International Journal of Scientific Research in Computer Science, Engineering and Information Technology
© 2017 IJSRCSEIT | Volume 2 | Issue 4 | ISSN : 2456-3307

Secure Protocol for Jamming Attacks and Time-Delayed Broadcast in Wireless Communications

E. Meena[1], Dr. G. Ravi [2]

[1] Master of Philosophy, Department Of Computer Science, Jamal Mohamed College, Tiruchirappalli, Tamilnadu, India
[2]Associate Professor& Head, Department Of Computer Science, Jamal Mohamed College, Tiruchirappalli, Tamilnadu, India

ABSTRACT

The main aim of this research is to transmit/convey the information from transmitter to the receiver even if there is jammer or a malicious node placed between them. Jammer is a device which emits high power and high bandwidth signal which blocks the low power communication signals. Jammer is designed in such a way to block specific frequency spectrum. The Jammer can block only the signal so this paper which transfers data in the form of time intervals which cannot be blocked. This paper proposes a TDBS, which implements the broadcast operation as a sequence of unicast transmissions scattered in frequency and time. 3DES(Triple Data Encryption Standard) Algorithm which is based on DES, it has been proven reliability and a longer key length that excludes many of the attacks that can be used to lessen the amount of time it takes to break DES. Network Scheduling Algorithm (NSA), which implements the time several network scheduling algorithms have been developed. Network Traffic Analysis is the process of identifying the malicious packets within the traffic. The traffic statistic which is used for understanding and evaluating the network operations.

Keywords: Jammers, Triple Data Encryption Standard (3DES), Network Scheduling Algorithm (NSA), Time-Delayed Broadcast Scheme (TDBS), Network Traffic

I. INTRODUCTION

Network security is defined by the protection to a network from unauthorized access. Network security contains the authorization of access to data in a network, which is controlled by the network administrator. The network contains a collection of nodes connected via wireless links. Nodes may communicate directly or indirectly through multiple hops. It can be communicated both in unicast and broadcast mode. Symmetric keys are shared among all intended receivers in the encrypted broadcast communications. Wireless communications are vulnerable to deliberate interference attacks, generally referred to as jamming. Conventional anti jamming techniques depend on spread spectrum (SS) communications, such as direct sequence spread spectrum (DSSS) and frequency hopping spread spectrum (FHSS). DSSS provides bit-level security by spreading bits according to a secret pseudorandom noise (PN) code, known only to the communicating parties. In FHSS, both the sender and receiver hop synchronously using a secret random frequency hopping (FH) sequence. For jamming-resistant broadcast communications, a common secret to be shared between both the sender and (potentially non-trustworthy) receiver. Receivers decode transferred messages by exhaustively applying each PN code in the public codebook. An advanced adversary with sufficient computation power can block a UDSSS system if it can recover the specific PN code by consuming the public codebook before the termination of the current transmission.

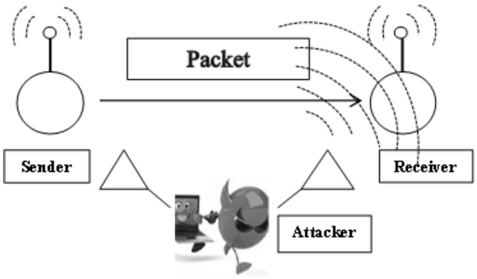


Figure 1. Jamming attack in wireless network

The Time-Delayed Broadcast Scheme (TDBS) as an emergency mechanism for temporarily renovating broadcast communications until inside jammers are physically removed from the network. TDBS varies from classical FHSS designs in that two communicating nodes do not follow the similar FH sequence, but are assigned unique ones. To assure resilience to inside jammers, the locations of these unicast transmissions, defined by a frequency band/slot pair, are only partially known to any subset of receivers. Assuming that the jammer can only interfere with a definite number of frequency bands, a subset of the unicast transmissions are interference-free, thus transmitting broadcast messages.

Some methodologies are projected in this paper Cryptography is a secured system which is used to renovate the text to imperceptible format, which cannot be fragmented easily by the third party. This Mechanism delivers exceptional security to the information which is transmitted to the other user of the communication channel. Triple DES systems are more secure than single DES. It contains both encryption and decryption, networking scheduling algorithm is used for accomplishes the sequence of network packets to transmit and receive queues of the network interface controller. The proposed TDBS propagates broadcast messages as a series of unicast transmissions, widen both in frequency and instance. Network traffic analysis is also a concern in computer security which is used to avoid such attackers who can acquisition important data by monitoring the frequency and timing of network packets.

II. RELATED WORKS

The Jamming attacks are physical layer vulnerability, a refined adversary who manipulates knowledge of the protocol mechanism along with cryptographic quantities extracted from conceded nodes to maximize the effect of his attack on higher-layer functions. C. Popper et al [2] concentrated on a related however distinctive issue for broadcast communication: How to empower robust against jamming broadcast without shared key? Thus the path has been chosen for transferring file from one node to another using network scheduling.

L. Lazos et al [3] proposed new security metrics that quantify the ability of the adversary to deny access to the control channel and the overall delay incurred in re-establishing the control channel until the jammer and the compromised nodes are removed from the network.

M. Strasser et al [4] address and depict the opposition to jamming/key establishment circular dependency issue: against jamming spread spectrum communication procedures depend on a shared key and key establishment depends on a jamming-safe communication. Reactive jammers disrupt legitimate transmission in a more active and versatile manner than non-reactive jammers.

When data is transmitted from one host to another host, an attacker may try to attack the packet or data which is in transit. To avoid such kind of attack in time critical wireless application and transferring the message securely in a wireless application. The main aim of this paper is modeling and detecting jamming attacks against time-critical wireless networks. To extent network performance, packet loss and throughput metrics are used. For the computational process, the performance of time-critical applications, message invalidation ratio metric is used. This approach is inspired by the comparison between the behavior of a jammer who attempts to disrupt the delivery of a message and the behavior of a gambler who intends to win a gambling game [6]

III. PROPOSED METHODOLOGY

In this proposed methodology, the problem of jamming under an internal hazard model. An attacker who is aware of network secrets and the execution details of the network. The attacker uses data for launching selective jamming attacks in which specific messages of high-performance are targeted. There are some methodologies are proposed in this paper. They are,

- 3DES Algorithm (For data encryption and Decryption)

- Network Scheduling Terminology
- Time- Delayed Broadcast Scheme (TDBS)
- Network Traffic Analysis

A. Triple Data Encryption Standard (3DES)

Triple DES (3DES) is termed as a Triple Data Encryption Standard, which is generating the Triple Data Encryption Algorithm (TDEA) symmetric-key block cipher. It uses the Data Encryption Standard (DES) cipher algorithm triple times to each data block.

The original DES cipher's key size of 56 bits was typically sufficient when that algorithm was designed, but the availability of increasing computational power made brute-force attacks feasible. Triple DES which is shown in Figure.1 provides a relatively simple method of increasing the key size of DES to protect against such attacks, without the need to design a completely new block cipher algorithm.

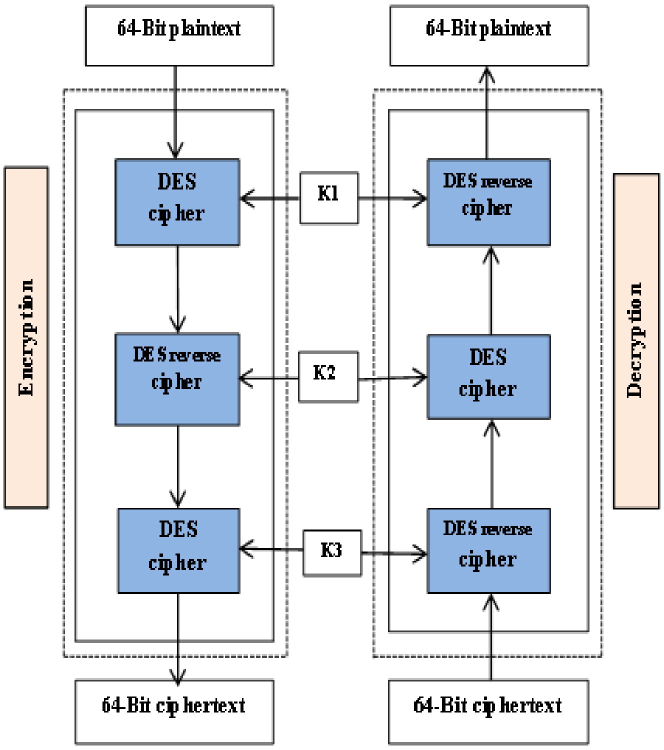


Figure 2. Working principle of Triple DES

Triple DES consists of three keys K_1, K_2 and K_3, each of 56 bits (excluding **parity bits**).

1) Encryption

$$\mathbf{C= E_{K3}(D_{K2}(E_{K1}(plaintext)))}$$

Initially, the 3DES encrypts with K_1, *decrypt* with K_2, and then encrypt with K_3.

2) Decryption

$$\mathbf{P = D_{K1}(E_{K2}(D_{K3}(ciphertext)))}$$

i.e., 3ES decrypt with K_3, *encrypt* with K_2, and then decrypt with K_1.

Each triple encryption encrypts with **one block** of 64 bits of data.

In each case, the middle operation is the reverse of the first and last keys. When using the **keying option** 2 and sends **backward compatibility** with DES with keying option 3 is the strength of the algorithm.

3) Keying Option

The standards describe three keying options:

Keying option 1

All three keys are independent.

Keying option 2

K_1 and K_2 are independent, and $K_3 = K_1$.

Keying option 3

All three keys are same, i.e. $K_1 = K_2 = K_3$.

Keying option 1 is the robust, with 3 × 56 = 168 independent key bits.

Keying option 2 delivers less security, with 2 × 56 = 112 key bits. This option is robust than single DES encrypting twice, e.g. with K_1 and K_2, because it protects against **meet-in-the-middle attacks**.

Keying option 3 is equal to DES, with only 56 key bits. It provides backward compatibility with DES because the first and second DES operations terminate out.

Each DES key is technically stored or transferred as 8 bytes, each of odd parity, so a key bundle requires 24 bytes for option 1, 16 for option 2, or 8 for option 3.

Advantages of 3DES

3DES is easy to implement (and accelerate) in both hardware and software.

- 3DES is pervasive: most systems, libraries, and protocols comprise support for it.

4) 3DES modes

The 3DES implementation unit supports the following nodes

- ECB (electronic code book)
- CBC (cipher block chaining)

In addition to these modes, the DEU can compute Triple-DES. Triple-DES is an extension to the DES algorithm in which every 64-bit input block is sorted out three times.

B. Network Scheduling Terminology

The network scheduler also called as packet scheduler which is used to manage the sequence of network packets.

- **Active queue management (AQM*)*** – the employment of an arbiter program
- **Network traffic control** – an umbrella term for all methods aimed at the control of traffic
- **Traffic shaping** – a form of AQM, where the available bandwidth is being limited to match certain use cases
- **Link sharing** – this term is used when more individuals or customers share the same Internet connection
- **Traffic prioritizing** – a form of AQM, that selectively prioritizes certain network packets (e.g. VoIP-packets)
- **TCP Turbo** – by prioritizing ACK-packets on the upload, a slowdown of the download rate of a TCP connection is prevented
- **Bandwidth management –** the management of the available bandwidth.

C. Time-Delayed Broadcast Scheme

The Time-Delayed Broadcast Scheme (TDBS) as an urgent situation mechanism for temporarily restoring broadcast communications awaiting inside jammers are actually removed from the network. TDBS differs from traditional FHSS designs in that two communicating nodes do not pursue the same FH sequence, but are assigned unique ones. Unlike the distinctive broadcast in which all receivers adjust to the same channel, TDBS propagates broadcast messages as a series of unicast transmissions, widen both in frequency and instance. To ensure resilience to inside jammers, the locations of these unicast transmissions, describe by a frequency band/slot pair, are only moderately known to any subset of receivers.
TDBS can operate in two modes. They are Sequential Unicast mode (SU) and Assisted Broadcast mode (AB).

- TDBS-SU: Sequential Unicast mode
- TDBS-AB: Assisted Broadcast Mode

D. Network Traffic Analysis

Network traffic analysis is the method of recording, reviewing and analyzing network traffic for the purpose of performance, security and/or common network process and management. Network traffic analysis is completed to get in-depth insight into what type of traffic/network packets are flowing over a network. Generally, network traffic analysis is accomplished over a network bandwidth monitoring software/application.

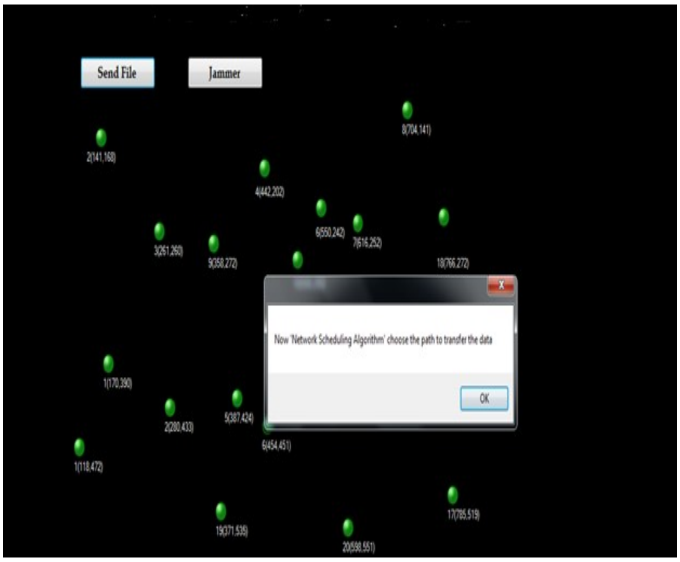
- Understanding and assessing the network utilization
- Download/upload speeds
- Type, size, origin and destination and content/data of packets

Network security staff uses network traffic analysis to classify any malicious or suspicious packets within the traffic. In addition, network administrations seek to observe download/upload speeds, throughput, Network content, etc. to recognize network procedures. Network traffic analysis is used by attackers to scrutinize network traffic models and detect any vulnerability to break in or retrieve sensitive data.

The proposed methodologies are used to secure the data which is transferring from one node to another without depredation and collision attack

IV. EXPERIMENTAL RESULTS

Experimental result demonstrates that the node has been transferring from one node to another through wireless medium with high-level security. The path has been selected for transferring file from one node to another node using network scheduling process which is shown in the Figure.3.



Now 'Network Scheduling Algorithm' choose the path to trandfer the data

Figure.3. Network Scheduling Process

The data has been transferred without any attacks on the wireless medium which is shown in the Figure.4.

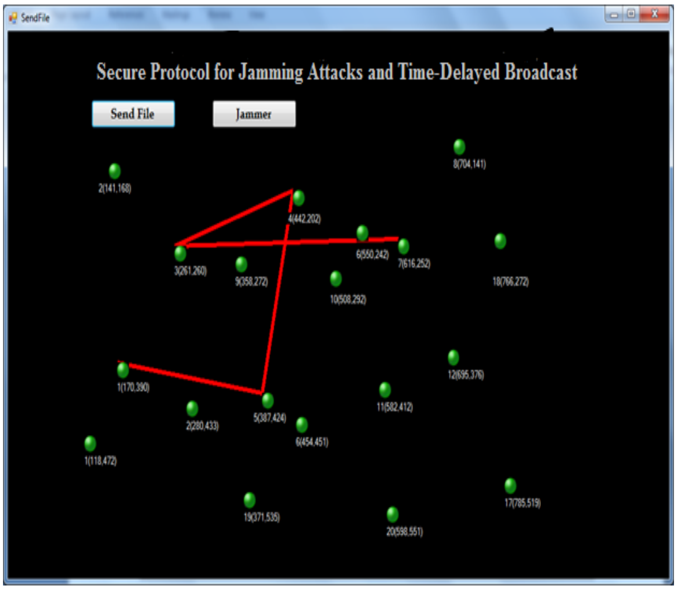
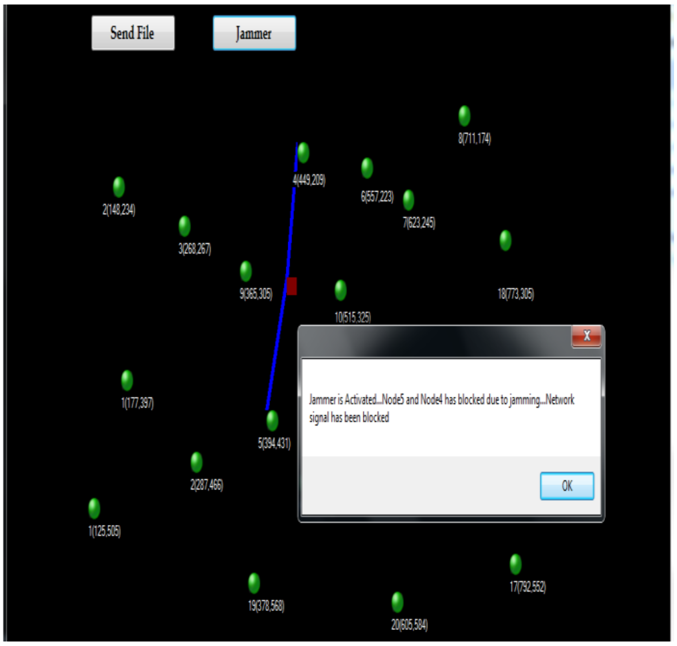


Figure.4. Data Transmission without Jamming Attack

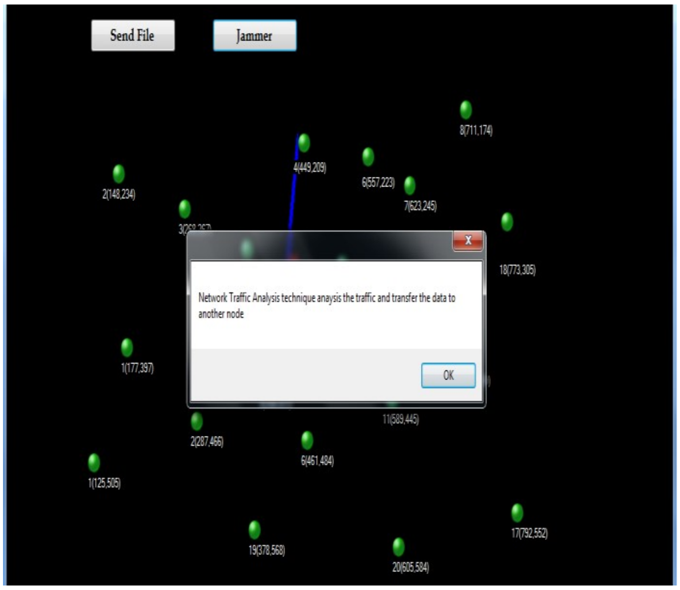
The jammer has been activated while transmission process which is shown in the Figure.5.



Jammer is Activated...Node5 and Node4 has blocked due to jamming...Network signal has been blocked

Figure.5. Jammer Activation

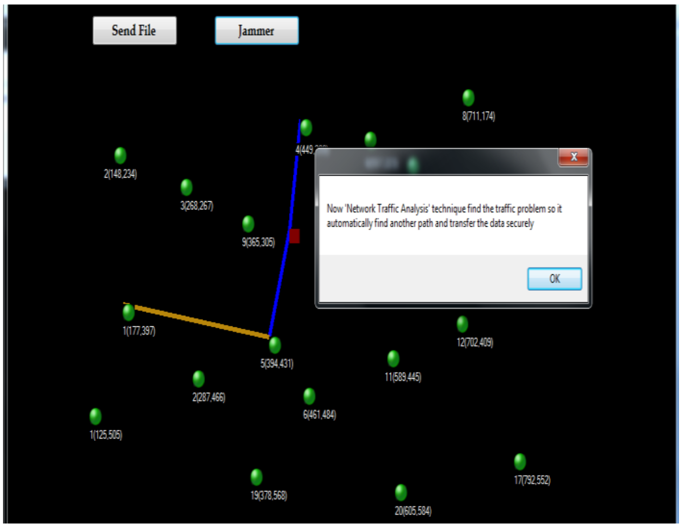
Here, the analysis of network traffic has been performed using the TDBS to avoid time delay in network transmission which is shown in the Figure.6.



Network Traffic Analysis technique anaysis the traffic and transfer the data to another node

Figure.6. Network Traffic Analysis

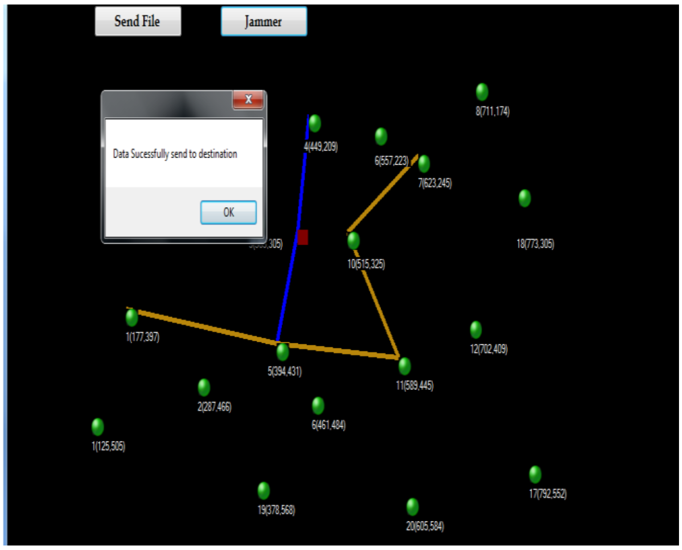
The secured data transmission is processed under network traffic analysis which is shown in the Figure.7.



Now 'Network Traffic Analysis' technique find the traffic problem so it automatically find another path and transfer the data securely

Figure.7. Secure Data Transmission

Finally, the message has been sent successfully to the destination with high-level security which is shown in the Figure.8.



Data Sucessfully send to destination

Figure.8. Successful Message Transmission

Thus the implementation is helpful to achieve the collision-free channel allocation and increase security control and throughput and also avoid packet loss in the wireless network.

V. CONCLUSION

The proposed TDBS, which implements the broadcast operation as a sequence of unicast transmissions scattered in frequency and time. Because the adversary is limited in the number of channels can jam, several unicast transmissions remain interference-free. Triple DES provides high confidentiality, throughput, and low power consumption. In Network scheduling algorithms, the network scheduler accomplishes the buffer and it mapped the problem of accumulating FH sequences for the TDBS to the problem of 1-factorization of complete graphs. Usually, network traffic analysis is performed through a network bandwidth monitoring software or application. The security properties of TDBS is evaluated under both an external and an internal threat model and exposed that TDBS maintains broadcast communications even when multiple nodes are compromised.

VI. REFERENCES

[1]. M. Abdel Rahman, H. Rahbari, and M. Krunz. “Adaptive frequency hopping algorithms for multicast rendezvous in DSA networks”.

[2]. C.Popper, M. Strasser, and S. Capkun. “Jamming-resistant communication without shared keys”, in symposium on Security and Privacy, 2009.

[3]. L. Lazos, S. Liu, and M. Krunz. “Mitigating jamming attacks in multi-channel ad hoc networks”.

[4]. M. Strasser, S. Capkun, C. Popper, M.Cagalj, “Jamming resistant key establishment using uncoordinated frequency hopping ,”in Proc. IEEE Symp . Security and Privacy, Washington, USA, May 2008, pp. 64-78.

[5]. K. Bian, J. Park, and R. Chen. “A quorum-based framework for establishing control channels in dynamic spectrum access networks”.

[6]. Sivagami.S, Poornima Mohapatra.B, Priya darshini.G.R, Charukeerthy.V.S: ’’Jamming Attack Detection and Evaluating Using Wireless Application”.

[7]. Y. Zhang, G. Yu, Q. Li, H. Wang, X. Zhu, and B. Wang. “Channel-hopping based communication rendezvous in cognitive radio networks”.

[8]. S. Gollakota and D. Katabi. “Zigzag decoding: Combating hidden terminals in wireless networks”.

[9]. Sisi Liu, Loukas Lazos, Marwan Krunz, "Time-Delayed Broadcasting for Defeating Inside Jammers", IEEE Transactions on Dependable and Secure Computing, vol. 12, no. , pp. 351-365, May-June, 2015.

[10]. Y. Liu, P. Ning, H. Dai, and A. Liu. “Randomized differential DSSS: Jamming-resistant wireless broadcast communication.