International Journal of Research
Available at https://edupediapublications.org/journals
p-ISSN: 2348-6848
e-ISSN: 2348-795X
Volume 04 Issue 03
March 2017

Joint Relay and Jammer Selection for Secure on Relay Networks

V. Swathi Mounika[1], G. Bala Raju [2]

[1]PG Scholar, Dept of CSE, Sri Sunflower College of Engineering and Technology, Lankapalli, Krishna Dist, AP.

[2] Assistant Professor, Dept of CSE, Sri Sunflower College of Engineering and Technology, Lankapalli, Krishna Dist, AP.

Abstract: *To address the problem of jamming under an internal threat model is consider a sophisticated adversary. Jamming attacks is very most urgent threats harming the dependability of wireless communication. Jamming attacks may be used as a certain case of Denial of service (DoS) attacks. Typically jamming has actually been addressed under an external threat model.We state selective jamming attacks are performing real time packet classification in physical layer.The packet loss is identified by Homomorphism Linear Authenticator (HLA) based public auditing method. This setup is implemented in AODV routing protocol with RREQ. This algorithm improves the result of entire Wireless Network by detecting the malicious node and to avoid them and provides reliable transmission in Wireless packet delivery. The jamming attack by JADE Method is used to security our data by using Multi Key Generation algorithm. Jamming Attack Detection is Estimation (JADE) scheme and establishes the hacker Multi Key Generation techniques isproposed in the journalism and it will be explained using through the encryption and decryption multiple key pairs.*

Index Terms: Jamming attacks, Types of jamming attacks, CA, JADE, Denial-of-Service. -HLA, ADR message, Wireless Networks, Packet Classification

1. .INTRODUCTION

Wireless networks arevulnerable to number of security threats is open nature of the wireless medium. Anyone with a transceiver will pay attention to in progress transmissions inject spurious messages, many transmission of authenticate ones [1]. One ways for degrading the network results is by jamming wireless transmissions in the simplest type of jamming the adversary corrupts transmitted messages by causing

electromagnetic interference within the network operational frequencies, and in proximity to the targeted receivers [2]. Link error and small packet dropping is two sources for packet losses in multichip wireless ad hoc network. While observing a sequence of packet losses in the network [3]. We interested in determining whether the losses are caused by link errors only the combined effect of link errors and small drop nodes that are part of the route exploit their knowledge of the communication context to selectively drop a small amount of packets critical to the network performance [4]. Jammers disrupt the wireless communication by generating highpower noise many sources and destination. Since jamming attacks totally corrupt the performance of wireless networks the JADE effective model is required to find their presence and to avoid them. Constant deceptive reactive, intelligent and random jammers isfew jamming techniques used in wireless medium [5].The data destitutionthe wireless network using Multi Key Generation algorithm.We send the secure data by Multi Key Generation algorithm using process. They are Node creation, Key generation, analyzing the attacker node we are explaining the jamming attack using Multi Key Generation algorithm.

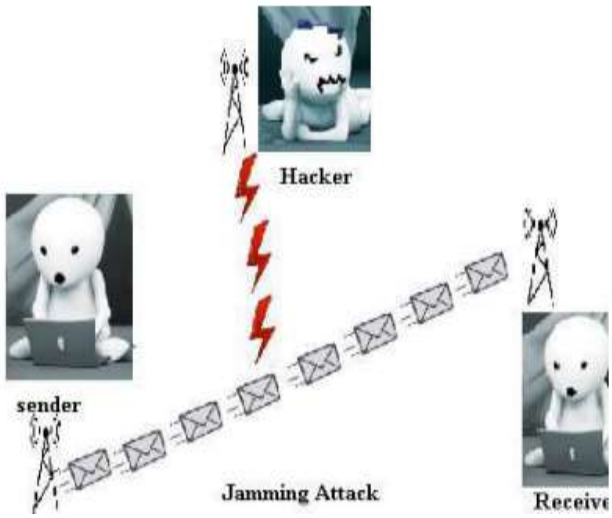
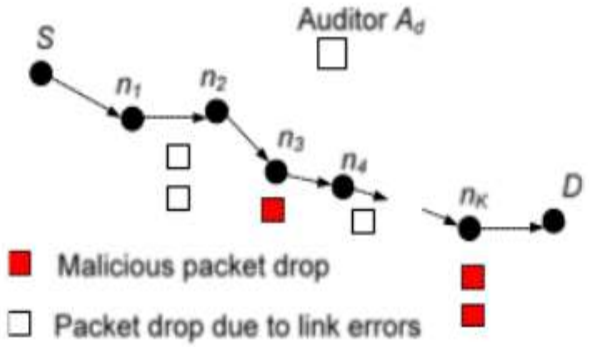


Fig No 1. Jamming Techniques

2. RELATED WORK

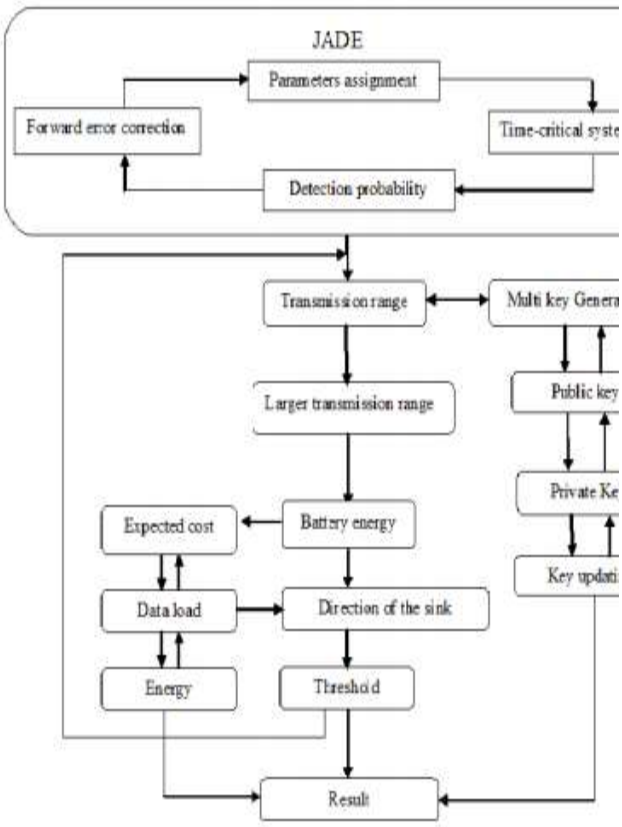
A constant jammer incessantly emits a radio radiation that represents random bits andsignal generator doesn't take any MAC protocol. Sender continuously senses the medium is busy [6]. It always drops the throughput to zero for an extended amount of time till it runs out of energy. Deceptive Jammers Different from the continuous jammers, deceptive jammers is transmit random bits instead they transmit semi-valid packets. They drop the throughput to zero they're not energy efficient. Random jammers on the opposite hand energy efficient a bit less efficient in denying service [7].To launch selective jamming

attacks the jammer needs to be good at implementing a classify then jam policy just is completion of a wireless transmission. Jamming attacks are harder to counter and have now more security problems. Some working jigs have been proven to cause severe Denial-of-Service (DoS)[8] attacks against wireless networks. Within the simplest model of jamming the jammer interferes is reception of messages by transmitting an eternal jamming signal. Under this model jamming methods add the continuous random transmission of high power interference signals [9]. Spread spectrum techniques like the Frequency Hopping Spread Spectrum (FHSS) and the Direct Sequence Spread Spectrum (DSSS) have been used to eliminate the jamming attacks Nevertheless such necessity prevents these techniques from being successful for anti-jamming broadcast communication in which a jammer may find the shared key from a compromised or more possibly from a malicious receiver and interrupt the reception at the normal receivers[10].



3. PROPOSED WORK

A Solution to the Selective jamming attack in wireless network is encryption of packet that is going to send. First symmetric encryption is applied to the packet data except destination. We hide data from adversary [11]. after encryption of data recommitment value that means key is send many message by applying padding functionchange attack alerts and identifying potential attacks and analyzing alerts and other data to diagnose. The proposed system is based on detecting the correlations between the lost packets over each hop of the path. The basic idea is to model the packet loss process of a hop as a random process alternating between 0 (loss) and 1 (no loss). We develop a homomorphism linear authenticator (HLA) based public auditing architecture that allows the detector to verify the truthfulness of the packet loss information reported by nodes [12].



4. CRYPTO-ARITHMETIC PUZZLE

Module Working of this module is same like cryptographic puzzle but only difference is in this method instead of normal keyword for puzzle we use crypto-arithmetic puzzle to hide the key. Crypto-arithmetic is a genre of mathematical puzzles in which the digits are replaced by letters of the alphabet or other symbols. Arithmetic puzzle is like SEND + MORE = MONEY.

A. Algorithm:

Step 1: Scan the input strings.

Step 2: Check that the input is proper.

Step 3: Put the letters or symbols in ARRAY [13].

Step 4: Apply arithmetic rules and try to reduce the solution space.

Step 5: If the number of distinct letter is less than 10, then fill the rest of the indices of ARRAY with don't care symbols. This ARRAY [14] now is our current generation.

Step 6: For manyl times, generate two random numbers m, n and swap the contents of index m and n of any one chromosome of the current generation and copy this new chromosome to the next generation.

B. JADE

This method is intended to control and change Wireless Sensor Network. In principle, JAWS is agent system built on JADE platform it consistsmany agents is communicate with Wireless Sensor Nodes, We are connect the values from particular sensor nodes called motes. We are also take inject mobile code. We can basically change behavior of that mote and in extension of total network. We explain our use of concept of services in our system services is natural and most viable concept in our approach to control and change Wireless Sensor Network [15].

C. ADHOC ON-DEMAND DISTANCE VECTOR (AODV)

AODV routing is an algorithm use for identify route for peer to peer connection many sensors. AODV relies is broadcast route discovery mechanism, which is used to dynamically establish route table entries at intermediate nodes [16]. Each seniors as router and routes is obtain only when needed. AODV is broadcast route request (RREQ) to all and whoever in the range of the frequency being transmitted is receive RREQ. Any sensor which meets the data in the RREQ will answer RREQ with route reply (RREP). The sender gets the RREP, it now has the peer-to-peer connection and ready to send.

5. RESULTS

In this section the impact of the jamming network is analyzed. The results are plotted as X-graph. The parameters like Route discovery time, throughput, based on hiding methods comparison graphs are to taken from trace file of the output and graphs are plotted.

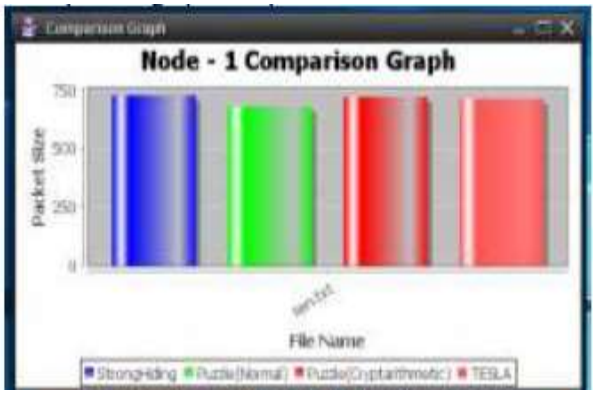


Fig 4: hiding method comparison

Proposed method is less time to detect the packets data between arriving and displaying every packet on the screen. Proposed system uses robust normal distribution in order to get the statistical feature of the users behavior

6. CONCLUSION AND FUTURE SCOPE

In our proposed system is proved the open nature of the wireless medium leaves it vulnerable to intentional interference attacks, number of referred to as jamming. And also this intentional interference with wireless transmissions is used as a launch pad for mounting Denial-of-Service attacks on wireless networks. Even carefully user-customized applications isvulnerable due to incorrect defaults limitations in the visualizations themselves and weaknesses in the overall system. To help counter these attacks this system is better speed to

compare existing models in terms of attack stopping and packets hiding is take Jamming Attack Detection based on Estimation (JADE) scheme is used to identify jamming attack and used to detect jammer. We use multi key generation for security of our message from hacker then we send secured file to destination. Variety of jamming attacks is high and proposed methods detection rate is low and applying multi key knowledge elected to the jammers finally find best results for energy, PDR (Packet Error Rate), Detection rate, Detectionprobability many models remain to be explored in our future work.

7. REFERENCES

[1] T. X. Brown, J. E. James, and A. Sethi. Jamming and sensing of encrypted wireless ad hoc networks. In Proceedings of MobiHoc, pages 120–130, 2006.

[2] Selective Jamming Attacks in Wireless Networks. Alejandro Proano, LoukasLazos. 2010. s.l. : IEEE ICC, 2010.

[3]. C. Wang, Q. Wang, K. Ren, and W. Lou, "Privacy-preserving public auditing for data storage security in cloud computing," in Proc.IEEE INFOCOM Conf., Mar. 2010,.

[4]. Y. Zhang, L. Lazos, and W. Kozma, "AMD: Audit-based misbe-havior detection in wireless ad hoc networks," IEEE Trans. Mobile Comput., PrePrint, Vol. 99, published online on 6 Sept. 2013.

[5]. Z. Liu,H.Liu,W.Xu, and y. Chen, "Exploiting Jamming-Caused Neighbor Changes for Jammer Localization" IEEE,2012 vol. 23,no. 3,pp.547-555.

[6] Selective Jamming Attacks in Wireless Networks. Alejandro Proano, LoukasLazos. 2010. s.l. : IEEE ICC, 2010.

[7] An Improved Detection Method for Different Types of Jamming Attacks in Wireless Networks. Bo Yu, Lu-Yong Zhang. 2014. s.l. : IEEE 2nd International Conference on Systems and Informatics, 2014, pp. 553-558.

[8] Enhanced Packet Dissembling Schemes for Selective Jamming Attacks Prevention in Wireless Networks PushphasChaturvedi, International Journal of Scientific and Research Publications, Volume 3, Issue 6.

[9] M.Wilhelm, I.Martinovic ,J.Schmitt, and V.Lenders. Reactive Jamming in Wireless Networks: How realistic is the threat? In proceddings of Wisec, 2011.

[10] Mr. PushphasChaturvedi Mr. Kunal Gupta Detection and Prevention of various types of Jamming Attacks in Wireless Networks. In IRACST International Journal of Computer Networks and Wireless Communications, ISSN: 2250-3501 Vol.3, No2.April 2013.

[11] A Novel Method for Preventing Selective Jamming Attacks in Wireless Networks. Ashrafunnisa, G. Sridevi. Sep - Oct. 2013. 5, Sep - Oct. 2013, International Journal of Modern Engineering Research, Vol. 3, pp. 2827-2830. ISSN: 2249-6645.

[12]. A. Proano and L. Lazos, "Selective jamming attacks in wireless networks," in Proc. IEEE ICC Conf., 2010, pp. 1–6.

[13] Mr. PushphasChaturvedi Mr. Kunal Gupta Detection and Prevention of various types of Jamming Attacks in Wireless Networks.

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

[15]. Zhuo Lu Wenye Wang Cliff Wang," From Jammer to Gambler: Modeling and Detection of Jamming Attacks against Time-Critical Traffic" IEEE 2011.

[16]. C. Wang, Q. Wang, K. Ren, and W. Lou, "Privacy-preserving public auditing for data storage security in cloud computing," in Proc.IEEE INFOCOM Conf., Mar. 2010,.