Volume: 07 Issue: 04 Pages: 2810-2816 (2016) ISSN: 0975-0290

Jamming Attack Detection Using Key Exchange in Wireless Network

R.Maheswari
M.Phil Scholar, Department of Computer Science, Sree Saraswathi Thyagaraja College, Coimbatore-46
Email: ramarajmahes106@gmail.com

S.Rajeswari
HOD of PG, Department of Computer Science, Sree Saraswathi Thyagaraja College, Coimbatore-46
Email: rajeswari75_gopal@yahoo.co.in

ABSTRACT

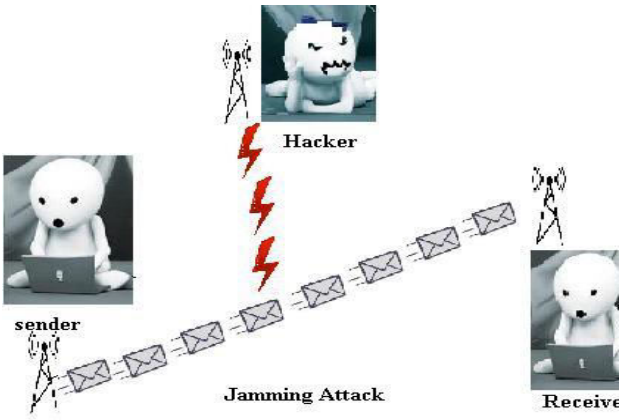
The effort of this article is regarding to detect jamming attacks in wireless networks. The Jamming detection and techniques have been proposed in the journalism. They established results by the authors are often CA and JADE as most of the jamming regions are closely marked, and they do not help to clearly differentiate jamming mechanisms. We explore a different jamming attack by discovering the relationship between five parameters. Packet delivery ratio, Total-message-size, Probability detection, Energy, End-To-End Delay and we are using JADE Method for indentifying malicious node. This proposed system used to find out the jamming attack by JADE Method and we used to protect our data by using Multi Key Generation algorithm. Jamming Attack Detection based on Estimation (JADE) scheme and establishes the hacker. Multi Key Generation techniques have been proposed in the journalism and it will be explained using through the encryption and decryption multiple key pairs.

Keywords: Jamming attacks, Types of jamming attacks, CA, JADE, and Multi Key Generation algorithm.

Date of Submission: Feb 05, 2016 Date of Acceptance: Feb 08, 2016

I. INTRODUCTION

Wireless networks make use of shared broadcast medium; they are open to several malicious attacks. Jamming attacker intercepts while data transmission and blocks or jams the legal transmission. Jammers disrupt the wireless communication by generating high-power noise between sources and destination. Since jamming attacks totally corrupt the performance of wireless networks, the JADE effective mechanisms are required to detect their presence and to avoid them. Constant, deceptive, reactive, intelligent, and random jammers are few jamming techniques used in wireless medium. JADE is probabilities detection. Transmission of secure data typically relies on encryption and decryption "keys" generated by complicated algorithms and swapped between sender and receiver so encrypted data can be deciphered. These keys are generally considered secure. The data can be encrypted by the Source node and data can be decrypted by the Destination node properly. The data share by the wireless network using Multi Key Generation algorithm. And we can send the secure data by Multi Key Generation algorithm using these below process. They are Node creation, Key generation, analyzing the attacker node, Encryption/decryption of data, path selection, and performance evaluation. In our paper we are explaining the jamming attack using Multi Key Generation algorithm.



II. EXISTING SYSTEM

Cooperative algorithm and JADE are the existing system in our paper.

2.1 COOPERATIVE ALGORITHM

Cooperative Algorithm is a cooperative multiple antenna technique for improving or maximizing total network channel capacities for any given set of bandwidths which exploits user diversity by decoding the combined signal of the relayed signal and the direct signal in wireless multi hop networks. A conventional single hop system uses direct transmission where a receiver decodes the information only based on the

Volume: 07 Issue: 04 Pages: 2810-2816 (2016) ISSN: 0975-0290

direct signal while regarding the relayed signal as interference, whereas the cooperative diversity considers the other signal as contribution. That is, cooperative diversity decodes the information from the combination of two signals. Hence, it can be seen that cooperative diversity is an antenna diversity that uses distributed antennas belonging to each node in a wireless network. Note that user cooperation is another definition of cooperative diversity. User cooperation considers an additional fact that each user relays the other user's signal while cooperative diversity can be also achieved by multi-hop relay networking systems.

2.2 JADE

This system is intended to control and monitor Wireless Sensor Network. In principle, JAWS is agent system built on JADE platform. It consists of several agents that are able to communicate with Wireless Sensor Nodes. Via communication, we are able to obtain values from particular sensor nodes called motes. We are also able to inject mobile code to each mote so we can basically change behaviour of that mote and in extension of whole network. In this paper we explain our use of concept of services in our system. As will be shown, services are natural and most viable concept in our approach to control and monitor Wireless Sensor Network [2].

III. PROPOSED SYSTEM

This proposed system used to find out the jamming attack by JADE Method and we used to protect data by using Multi Key Generation algorithm. Networking simulation is used to simulate our network performance first we used to generation 60 nodes to simulate. Next the shared key can be generated in both sender and receiver side. We can able to send the data both sender and receiver side it should have the similar shared key. At last we find out the attacker node by using the JADE. And we can send the secure data by Multi Key Generation algorithm using these below process. They are Node creation, Key generation, analyzing the attacker node, Encryption/decryption of data, path selection, and performance evaluation.

3.1 NODE CREATION:

We are creating the 60 nodes for data sending in network simulation. In that 60 nodes we ha e selected one node as sources and another one node as destination nodes are included and additional node for path creation. In the key generation secure share key is created for sources node and destination node. The authentication key is must be similar for sender node and receiver node or otherwise data can't be transfer.

3.2 ANALYZING THE ATTACKER NODE:

We are using JADE Method we indentifying malicious node. JADE is probabilities detection. JADE is Jamming Attack Detection based on Estimation scheme. The following process can be used to indentify malicious node.

1) A process has only two outcomes: the jammer either wins or loses. That is, either the jammer keeps successfully jamming every transmission until the delay is larger than the threshold, or the transmitter successfully delivers the message within the timing constraint [2].

2) The jammer must cumulatively collect the reward, i.e., message delay. Every time he jams a physical transmission, a certain amount of delay contributes to the overall message delay [2].

3.3 PATH SELECTION

After identifies the malicious node, the remaining node are used to creating path for the data sending

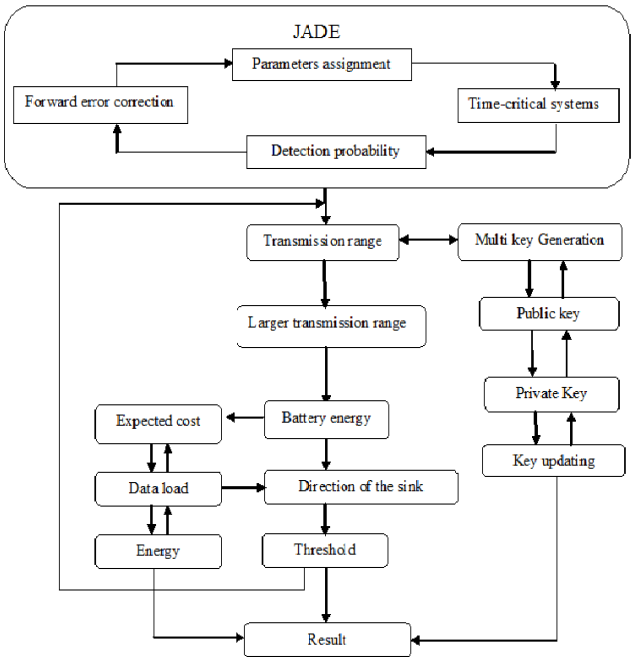
3.4 ENCRYPTION/ DECRYPTION OF DATA

The data can be encrypted by the Source node and data can be decrypted by the Destination node properly. The data share by the wireless network using Multi Key Generation algorithm.

3.5 PERFORMANCE EVALUATION

Using the retreat node we build path for sending the secure data without delay and data loss to the Destination.

3.6 FLOW CHART



Volume: 07 Issue: 04 Pages: 2810-2816 (2016) ISSN: 0975-0290

3.7 MULTI KEY GENERATION

Multi Key generation is the process of generating keys cryptography. A key is used to encrypt and decrypt whatever data is being encrypted /decrypted. Keeping data secret requires keeping this key secret.

Asymmetric key cryptography overcomes the key management problem by using different encryption and decryption multiple key pairs. Having knowledge of multiple key, say the encryption key, is not sufficient enough to determine the other key - the decryption key. Therefore, the encryption key can be made public, provided the decryption key is held only by the party wishing to receive encrypted messages (hence the name public/private key cryptography). Anyone can not use the public key for others public keys and to encrypt a message, only for recipient can decrypt it. This system is sender send the message to the receiver by packets. In that packets messages are encrypted and it will be separated into multiple packets with a key every packets have a secret key every packets can opened by secret key so the hacker can't easily access the packets. In this proposed system is a very less expensive and easily configure and very accurate report can created in this proposed system.

3.7.1 ENCRYPTION PROCESS

Encryption is a formula used to turn data into a secret code. Each algorithm uses a string of bits known as a "key" to perform the calculations. The larger a key is (the more bits in the key), the greater the number of probable combinations that can be created, thus making it harder to break the code and unscramble the contents [1].

- Set the number
- Set dummy symbol
- Combine symbol table and dummy symbol table to symbol table with dummy (STWD)
- Set rotated byte and rotate symbol table with dummy
- Transpose the symbol table after rotation
- Shift the symbol table after transposition
- Complement the symbol table after shift
- Packed control byte table
- Shift the control byte table
- Combine symbol table after
- complement and control byte after shift to
- Get cipher text (CT)

3.7.2 DECRYPTION PROCESS

Decryption is generally the reverse process of encryption. It is the process of coding the data which has been encrypted into a secret format. An authorized user can only decrypt data because decryption requires a secret key or password [1].

- Get the cipher text (CT)
- Separate cipher text into control byte after separation (CBAS) and symbol table after separation (STAS)
- Shift control byte after separation
- Pack control byte after shift
- Complement symbol table after separation
- Shift symbol table after complement
- Transpose the symbol table after shift
- Rotate symbol table after transposition
- Get plaintext (PT).

IV. IMPLEMENTAION

4.1 NETWORK FORMATION

In this network formation we created 60 nodes in the network. Base station is used to Monitoring are shown in Fig 1.

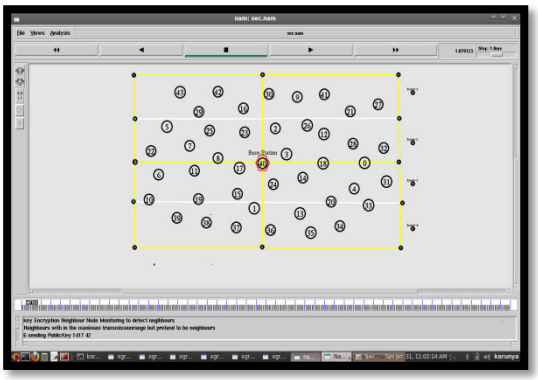


Fig 1 Network Formation

4.2 DETECTION OF MALICIOUS NODE

In this screen it shows node 6 is a source and node 31 is a destination node. First sources send the dummy data to the entire node for analyzing the malicious attack node. After implement the JADE method we identify the malicious nodes. Due to this type of attack the data can loss from source to destination. Malicious nodes are 0, 3, 8, 11, 12, 13, 16&24 shown as Fig 2.

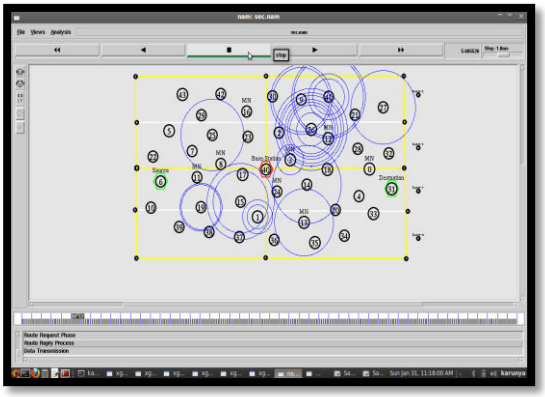


Fig 2 Detection of Malicious Node

Volume: 07 Issue: 04 Pages: 2810-2816 (2016) ISSN: 0975-0290

4.3 DROPPING:

In this screen it shows the energy loss, message dropping.

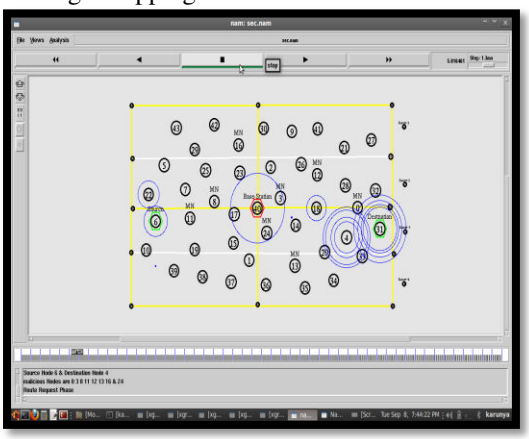


Fig 3 Dropping

4.4 SEARCHING THE NEAREST PATH

In this screen it shows the source and destination finding the shortest path without malicious nodes.

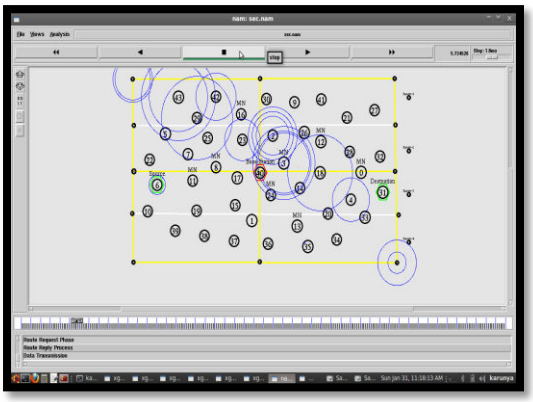


Fig 4 Searching the Nearest Path

4.5 ANALYZING THE NEAREST PATH

In this screen it shows the source and destination find the nearest path. In that path highlighted by Yellow color node (6, 7, 25, 23, 2, 26, 18, 4, 31)as shown in Fig 5.

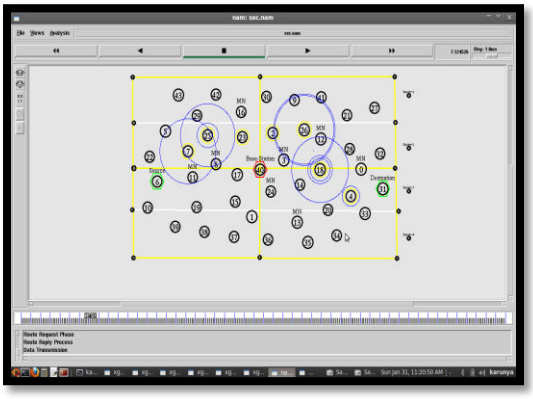


Fig 5 Analyzing the Nearest Path

4.6 ROUT REQUEST PHASE

In this screen it shows, the source is sending the Request frame to destination.

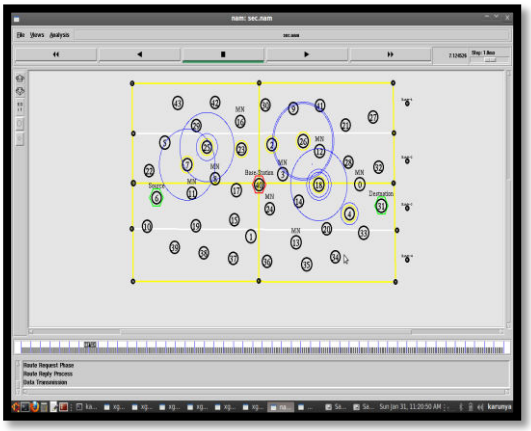


Fig 6 Rout Request Phase

4.7 ROUTE REPLY PROCESS

In this screen it shows the destination sending acknowledgment to source. Before transmitting, a node sends a Request frame to the destination. When the Request arrived to the destination, it replay back to frame if it is not currently busy.

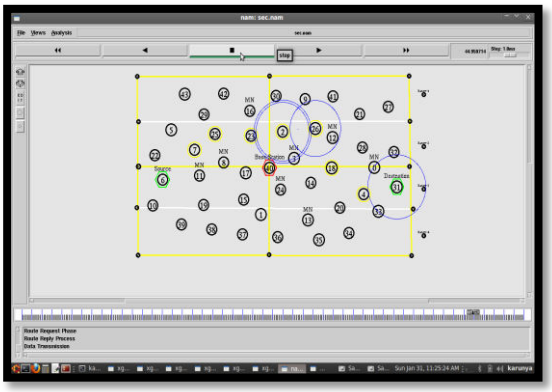


Fig 7 Route Reply process

4.8. DATA TRANSMISSION

In this screen it shows, in that data transmission process the video file split into multiple files using shared key. Allocate the secured key to every spited file. The source encrypted the video file and send to destination. It decrypted video file. If any security key is missing the destination cant received the video file. We are implementing Multi Key Generation Algorithm.

Volume: 07 Issue: 04 Pages: 2810-2816 (2016) ISSN: 0975-0290

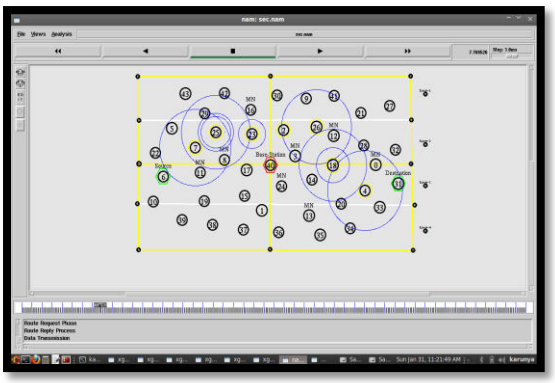


Fig 8 Data Transmission

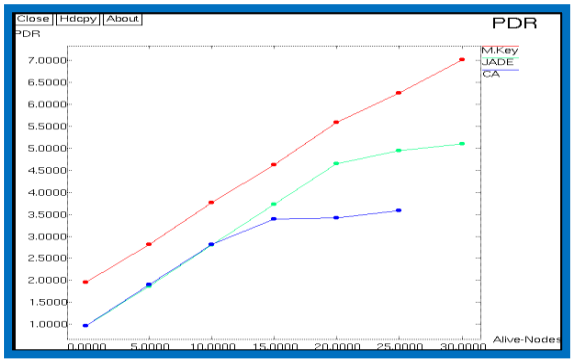
V. PERFORMANCE METRICS

The Network Performance in Simulation environment is measured in Packet delivery ratio, Total-message-size, Probability detection, Energy, And End-To-End Delay.

5.1 PACKET DELIVERY RATIO

It is the ratio can send total number of packets correctly send by sources and total number of packet received by destination. For an environment with noise and interference, the PDR is measured at the receiver side as the ratio of number of packets received using JADE. In general, The Packet delivery ratio is a number of delivered data packet to the destination. This illustrates the level of delivered data to the destination. Multiple key, JADE has better compared to CA (Cooperative Algorithm).

PDR = T.NO Packet Send - T NO Packet Drop
Packet

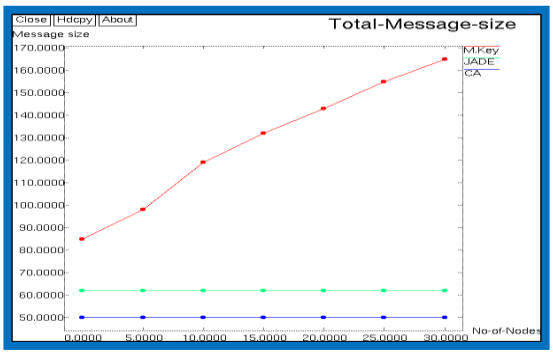


Protocols	Packet Delivery Ratio					
M.KEY	1.960	2.810	3.770	4.620	5.590	6.250
JADE	0.960	1.870	2.800	3.720	4.650	4.950
PER	0.960	1.903	2.815	3.398	3.420	3.580

5.2 TOTAL-MESSAGE-SIZE

In this existing system we can transfer not only text file we can also treansfer video file but its take long time. In that proposed system we using multiple key generation algorithm large data can send,but it takes less time only.In proposed we transfer large video file, in existing we transfer only text file.

Total-Message-Size = PacketSizeX Interaval (Null)
Maximum Packet

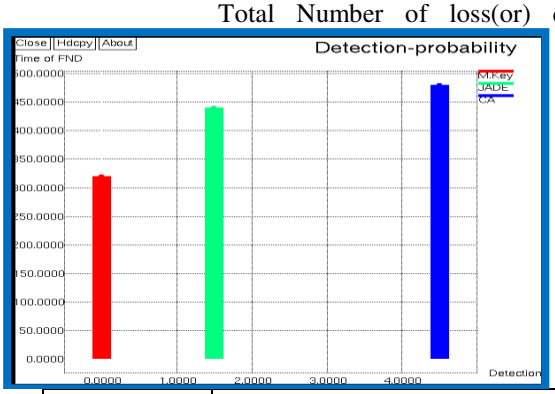


Protocols	Jammers						
M.KEY	85	98	119	132	143	155	165
JADE	62	62	62	62	62	62	62
PER	50	50	50	50	50	50	50

5.3 PROBABILITY DETECTION

In This paper presents a probability-based Jamming Attack Detection based on Estimation (JADE) scheme to select sensor nodes as probe stations by considering the probability distribution of sensor nodes and according to this principle they finding the fault distribution information in wireless networks. Jamming Attack Detection based on Estimation scheme is also used as proposed in this paper. The simulation established that the Multi Key Generation algorithm. The proposed has lower detection probability compared to existing.

Detection probability= ThresholdXPacket
Total Number of loss(or) drop



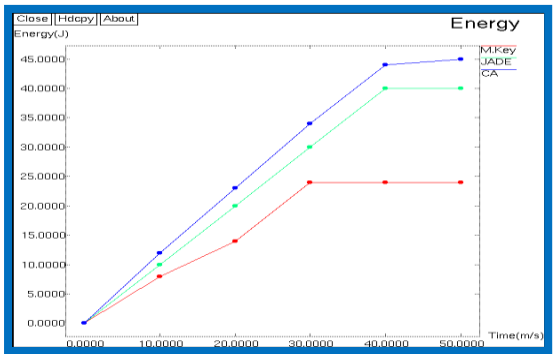
Protocols	**Probability Detection**			
M.KEY	100	200	300	320
JADE	140	240	340	440
PER	180	280	380	480

Volume: 07 Issue: 04 Pages: 2810-2816 (2016) ISSN: 0975-0290

5.4 ENERGY

Energy is a large, complicated line item in every wireless operator's expense budget**.** The energy costs for working a network are huge and the energy consumption has a potentially large. Energy graph is represented. Red & green line shows new energy and blue line shows previous energy. New proposed system takes less energy as compared to the existing system. So, new technique is more efficient.

Energy= Total Number of Packet X Send
Received

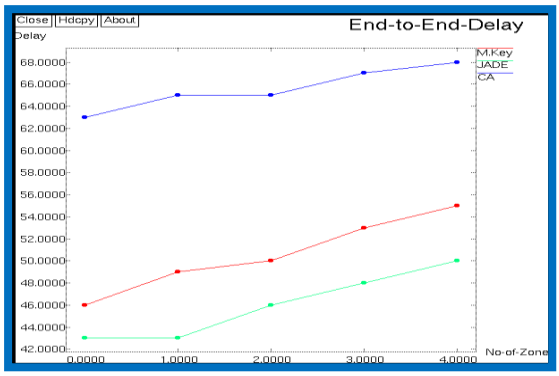


Protocols	ENERGY					
M.KEY	0	8	14	24	24	24
JADE	0	10	20	30	40	40
PER	0	12	23	34	44	45

5.5 ENDS-TO-END DELAY

End-to-end delay is defined as a average time taken by a data packet to arrive in the destination. End-to-end delay Accor data transfer through malicious node. Multiple key, JADE has a lower delay value compare to existing CA (Cooperative Algorithm).In proposed, it take less delay time because it is more power full. In existing, it takes more delay time.

End-To-End Delay = Total No of Packet + Interval
Time



Protocols	End-to-end Delay				
M.KEY	46	49	50	53	55
JADE	43	43	46	48	50
PER	63	65	65	67	68

VI. CONCLUSION

A wireless network needs a wide protection for secure data to transmission. Jamming attack must be discovered in order to save the wireless network. Using with several techniques many researchers try to find the solution. In this paper we discuss about wireless network, jamming attack, types of jammer, how to identify jammer, and we implementing Multi key Generation Algorithm and JADE for sending data without data loss.

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 protect our message from hacker then we can send secured file to destination. We apply the Multi Key Generation Algorithm; the source encrypted the video file and send to destination, It will decrypted video file. If any security key is lost the destination can't received the video file. We exchange shared key for security purpose. Using undisclosed secret keys in spread spectrum is very effective against jammers that have no knowledge to the keys; Variety of jamming attacks is high and proposed methods detection rate is low and applying multi key knowledge elected to the jammers finally identified best results for Energy, PDR (Packet Error Rate), Detection rate, Detection-probability.

REFERNCES

1. http://www.lantronix.com/wp-content/uploads/pdf/Encryption-and-Device-Networking_WP.pdf

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

3. Ali Hamieh and Jalel Ben-Othman, "Detection of Jamming Attacks in Wireless Ad Hoc Networks using Error Distribution", IEEE, 2009

4. 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

Volume: 07 Issue: 04 Pages: 2810-2816 (2016) ISSN: 0975-0290

5. Rui Zhang, Yanchao Zhang and Xiaoxia Huang,"JR-SND: Jamming-Resilient Secure Neighbor Discovery in Mobile Ad Hoc Networks", International Conference on Distributed Computing Systems,2011

6. D.Abirami and R.Venkatesen ," Estimation and Identification of Jamming Attack in Wireless Network" (IJARTET) Vol. II, Special Issue XXV, April 2015

7. Ramya Shivanagu1 and Deepti C2, "A Security Mechanism Against Reactive Jammer Attack In Wireless Sensor Networks Using Trigger Identification Service", IJSPTM, 2013

8. D.J. Thuente and M. Acharya ," Jamming Sensor Networks: Attack and Defense Strategies"2006

9. Geethapriya Thamilarasu, Sumita Mishra and Ramalingam Sridhar,2011," Improving Reliability of Jamming Attack Detection in Ad hoc Networks", (IJCNIS) Vol. 3, No. 1, April 2011

10. Mingyan Li, Iordanis Koutsopoulos, Radha Poovendran," Optimal Jamming Attacks and Network Defense Policies in Wireless Sensor Networks"

11. Rasamalla Naresh and K.Pranav Kumar et al, "Prevention Of Selective Jamming Attacks Using Packet Hiding Methods In Wireless Networks " International Journal of Computer Science and Mobile Computing, Vol.3 Issue.10, October- 2014, pg. 25-28

12. T.Ho, R. Koetter, M.Medard ,D.R.Karger, amd M.E-ros."The bena-ts of coding over routing in a randomized setting" In proc. IEEE International Symposium on Information Theory (ISIT'03), PAGE 441,Yokohama,Japan,2003.

13. B.Parno, A.Perrig and V.Gliogor," Distributed detection of node replication attacks in sensor network" In Proc. 2005 IEEE Symposium on Security and Privacy, Pages 49-63,Oakland,CA,USA,May 2005

14. P.Tangue, M.Li and R. Poovendran," Probabilistic mitigation of control channel jamming via random key distribution" (PIMRC'07),Athens, Greece, September 2007

15. M._Cagalj, S._capkun, and J._P.HUbaux "Wormhole-based anti jamming techniques in sensor networks IEEE Transaction on mobile computing" 2007

16. K.Pelechrfinis, I.Koustsopoulous, I.Broustis, and S.V. Krishamurthy, "Lightweight Jammer Localization in wireless networks: System Design and Implementation," Pro. IEEE GLOBECOM, 2009.

17. A. Wood, J.Stankovic and S.Son," JAM: A Jamming-Area Mapping Service for sensor Network" Proc. 24th IEEE Int'lReal-Time Sytem Symp., 2003

18. Salem M., Sarhan A., Abu-Bakr M., "A DOS Attacks Intrusion Detection and Inhibition Technique for wireless Computer Network", ICGST-CNIR,Volume(7)ISSUE(I),July 2007

19. Wu S.L., Lin C.Y., TsengY.C., Lin C.Y., Sheu J.P., "a Multi- Channel MAC Protocol with Power Control For Multi Hop Mobile Adhoc Network," The Computer J., vol. 45, no.1, 2002. Pp:101-101

20. Mpitziopoulos A., Gavalas D., Pantziou G., "Defending Wireless Sensor Networks from Jamming Attacks", in Proceedings of the 18th Annual IEEE International Symposium on Personal, Indoor and Mobile Radio Communications (Pimrc'07),Athens., Greece, 3-7 September,2007

21. Ali Hamieh, Jalel Ben-Othman, "Detection of Jamming Attacks in Wireless Ad Hoc Networks using Error Distribution", IEEE, 2009.