming attacks are much harder to counter. They have been shown to actualize severe Denial-of-Service (DoS) attacks against wireless networks.

In the simplest form of jamming, the adversary interferes with the reception of messages by transmitting a continuous jamming signal, or several short jamming pulses. Typically, jamming attacks have been considered under an external threat model, in which the jammer is not part of the network. 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.

Conventional antijamming 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 pseudonoise (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.

*Drawbacks*

- The problem of selective jamming attacks in wireless networks
- Adversaries with internal knowledge of protocol specifications and network secrets can launch

ISSN: 2321-9653

INTERNATIONAL JOURNAL FOR RESEARCH IN APPLIED SCIENCE AND ENGINEERING TECHNOLOGY (IJRASET)

low-effort jamming attacks that are difficult to detect and counter.

- selectively targeting messages of high importance
- selective jamming in terms of network performance degradation

*4.2 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 to severely degrade the throughput of an end-to-end flow.

To launch selective jamming attacks, the adversary must be capable of implementing a "classify-then-jam" strategy before the completion of a wireless transmission. Such strategy can be actualized either by classifying transmitted packets using protocol semantics, or by decoding packets on the fly. In the latter method, 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. Selective jamming requires an intimate knowledge of the physical (PHY) layer, as well as of the specifics of upper layers. 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 with physical-layer characteristics.

*Product Perspective*

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.

*Product Features*

This system we develop three schemes that prevent classification of transmitted packets in real time secure packet transmission. Cryptographic primitives such as commitment schemes, cryptographic puzzles, and all-or-nothing transformations. Detect Adversary node

*Advantages*

- We develop three schemes that prevent classification of transmitted packets in real time
- Cryptographic primitives such as commitment schemes, cryptographic puzzles, and all-or-nothing transformations.
- The server sends one cryptography puzzle to intermediate nodes it solves particular time periods.
- Server first chooses the commitment node regarding to transfer the data to destination.
- Detect Adversary node
- Server can identify the inside attacker and outside attacker.
- Secure packet transmission.

## 5. MODULES

ISSN: 2321-9653

INTERNATIONAL JOURNAL FOR RESEARCH IN APPLIED SCIENCE AND ENGINEERING TECHNOLOGY (IJRASET)

The project contains five modules. They are

Commitment Scheme
Cryptographic Puzzle Scheme
Identify Adversary/Legitimate Node
All or nothing transformations Scheme
Receive hiding packets.

*Modules Description*

## 6. COMMITMENT SCHEME

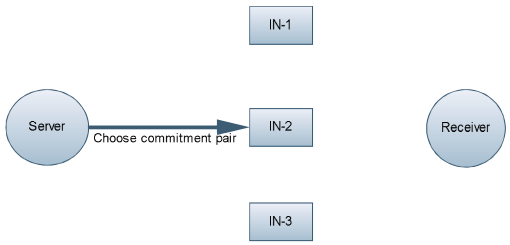



Fig 6.1 Server Choose the commitment Pair

In our context, the role of the committer is assumed by the transmitting node S. The role of the verifier is assumed by any receiver R, including the jammer J. The committed value m is the packet that S wants to communicate to R. To transmit m, the sender computes the commitment/decommitment pair and broadcasts C. The hiding property ensures that m is not revealed during the transmission of C. To reveal m, the sender releases the decommitment value d, in which case m is obtained by all receivers, including J. Note that the hiding property, as defined in commitment schemes, does not consider the partial release of d and its implications on the partial reveal of m. In fact, a common way of opening commitments is by releasing the committed value itself.

For most applications, partial reveal of m with the partial release of d does not constitute a security risk. After all, the committer intends to reveal m by exposing d. However, in our context, a partial reveal of m while d is being transmitted can lead to the classification of m before the transmission of d is completed. Thus, the jammer has the opportunity to jam d instead of C once m has been classified. To prevent this scenario, we introduce the strong hiding property: - Strong hiding. For every polynomial-time party V interacting with A and possessing pairs part, there is no (probabilistic) polynomially efficient algorithm that would allow V associate C with m and C0 with m0, with non-negligible probability. Here, dpart and d0 part are partial releases of d and d0, respectively, and the remaining parts of d and d0 are assumed to be secret. In the above definition, it is easily seen that the release of dpart must be limited to a fraction of d, in order for m to remain hidden. If a significant part of d becomes known to the verifier, trivial attacks, such as brute forcing the unknown bits of d, become possible

## 7. CRYPTOGRAPHY PUZZLE SCHEME

We present a packet-hiding scheme based on cryptographic puzzles. The main idea behind such puzzles is to force the recipient of a puzzle execute a predefined set of computations before he is able to extract a secret of interest. The time required for obtaining the solution of a puzzle depends on its hardness and the computational ability of the solver.

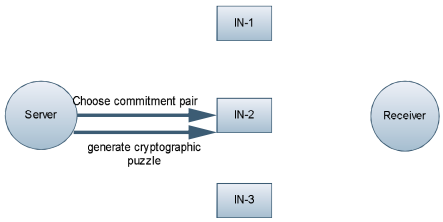



Fig 7.1 Server sends the cryptography puzzle to the intermediate nodes

ISSN: 2321-9653

INTERNATIONAL JOURNAL FOR RESEARCH IN APPLIED SCIENCE AND ENGINEERING TECHNOLOGY (IJRASET)

Identify Adversary/*Legitimate* Node:

Identify the adversary using cryptographic puzzles within the network. When the node can solve the within the time period then the server can be assumed as a legitimate node otherwise adversary node. The cryptographic puzzle is very complicated to solve because it is randomly generated and that solving key known only by the legitimate node. If the server node identify that the node is adversary then it will alter commitment pair and then allocate cryptographic puzzle to commitment intermediate node.

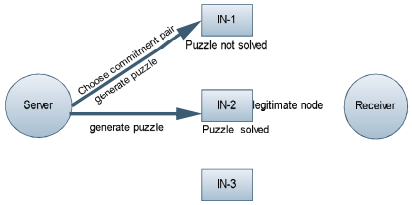



Fig 7.2 Server Identify the Authenticate node

## 8. ALL OR NOTHING TRANSFORMATION SCHEME:

An AONT serves as a publicly known and completely invertible preprocessing step to a plaintext before it is passed to an ordinary block encryption algorithm. A transformation f, mapping message m ¼ fm1; . . .;mxg to a sequence of pseudomessages m0 ¼ fm0 1; . . .;m0 x0g, is an AONT 1) f is a bijection, 2) it is computationally infeasible to obtain any part of the original plaintext, if one of the pseudomessages is unknown, and 3) f and its inverse f_1 are efficiently computable. In our context, packets are preprocessed by an AONT before transmission but remain unencrypted. The jammer cannot perform packet classification until all pseudomessages corresponding to the original packet have been received and the inverse transformation has been applied. At the receiver, the inverse transformation f_1 is applied after all x0 pseudomessages are received, in order to recover m.

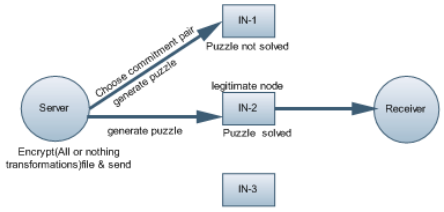



Fig 8.1 Using all or Nothing Scheme for sends packets to destination

## 9. RECEIVE HIDING PACKETS:

When the receiver node receives the all or nothing transformations data and gives proper response to server. Then the receiving packets are extracts in the receiver side. In our proposed system more secure in packet transmission within the network. Our scheme preventing the real time packets transmission by combining the commitment scheme, cryptographic puzzles, all (or) nothing transformations scheme.

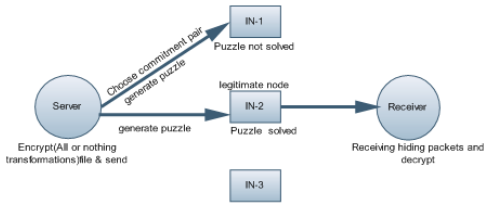



Fig 9.1 Destination user Receive the Packets Securely

## 10. CONCLUSION

We addressed the problem of selective jamming attacks in wireless networks. We considered an internal adversary model in which the jammer is part of the network

ISSN: 2321-9653

INTERNATIONAL JOURNAL FOR RESEARCH IN APPLIED SCIENCE AND ENGINEERING TECHNOLOGY (IJRASET)

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 ongoing transmission. We evaluated the impact of selective jamming attacks on network protocols such as TCP and routing. 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 with physical-layer characteristics. We analyzed the security of our schemes and quantified their computational and communication overhead.

## 11. REFERENCES

[1] 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.

[2] M. Cagalj, S. Capkun, and J.-P. Hubaux, "Wormhole-Based Anti-Jamming Techniques in Sensor Networks," IEEE Trans. Mobile Computing, vol. 6, no. 1, pp. 100-114, Jan. 2007.

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

[4] T. Dempsey, G. Sahin, Y. Morton, and C. Hopper, "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. 2009.

[5] Y. Desmedt, "Broadcast Anti-Jamming Systems," Computer Networks, vol. 35, nos. 2/3, pp. 223-236, Feb. 2001.

[6] K. Gaj and P. Chodowiec, "FPGA and ASIC Implementations of AES," Cryptographic Engineering, pp. 235-294, Springer, 2009. [7] O. Goldreich, Foundations of Cryptography: Basic Applications. Cambridge Univ. Press 2004.

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

And Services (MobiSys), 2008.

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

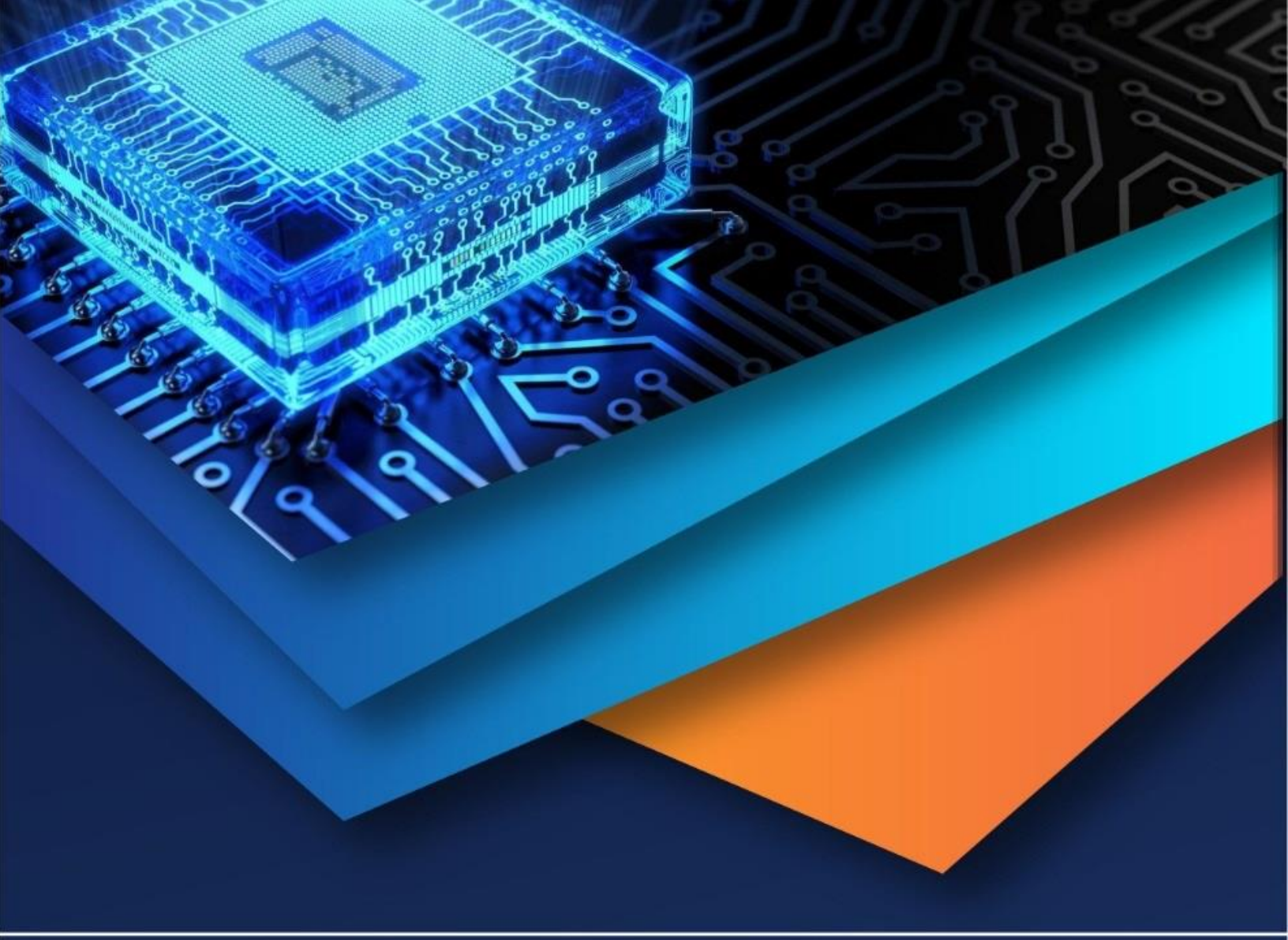
[10] A. Juels and J. Brainard, "Client Puzzles: A Cryptographic Countermeasure against Connection Depletion Attacks," Proc. Network and Distributed System Security Symp. (NDSS), pp. 151-165,

AUTHORS PROFILE

P.Rajkumar,

Completed B.Sc., (Computer Science) and M.Sc, (Computer Science) in Bharathiar University Arts and Science College, Valparai.

And Pursuing M.Phil, (Computer Science) in Sri Krishna Arts and Science College, under the guidance of Mrs. J.LEKHA M.sc, .M.phil Assistant Professor.



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

# INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Call : 08813907089 (24*7 Support on Whatsapp)