Volume 8, No. 4, May 2017 (Special Issue)
ISSN No. 0976-5697
International Journal of Advanced Research in Computer Science
REVIEW ARTICLE
Available Online at www.ijarcs.info

An Analytical Survey on Covert Channels in Ad-hoc Wireless Network

Amarpreet Singh
Research Scholar
IKG PTU, Jalandhar, Punjab India
amarmandeep2@gmail.com

Prof.(Dr.) Vijay Dhir
Director R&D, SBBS University
Jalandhar, Punjab, India
drvijaydhir@gmail.com

***Abstract:* - During the past two decades people have been moving from limited access of information to ultimate access of information. To achieve ultimate access, new technology is demanded. Wired connectivity has been introduced since the beginning of computer networks, but the introduction of wireless networks creates a new era of its applications. Basically it frees the devices from hard connections such as wires and cables. Unfortunately it introduces new types of problems. Because of the nature of wireless, anyone can receive and access data as long as they are in the range of the signal. This simple feature makes the wireless system really vulnerable to some attacks. That is why a large number of researchers are interested in the field of wireless security. In this review paper, we will study about covert, techniques of covert and its applications.**

Keywords: - Covert, Ad-hoc wireless network, computer network, cryptography, steganography, watermarking

I. INTRODUCTION

The growth and convergence of technology, computers, and networks have enabled organizations and businesses to develop information-centric processes. With the growing reliance on information and information technology, maintaining the confidentiality of sensitive data stored in computers is paramount to the success and failure of business.

Computer network is unpredictable due to information warfare and is prone to various attacks. Not only wired but wireless communication is also vulnerable to such attacks due to randomness caused by the wireless environment. Factors such as mobility, RF interference, or collision avoidance algorithms can contribute to non-determinism. In particular, nodes in ad-hoc wireless networks have to cooperate with each other in order to accomplish many networking functions as routing and channel access. Moreover current Internet facilities are built on the foundation of standard rules and protocols, which usually allow a considerable amount of "freedom" to their designers which again make the communication vulnerable to various attacks.

Many security measures are suggested to counter these attacks such as cryptography, steganography, watermarking and covert channels. Cryptography hides the contents of the message from an attacker, but not the existence of the message. Steganography and watermarking bring a variety of very important techniques how to hide important information in an undetectable and/or irremovable way in audio and video data. They even hide the very existence of the message in the communicating data. But the covert channel is different from them.

A covert channel is a logical link between two compromised systems through which two end applications can secretly exchange information without being detected. A covert channel remains undetectable to an intermediary, despite the fact that the intermediary may have privileges such as an ability to intercept and observe all communication traffic along this channel. A covert channel is designed to be hidden within the normal communication traffic of a legitimate logical channel, such as TCP or UDP. Secret information is embedded in the legitimate channel packets in such a way that only the end applications can detect and retrieve this information. Anyone else watching the network traffic is unable to detect the presence of such information in the legitimate channel packets.

Covert Channels have been defined for the first time by Lampson in 1973. A path of communication that wasn't designed for [that sort of] communication between two processes. It was authorized to communicate, but not in the way they actually are. [1]

According to 1985 U.S. DoD publication a covert channel is "a communication channel that can be exploited by a process to transfer information in a manner that violates system security policy"[2].

According to Murdoch [3], a covert channel can be described as a communication in a computer system where the sender and the receiver plan to leak information over a channel which is not designed for that communication to take place, in violation of a required access control policy.

G.J. Simmons discussed one of the most common and perhaps the best vehicle for discussing the dynamics of covert communications is found in what is known as the "prisoners' problem" initially by in 1983.[4]

Actually covert channel is a double word communication as it has legitimate use also. At one instance to a particular entity it may act as a threat, alternatively, it can be used as subversive means of achieving confidentiality and maintaining anonymity for another. It can be used to protect privacy or increase security of critical communication. Because a covert channel hides within a legitimate logical channel, it is a very simple yet effective mechanism for exchanging information between two end applications without alerting any firewalls or intrusion detectors on the network. It could offer communication completely hidden from the view of the watchers. For extremely sensitive applications, it may be advantageous to transmit certain data covertly. This provides an additional

CONFERENCE PAPERS
National Conference on Emerging Trends on Engineering & Technology (ETET-2017)
On 21st April 2017
University Inst. of Engg. & Tech. & University Inst. of Computer, SBBS University, Punjab (India)

layer of security to that provided by the different layers of the protocol stack.

Covert channels are best suited for sensitive data and their success rate is high if data burst is small.

II. TYPES OF COVERT CHANNEL

Covert storage channels-Involves the direct or indirect writing to storage location by one process and direct or indirect reading of the storage by another process. They use an attribute of a shared resource (e.g. sectors on a disk, unused bits in a packet header or the payload) that is shared by two subjects/processes at different security levels to send/lead information. [24]

A covert storage channel transfers information through the setting of bits by one program and the reading of those bits by another.

Covert storage channels occur when out-of-band data is stored in messages for the purpose of memory reuse. Examples would include using a file intended to hold only audit information to convey user passwords--using the name of a file or perhaps status bits associated with it that can be read by all users to signal the contents of the file. Steganography, concealing information in such a manner that no one but the intended recipient knows of the existence of the message, is a good example of a covert storage channel.

Covert Timing Channels- They use a temporal or ordering relationship among accesses to shared resources to send/lead information. Examples: packet inter-arrival times of Internet traffic, system paging rate, I/O or network usage rates, process creation rate, and time slice relinquishment.

Covert timing channels convey information by modulating some aspect of system behavior over time, so that the program receiving the information can observe system behavior and infer protected information. In some instances, knowing when data is transmitted between parties can provide a malicious user with privileged information. Also, externally monitoring the timing of operations can potentially reveal sensitive data. For example, a cryptographic operation can expose its internal state if the time it takes to perform the operation varies, based on the state.

Covert channels are frequently classified as either storage or timing channels. Some examples of covert timing channels are the system's paging rate, the time a certain transaction requires to execute, and the time it takes to gain access to a shared bus.

III. RELATED WORKS

Many papers have been published to deal with the matter of covert channel. A number of the existing covert channel algorithms are summarized here:

Storage covert channels often store hidden messages in a particular section of covert traffic and the covert receiver checks the corresponding section to obtain the hidden message. On the other hand, timing covert channel uses the timing characteristics of the system to transmit the message [11]. For example, delay times between the packets can be used for this purpose, and the hidden receiver recognizes the messages by observing the behavioral signs of hidden transmitter [11].

Communication can be done steadily in the VANET network with the establishment of Covert channels between those nodes [38]. If the covert channel is established in the VANET network, then the security is maintained between High profile vehicle and Security provider vehicle and can share secret data covertly with each other and the attacker or you can say that the other vehicles that are present in this network can't detect the covert channels. Covert channels can be established into two ways: Covert Storage channel and Covert Timing channel [38]. Utilizing the unused fields of the packets for covert channel establishment has been widely investigated [11]. For example, the ACK frame's destination address field can be used as a medium for covert communication in the IEEE 802.11 protocol [12]. MANET's routing protocols can be considered as another space for covert channel establishment [13]. S.Li and A. Ephremides [13] discuss the use of various features in AODV routing algorithm for covert channel establishment. "Timing of the route request", "source sequence number filed in the route request", "lifetime field of the route reply", and "destination ID field in the route request" are some examples of these features. However, most of these covert channels are statistically detectable and cannot be considered as network steganography. In addition, the firewalls and routers are usually configured to change the unused fields to avoid hidden channels [5].

Timing covert channels are built by manipulation of temporal patterns of the communication networks. In fact, hidden messages are transmitted by controlling the number of events in a period of time. If sufficient security measures, against the statistical analysis, are considered in the design of timing covert channels, the designed method can be considered as network steganography.

Covert channels should be created with the existence assumption of the means for traffic flow's model detection. Therefore, a network steganography method tries to mimic the behavior of overt channels to be less likely detect. For example, model-based covert channels mimic the behavior of real traffic, and they are not easily detected [15, 16]. The proposed method in [15] is based on the extraction of statistical properties of legitimate network traffic, and it is consisted of four parts: filter, analyzer, encoder, and the transmitter. In the filter part, the statistical properties related to the legitimate traffic are extracted, and then in the analyze part, a model, matched to these properties, is used at the encoder and transmitter parts. In [6], a covert channel is designed based on a collision control algorithm. In this study, the hidden message is transmitted by the observed number of collisions over a period of time. A similar method is presented in [7], which is based on the classification tree of the collision avoidance protocol.

Packet retransmission and rate switching approaches are other means for covert channel establishment in wireless networks [8, 17]. In [17], packet retransmission is used to create covert channel. This paper uses the "Retry bit" and "More data" fields for synchronization and the "Destination/ID" field for the covert data transmission. In [8], rate switching of the 802.11 protocol is used for covert

channel creation in wireless networks. The target of the rate switching protocol is to choose a data rate that optimizes the node's performance. The proposed covert channel is established between a workstation and an access point (AP). Access point observes the sequence of data rates and decodes the hidden message accordingly. This covert channel has low bit rate with 100% accuracy in decoding the hidden messages. In [18], the probability distribution of the different data rates in the wireless networks is used as a mean for covert channel detection. Euclidean distance is used to calculate the similarity of the probability distribution of the data rates, used by the covert sender, and the possible data rate probability distributions in a wireless network. And with the use of measured Euclidean distance, the established covert channel will be 100% detectable.

CSMA/CA is an algorithm that is used in 802.11 standard to control the medium access in wireless networks [10]. The main feature of CSMA/CA is the randomness observed in the amount of back-off times, selected by the nodes in the busy channel condition. These random times are used to create covert channels in Covert_DCF [9]. The proposed method uses some fitting symbols to adapt its back-off distribution to an ordinary network performance. As these fitting symbols do not include any covert message, the covert channel's throughput is decreased. In [19], a covert channel is created by mimicking the behavioral characteristics of 802.11 wireless networks that result in low throughput with high level of covertness. The author of [20] creates a hidden channel using QoS features in 802.11e standard. QoS Control field is added to the frame in 802.11e. The combination of three fields of QoS, CF-Poll able, and CF-Poll request is used to create the covert channel. Paper [21] creates covert communication using the time intervals between the packets at the sender. The main goal of this paper is to create a timing channel that is robust against the noise in the network. The noise on such a channel can be the extra times applied between the packets transmission, forced by CSMA/CA. LDPC coding schemes are used to produce robustness against the noise. However, the bandwidth is wasted because of the LDPC usage, and according to the paper, 0.4 bit can be encoded in each packet.

A covert channel creation method in Ad hoc networks is also presented in [22]. This paper uses AODV routing protocol to create covert channel, while OLSR routing algorithm is used between the legitimate nodes in the network. Legitimate nodes discard the corrupted packets in the network, and the covert nodes extract the hidden data from these packets. In [23], the design of a covert channel in a hybrid network (a network that contains different kinds of networks) is proposed. The combination of Wi-Fi and 3G networks is used for this purpose. One network is used to transmit the key and the other to transmit the hidden message. Covert sender uses DES cryptography algorithm to encrypt the hidden message. The used key is transmitted to the hidden receiver with the use of 3G network, but the covert sender transmits the covert data on the Wi-Fi network.

Although the aforementioned covert channel methods create covert communications, they have some drawbacks. Storage covert channels [12] are not secure. They are detectable and can be eliminated from the system. Some other covert channels are secure enough but suffer from low bit rate [8, 13, 20, 23]. The covert channel proposed in [9] sacrifices its bit rate to achieve high security. The methods mentioned in [6, 7] are not practical because they use algorithms that are not practically so common. Some others [8, 17] only care about their long time behavior. Thus, they will be easily detected by short time monitoring of the system behavior. In this paper, a method is proposed to establish a covert channel in IEEE 802.11, which has high security along with high bit rate in comparison with the existing methods.

IV. COVERT TECHNIQUES

Highlights of some techniques that how undisclosed communications can be embedded in covert channels is explained as below:

A. Unused Header Bits: By exploiting protocols, such as TCP/IP, it is possible to encode a covert channel using reserved or unused bits of their headers, as proven in [27]. If there is no confirmation on the receiver or the protocol specifications do not impose explicit values, hidden data can be transmitted, (e.g. in "type of service" field of the IP header). In figure 1 we can see TCP/IP header and their exploitable fields, marked as underlined.

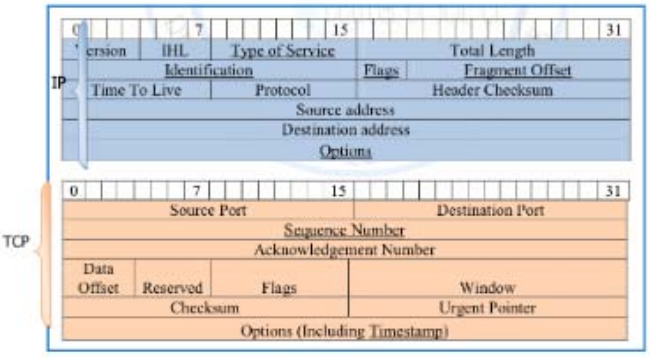

Figure 1. TCP/IP Header Structure (from [26])

Another possible exploit regards padding bits. Again, if the no specific value is imposed for padding, information can be covert within those bits.

B. Optional Header Fields: In spite of the usage of predefined header extensions regarding discretionary information transport on requisition, several protocols consent unheralded data to be carried in header extensions in order to augment the proficiency of protocols. One simple example is to covert masked data as an IP address in route record option.

C. Semantic Overloading of Header Fields: A different approach regarding covert techniques is the semantic overloading. It consists of exploiting syntactic variations of the overt channel to encode covert data whilst the channel is maintained semantically identical. For example, hidden content can be encoded using TCP sequence numbers in TCP header. In order to do it, the client chooses the ISN

CONFERENCE PAPERS
National Conference on Emerging Trends on Engineering & Technology (ETET-2017)
On 21st April 2017
University Inst. of Engg. & Tech. & University Inst. of Computer, SBBS University, Punjab (India)

(Initial Sequence Number), and it should be carefully chosen to prevent new incarnations sequence numbers to overlap with the ISNs previous ones. One example of a covert channel created in these circumstances is the use of each ISNs most significant byte, while enforcing the remainders to be set as zero, as proven in [29]. Higher layer protocols, mainly text based ones, like Hypertext Transfer Protocol (HTTP), offer further opportunities. By simply varying the use of upper and lower case, or the amount of spaces interleaving words, covert channel can be created.

D. Packet and Message Sequence Timing: Another technique relies on sequence timing. To establish a covert channel, in every time interval the sender adjusts its packet rate, while on the receiver's side, in order to decode the concealed data, he needs to measure the rate of the packets in each time interval. However, packet timing channels required synchronization mechanisms at both, sender and receiver sides, in order to alter the packet rate and obtain proper readings at the destination.

E. Payload Tunneling: This technique consists of using the payload tunneling one protocol into another. The major goal of this approach is to bypass firewalls responsible for restraining outgoing transmissions to a brief set of authorized application protocols, such as HTTP. Such methods can even be applied to Domain Name Server (DNS), tunneling information through the protocol. In this case, the client would request a name resolution for the host in the form of host.covertserver.com, where covertserver.com would be a modified DNS server participating in the covert channel, and host would be encoded covert data. All the covert information would be sent from the DNS server to the client in the DNS responses as text records.

V. APPLICATIONS OF COVERT CHANNELS

Applications of covert channels with some practical implementations are given below:

A. Covert Communication with skype: Skype is currently one of the most used P2P communication systems with a number of users of around 35 million [30]. Using the IP protocol, skype communication is made in an high cryptographic manner. Such communication aims to guarantee privacy for skype users, but it also covers said communication from firewalls as they usually do not verify ciphered contents and therefore creates an ideal ambient for covert communication. Skype uses the UDP protocol for communications and, as as many other protocols, it is susceptible to covert techniques, such as network covert storage channels through packet field manipulation. In [25], the authors successfully used skype's 70 bit packets, that do not carry speech, to conceal communications success-

fully. Such exploit is due to skype's method of transmitting data. Even though no dialog is being performed, like text or audio communication, skype continuously send data packets during the session time, as explained in [30].

B. Covert Communication in Social Networks: With facebook's acceptance and usage spreading worldwide, it became a craved target for covert channels. Such exploitation was performed in [28]. In this article, the authors have successfully implemented means to use social networks as a pipe for covert communications, specifically targeting facebook. The authors created an application, named FaceCat which operates based on users facebook accounts. Firstly, the software reaches for long-term cookies stored in cache. After successfully retrieved said cookies, the software starts to operate as an authenticated facebook user.

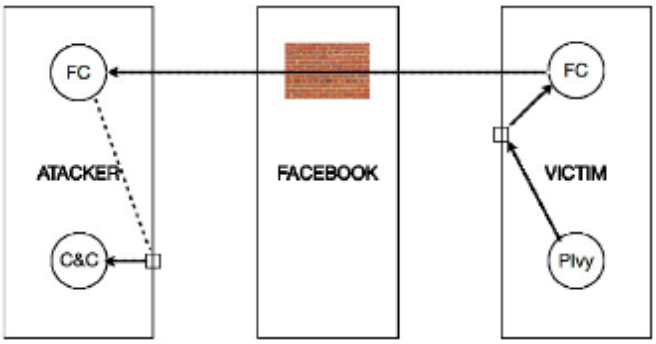

Figure 2. FaceCat operation method (from [28])

By manipulating cookies, a TCP session is established between the master node wall, the "attacker", and unrelated account walls, the "victims". The master node writes its own cookie on his wall, and awaits for connections. FaceCat is now able to read the cookie and, using a method, which authors called "pass-the-cookie", gain the ability to write on master's wall. Communications works using Base64 encoding as well as sequence numbers. The authors choose facebook's mobile interface as it was easier to parse and obtain the encoded messages and use Poison Ivy as a Remote Administration Tool (RAT), with the purpose of interpreting concealed data.

C. Covert Communication in TCP/IP: We must start this discussion by firstly introducing some concepts regarding TCP/IP. TCP/IP is a computer networking model and a set of communication protocols widely used on the Internet. It is composed by the TCP protocol for reliable communication and IP protocol for routing functions. The protocol's header is the combination of both, TCP and IP. In [27], Craig H. Rowland successfully implemented undisclosed communications using TCP/IP packet headers, adopting three different approaches.

a) Manipulation of the IP Identification Field: TCP/IP uses the IP identification field to reassemble packet ordering at the destination node. If - by some reason - a packet was to be lost along the way, the destination router would be aware of the lack of such packet and could not reconstruct data accurately until a retransmission of the packet would be received. By using a simple method of placing the ASCII representation of the characters he wished to encode in the identification field, Rowland managed to pass the word "HELLO" hidden, being subsequently reconstructed at the destination node. This method consists of having the client host to build a packet with the correct destination host,

encoded IP ID field and data regarding the source host. The remote host, while listening on a passive socket, receives the packet and decodes the information. Although effective, this implementation is easily detectable by firewalls and there is a high probability of losing data due to the need of packet overwriting by routers (TTL for example).

b) Initial Sequence Number Field: The second approach taken by the author consists in modifying the Initial Sequence Number Field. This field is used in the three-way handshake implemented by TCP in order to establish a reliable protocol negotiation with a remote server. It comes as an ideal field to conceal communications as it has a reserved 32 bit size. As in the previous example, the author encapsulates ASCII coding that refers to a given character in this field. They define the communication as a synchronized communication and encapsulate the ASCII code, taking in account the generation of more realistic sequence numbers through divisions.

c) The TCP Acknowledge Sequence Number Field "Bounce": Finally, the author refers to a third and last method entitled as The TCP Acknowledge Sequence Number Field "Bounce". In this method, the author uses basic IP spoofing (packet manipulation in order to forge the sender IP address) and bouncing technique (using IP spoofing, a packet is sent to a given server that then replies with an ACK/SYN with ISN +1). Basically, a packet is created with forged source IP address, port, destination IP address (the target system), destination port and a TCP SYN number forget with the data they wish to transmit. Then, it is sent to a bounce server that receives the packet, increments ISN by one number and replies to the forget IP address in the packet. The receiver system expects communication from the bounce server and when received, it interprets the ISN number minus one and therefore the ASCII value of the character.

VI. COVERT TECHNIQUES FOR SECURITY

A. RSA Algorithm: RSA is an algorithm used by modern computers to encrypt and decrypt messages. It is an asymmetric cryptographic algorithm. Asymmetric means that there are two different keys. This is also called public key cryptography, because one of them can be given to everyone. The other key must be kept private. It is based on the fact that finding the factors of an integer is hard (the factoring problem). RSA stands for Ron Rivest, Adi Shamir and Leonard Adleman, who first publicly described it in 1978. A user of RSA creates and then publishes the product of two large prime numbers, along with an auxiliary value, as their public key. The prime factors must be kept secret. Anyone can use the public key to encrypt a message, but with currently published methods, if the public key is large enough, only someone with knowledge of the prime factors can feasibly decode the message.

B. DES Algorithm: The Data Encryption Standard is a symmetric-key algorithm for the encryption of electronic data. Although now considered insecure, it was highly influential in the advancement of modern cryptography. It is developed in the early 1970s at IBM and based on an earlier design by Horst Feistel, the algorithm was submitted to the National Bureau of Standards (NBS) following the agency's invitation to propose a candidate for the protection of sensitive, unclassified electronic government data. In 1976, after consultation with the National Security Agency (NSA), the NBS eventually selected a slightly modified version (strengthened against differential cryptanalysis, but weakened against brute force attacks), which was published as an official Federal Information Processing Standard (FIPS) for the United States in 1977.

The publication of an NSA-approved encryption standard simultaneously resulted in its quick international adoption and widespread academic scrutiny. Controversies arose out of classified design elements, a relatively short key length of the symmetric-key block cipher design, and the involvement of the NSA, nourishing suspicions about a backdoor. The intense academic scrutiny the algorithm received over time led to the modern understanding of block ciphers and their cryptanalysis.

DES is now considered to be insecure for many applications. This is mainly due to the 56-bit key size being too small; in January 1999, distributed.net and the Electronic Frontier Foundation collaborated to publicly break a DES key in 22 hours and 15 minutes (see chronology). There are also some analytical results which demonstrate theoretical weaknesses in the cipher, although they are infeasible to mount in practice. The algorithm is believed to be practically secure in the form of Triple DES, although there are theoretical attacks. The cipher has been superseded by the Advanced Encryption Standard (AES). Furthermore, DES has been withdrawn as a standard by the National Institute of Standards and Technology.

C. AES Algorithm: The National Institute of Standards and Technology (NIST) started development of AES in 1997 when it announced the need for a successor algorithm for the Data Encryption Standard (DES), which was starting to become vulnerable to brute-force attacks. This new, advanced encryption algorithm would be unclassified and had to be "capable of protecting sensitive government information well into the next century," according to the NIST announcement of the process for development of an advanced encryption standard algorithm. It was intended to be easy to implement in hardware and software, as well as in restricted environments (for example, in a smart card) and offer good defenses against various attack techniques.

Conclusion and Future Scope

In this review papers we studied covert wireless technique of transferring information and data even in high security without altering the firewall or security contents. We also studied its applications on skype, facebook etc.

It is an emerging and hot topic for researchers. We can make this covert channels and network more secure by implementing new algorithms on the basics of pros & cons of existing algorithms.

References

[1] B. Lampson, "A Note on the Confinement Problem", Communications of the. ACM, vol. 16, no. 10, Oct. 1973, pp. 613-615.

CONFERENCE PAPERS
National Conference on Emerging Trends on Engineering & Technology (ETET-2017)
On 21st April 2017
University Inst. of Engg. & Tech. & University Inst. of Computer, SBBS University, Punjab (India)

[2] National Computer Security Center, US DoD, "Trusted Computer System Evaluation Criteria" , Tech. Rep. DOD 5200.28- STD, National Computer Security Center, Dec. 1985, http://csrc.nist.gov/publications/history/dod85.pdf

[3] Murdoch, S. J., "Covert channel vulnerabilities in anonymity systems", Ph.D. thesis, University of Cambridge (2007), technical report UCAM-CL-TR-706.

[4] G. J. Simmons, "The Prisoners' Problem and the Subliminal Channel", in Proceedings of Advances in Cryptology (CRYPTO), pp. 51–67, 1983.

[5] Goher S, Javed B, Saqib N. Covert channel detection:A survey based analysis, in High capacity optical networks and enabling technologies (HONET), 2012 9th international conference on 2012: 057–065.

[6] Dugo TM, Ephremides A. Covert information transmission through the use of standard collision resolution algorithms. Information Hiding 2000; 1768: 419–433.

[7] Li S, Ephremides A. A covert channel in MAC protocols based on splitting algorithms. Wireless Communications and Networking Conference, 2005 IEEE 2005; 2: 1168–1173.

[8] Calhoun TE, Cao X, Li Y, Beyah R. An 802.11 MAC layer covert channel. Wireless Communications and Mobile Computing 2012; 12(5): 393–405.

[9] Holloway R Beyah R. Covert DCF: A DCF-Based Covert Timing Channel in 802.11 Networks, in Mobile adhoc and sensor systems (MASS), 2011 IEEE 8th international conference on, 2011.

[10] G. I. . W, IEEE 802.11 WG. Part 11: wireless LAN medium access control, IEEE Std 802.11-2007 (Revisionof IEEE Std 802.11-1999), 2007.

[11] Zander S, Armitage GJ, Branch P. A survey of covert channels and countermeasures in computer network protocols. IEEE Communications Surveys and Tutorials 2007; 9: 44–57.

[12] L. Butti and F. Veysset, Wi-fi advanced stealth, Proc. Black Hat US, Aug, 2006.

[13] Li S, Ephremides A. Covert channels in ad-hoc wireless networks. Ad Hoc Networks 2010; 8(2): 135–147.

[14] Cabuk S, Spafford EH, Brodley CE. "Network Covert Channels: Design, Analysis, Detection, and Elimination. Purdue University: West Lafayette, IN., USA, December 2006.

[15] Gianvecchio S, Wang H, Wijesekera D, Jajodia S. Model-based covert timing channels: Automated modeling and evasion, Recent Advances in Intrusion Detection. 2008: 211–230.

[16] Liu Y, Ghosal D, Armknecht F, Sadeghi A-R, Schulz S, Katzenbeisser S. Hide and seek in time-robust covert timing channels. Computer Security-ESORICS 2009; 2009: 120–135.

[17] Christian K, Dittmann J, Lang A, Kühne T. WLAN steganography: a first practical review, Proceedings of the 8th workshop on Multimedia and security 2006: 17–22.

[18] Zhao H, Chen M. WLAN covert timing channel detection. Wireless Telecommunications Symposium (WTS) 2015; 2015: 1–5.

[19] Ahmadzadeh SA, Agnew G. Behavioral mimicry covert communication. Security and Privacy in Communication Networks 2012; 96: 134–153.

[20] Zhao H. Covert channels in 802.11 e wireless networks, in Wireless telecommunications symposium (WTS), 2014: 2014.

[21] Kiyavash N, Koushanfar F, Coleman TP, Rodrigues M. A timing channel spyware for the CSMA/CA protocol. Information Forensics And Security, IEEE Transactions On 2013; 8(3): 477–487.

[22] Salmanian M, Li M. A High Throughput Covert Overlay Network within a MANET, Military communications conference, MILCOM 2013-2013 IEEE 2013: 586-592.

[23] Zhang D, Du P, Yang Z, Dong L. Research on Covert Channels Based on Multiple Networks, Web technologies and applications 2014: 365–375.

[24] L. Qiu, Y. Zhang, F. Wang, M. Kyung, and H. Mahajan, "Trusted computer system evaluation criteria", in National Computer Security Center, Citeseer, 1985.

[25] Wojciech Mazurczyk, Maciej Karas, and Krzysztof Szczypiorski. Skyde: A skype-based steganographic method. arXiv preprint arXiv:1301.3632, 2013.

[26] Asst Prof Dr Ziyad Tariq Mustafa and Authman Waleed Khalid. Packet steganography using ip id.

[27] Craig H. Rowland. Covert channels in the tcp/ip protocol suite. First Monday, 2(5), 1997.

[28] Jose Selvi. Covert channels over social networks. In SANS Institute Reading Room site. SANS Institute, 2012.

[29] Sebastian Zander, Grenville Armitage, and Philip Branch. A survey of covert channels and countermeasures in computer network protocols. Communications Surveys & Tutorials, IEEE, 9(3):44–57, 2007.

[30] Jiangtao Zhai, Mingqian Wang, Guangjie Liu, and Yuewei Dai. Skylen: a skype-based length covert channel.

[31] Dhir, Vijay. "Alchemi.NET Framework in Grid Computing." Proceedings of the 3rd National Conference; INDIACom-2009 Computing For Nation Development at Bharati Vidyapeeth's Institute of Computer Applications and Management, New Delhi. 2009.

[32] Dr. Vijay Dhir, Er. Gagandeep Kaur ,"Execution of cloud using freeware Technology" , International Journal of Engineering Research in Computer Science and Engineering (IJERCSE), Vol 3, Issue 12, pp 22-29, December 2016.

[33] Vijay Dhir, Dr. Rattan K Datta, Dr. Maitreyee Dutta, "Grid Job Scheduling - A Detailed Study", International Journal of Innovative Research in Science, Engineering & Technology Vol.2, Issue 10, October 2013.

[34] Vijay Dhir, Dr. Rattan K Datta, Dr. Maitreyee Dutta, "Nimble@ITCEcnoGrid Novel Toolkit for Computing Weather Forecasting, Pi and Factorization Intensive Problems", International Journal of Computer Engineering & Technology (IJCET) , Vol:3 Issue:3, Dec 2012.

[35] Vijay Dhir, Dr. Rattan K Datta, Dr. Maitreyee Dutta, "Computational Grid based on Alchemi.NET framework", International Conference on Computer, Electrical, and SystemsScience and Engineering, Feb 10, 2009 WCSET 2009: World Congress on Science, Engineering & Technology Hong Kong March 23-25, 2009.

[35] Rakesh Kumar, Vijay Dhir, "Performance Comparison of Routing Protocols in Mobile Adhoc Networks", International Journal of Engineering Science and Technology (IJSET), Vol. 2, Issue 8, pp 3494-3502, August 10.

[37] Er. Amarpreet Singh, Er. Kimi Manchanda, "Establishment of Bit Selective Mode Storage Covert Channel in VANETS", IEEE International Conference on Computational Intelligence and Computing Research, 2015.

[38] Kimi Manchanda, Amarpreet Singh, "Covert Communication in VANETS using Internet Protocol Header Bit", International Journal of Computer Applications, Volume 123, Issue No. 17, August 2015.

CONFERENCE PAPERS
National Conference on Emerging Trends on Engineering & Technology (ETET-2017)
On 21st April 2017
University Inst. of Engg. & Tech. & University Inst. of Computer, SBBS University, Punjab (India)