Volume 4, Issue 5, May 2014 ISSN: 2277 128X

International Journal of Advanced Research in Computer Science and Software Engineering

Research Paper

Available online at: www.ijarcsse.com

Intelligent Packet Encoding using Crypto Arithmetic Puzzles against Jamming Attack in Wireless Network

Mr.Ugale Pradip[1]
M.Tech. Student,
Dept. of Information Technology,
PCST, Indore, India[1]

Ms.Hemlata Sunhare[2]
Associate Professor,
Dept. of Information Technology
PCST, Indore, India[2]

Mr.Sachin Patel[3]
HOD,
Dept. of Information Technology
PCST, Indore, India[3]

Abstract— Our paper contains techniques to secure packets against jamming attack in wireless network with puzzle loaded packet encoding technique Wireless network never has certain limited boundaries that can't be extended to attempt jamming attack due to this nature security flaws may get developed. The main motive of puzzle loaded packet encoding to force recipient of puzzle to execute predefined set of computations before taking secrets from packets This puzzle loaded drive presents added security which doesn't depend upon physical layer attributes but higher computations required Jammers ability depends on complexity of puzzle and jammers preparedness .

Keywords— Packets, Wireless network, jamming, intelligent encoding

I. INTRODUCTION

Wireless System Description:

In Wireless networks, there cables are not used to connect nodes in wireless network but technology is used to communicate between different nodes .As compared to wired network, wireless network are good because there is no need to introduce cables between different nodes

So it results in less installation cost In wireless network there are technologies used like WiFi, Bluetooth out of Bluetooth is used for smaller distances wireless signals transmitted with Bluetooth cover short distances

Jamming basics

Jamming is used to compromise nodes in wireless environment Its working goes in fake way like jammer ensures authorized users as he is also authorized one 2.4Ghz frequency can easily jammed by good attacker Signals are dropped by good attacker to a level where wireless network no longer works.

Jamming Types

Aim of jamming is to intentionally trying to interference with transmission and reception of message across the wireless channel

Jammer can be divided into following types

1. Constant jammer
   He continuously emits radio frequency signals transmits random bits of data to channel
2. Reactive Jammer
   He remains quite when channel is idle
3. Deceptive Jammer
   He constantly injects series of packets to the channel without any gap between subsequent transmission He also manages broadcasting of fabricated messages and reply old ones
4. Random Jammer
   He changes periods of jamming randomly

Key Points to compare jamming Attacks-

Following are some factors can be used to compare jamming attack

- Energy efficient
- Stealthy
- Strength against Phy. Layer techniques e.g. CDMA
- Strength against error correction module
- Management of behavior close to protocol standards
- Probability of detection

Disadvantages of existing system

1. Broadcast are mostly vulnerable under an internal threat model because all involved receiver must know secret used to protect transmission
2. Due to open nature of wireless medium it becomes vulnerable to intentional interference attacks
3. In this way it is easy to get important data by adjusting with any single receiver

Advantages of proposed system

1. Our results shows that jamming attacks leads to DoS with very low efforts by jamming node
2. Our system implements strong security properties

II. IMPLEMENTATION

Introduction

Due to puzzle key cryptography drive used recipient of a puzzle has to execute predefined set of computations before extracting packets It ensures enhanced added security which not relay on PHY layer attribute but it costs computation cycles .At the time of transmission this puzzle based drive allow to hide packets temporarily which are encrypted and this puzzle is send to receiver or destination jammer gets busy with solving it so he undergoes confusions

and results in failure regarding jamming

In below figure 1 simple communication system is described. At start puzzle is introduced, physical layer packet m is encoded, interleaved and modulated before it is transmitted over the wireless channel at the receiver end puzzle is evaluated then signal is demodulated deinterleaved and decoded to recover original message Adversary ability varies with implemented blocks

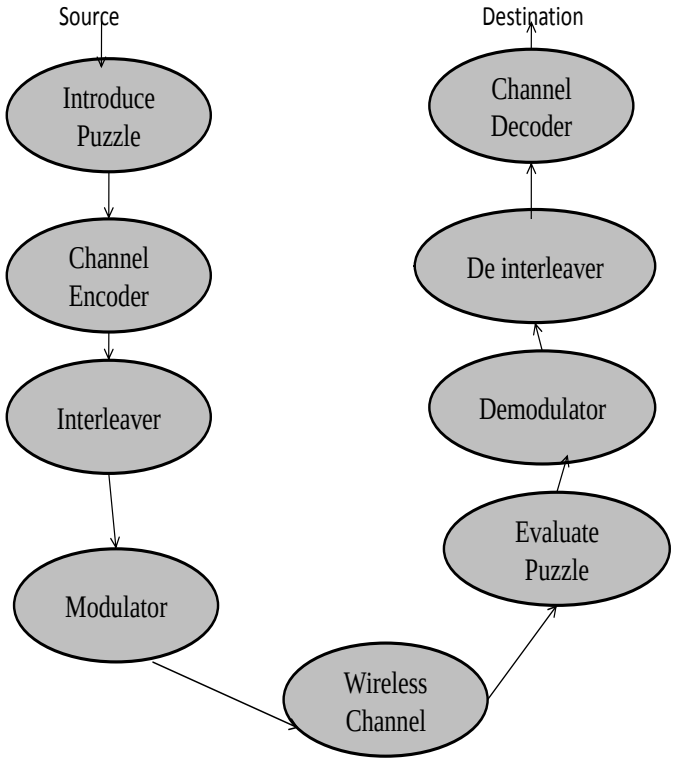

Figure 1: Generic system for communication

Cryptarithametic is science and art of solving and creating crypto arithmetic in this digits are replaced by letters of alphabet or other symbols .If any letter is repeated it is replaced with same digit each time Same digit is never assigned to two different letters so we need to find unique digit corresponding to unique letter

In this project we try to analyze security against jamming attack using cryptoarithamatic problems In cryptoarithamatic letters are substituted by digits in a way so each letter represents a unique digit The main aim is to find satisfactory sequence of digits which are used against all letters of problem which are binded to the condition of arithamatic operation

Let us see how cryptarithamatic problem work? It is a mathematical puzzle in which each letter represents a digit

Rule no 1= e.g. p=7 then pp=77

The main aim is to find value of each letter and it is ensured that no two letters are assigined same letter it is strictly followed

e.g. If p=7 then u=7…… it is not allowed

Rule no 2=

0 value is not assigined or allowded for starting letter

e.g. PRADIP P=0 is not allowed as we go deep in solving cryptoarithamatic problem

We come to know its very challenging and operates in many steps

Description

Let us see one example

SEND+MORE=MONEY

Here in this example M can only be equal to one because according rule when we add two 4 digit numbers their addition should not be more than 10000 and M can't be zero so now we have

SEND +1ORE=1ONEY

So now there two condition to have S+1=10 S must be 9 or 8

, 9 if it does not have carry

, 8 if carry is present

We can search 0 or 9 in doing addition or subtraction A relevant hint to find 9 or 0 we need to find columns containing 2 or 3 identical letters let us see following example

P* +P*=**P*

*S**+*A**=*S**

…….. if A=0, P+P=P

By using said rules we can evaluate –

SEND (9567) +MORE (1085) =MONEY (10652)

Wireless network are used for transferring related data of any kind between more than one nodes that are not physically connected Vulnerability is possible in wireless network due to its shared medium here jammer interrupts the communication between two legitimate users jammer tries to keep medium busy or cause high radio interference at the receiver

More precisely at link level corrupting a single bit in a packet will cause the packet to fail its checksum and be discarded

Jamming victim network is not transmit only activity It requires an ability to detect and identify victim network activity which is called as sensing The broadcast nature of wireless network makes it more susceptible to attack

III. EXPERIMENTAL RESULT

1. Following figure 2 shows average delay E(D) for finishing file transfer as a function of jamming probability which was taken over repeated experiments

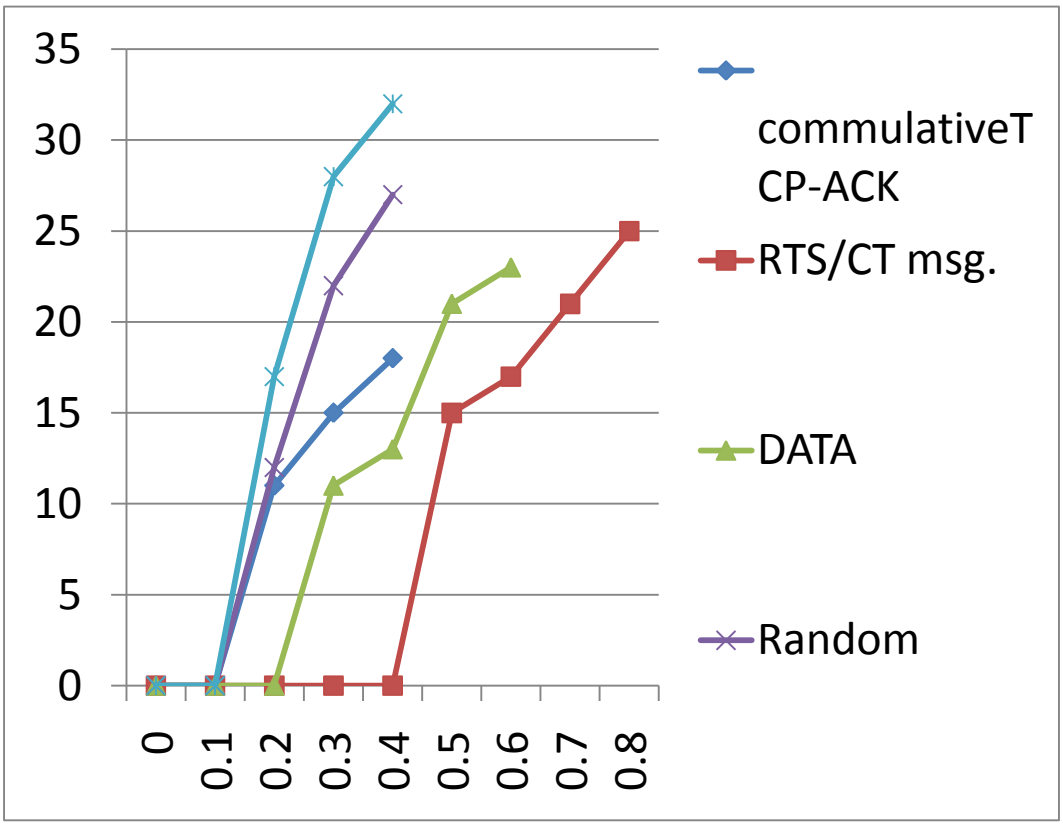

Figure 2: E(D)sec Vs jamming probability

2. Following figure 3 shows average ThroughputE[t] as a function of p for completing the file Transfer as a function of jamming probability P here we can find that all jamming attacks have significant impact on E(d)

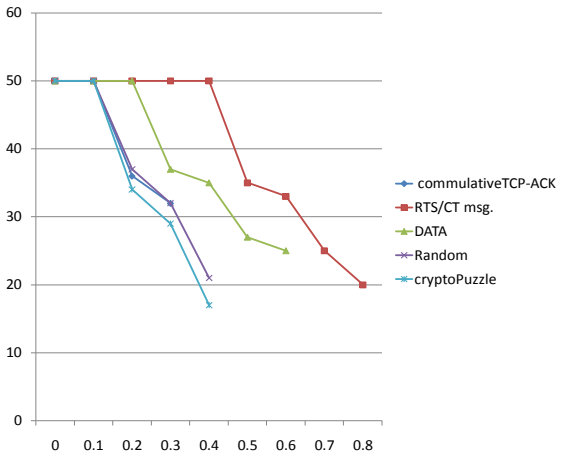

Figure 3:E(t) Vs jamming probability

3. Adversaries jamming ability against for expected values of probability P

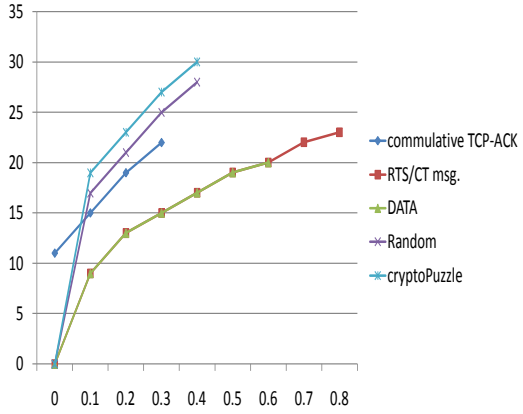

Figure 4: PacketsVs P

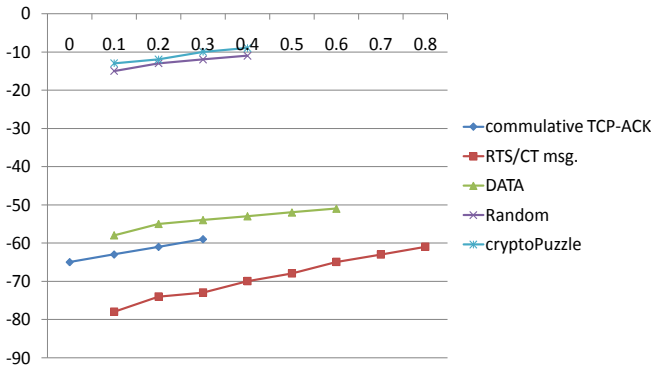

Figure 5: t Vs P

3. Above figure 5 shows how much time jammer remains active while completing the file transfer

IV. CONCLUSIONS

Our system implements strong security methods with security checks using cryptoarithametic puzzles against wireless network This system arranges security by adjusting intelligent packet encoding then interleaving and secure puzzle drive In this way we can add enhanced security measures in wireless network. We can stop performance degradation of network by very low effort by attacker with stated crypto puzzle prevention

REFERENCES

[1] Alejandro ProaE.no ,Loukas Lazos, "Packet-Hiding Methods for Preventing Selective Jamming Attacks", IEEE Transaction on dependable and Secure Computing, VOL. 9, NO.1, JAN-FEB 2012.

[2] M. Strasser, C. P¨opper, and S. ˇCapkun. Efficient uncoordinated Fhss anti-jamming communication. In *Proceedings of MobiHoc*, pages 207– 218, 2009

[3] M. K. Simon, J. K. Omura, R. A. Scholtz, B. K. Levitt "Spread Spectrum Communications Handbook", McGraw-Hill, 2001.

[4] Y. W. Law, M. Palaniswami, L. V. Hoesel, J. Doumen, P. Hartel, P. Havinga, "Energy- efficient link-layer jamming attacks against WSN MAC protocols", AC

[5] M. Wilhelm, I. Martinovic, J. Schmitt, and V. Lenders. Reactive jamming in wireless networks: How realistic is the threat? In *Proceedings of WiSec*, 2011.

[6] M. Wilhelm, I. Martinovic, J. Schmitt, V. Lenders, "Reactive jamming in wireless networks: How realistic is the threat?", In Proceedings of WiSec, 2011.

[7] D. Stinson. *Cryptography: theory and practice*. CRC press, 2006.

[8] A. Juels and J. Brainard. Client puzzles: A cryptographic countermeasure against connection depletion attacks. In *Proceedings of NDSS*, pages 151–165, 1999.

[9] M. K. Simon, J. K. Omura, R. A. Scholtz, and B. K. Levitt. *Spread* Spectrum Communications Handbook.McGraw-Hill, 2001.

[10] Y. W. Law, M. Palaniswami, L. V. Hoesel, J. Doumen, P. Hartel, and P. Havinga. Energy-efficient link-layer jamming attacks against WSN MAC protocols.*ACMTransactions on Sensors Networks*, 5(1):1–38, 2009.

[11] D. Thuente andM. Acharya. Intelligent jamming in wireless networks with applications to 802.11 b and other networks. In Proceedings of the IEEE Military Communications Conference MILCOM, 2006.

[12] T. X. Brown, J. E. James, A. Seth, "Jamming and sensing of encrypted wireless ad hoc networks", pages 120-130, 2006

