2011 3rd International Conference on Information and Financial Engineering
IPEDR vol.12 (2011) © (2011) IACSIT Press, Singapore

SUSCEPTIBILTITY OF adhoc protocols To covert channels (AN ANALYSIS AND COUNTERMEASURES)

S. K. INDUMATHI

DEPARTMENT OF M.C.A.
DR. AMBEDKAR INSTITUTE OF TECHNOLOGY
BANGALORE KARNATAKA INDIA

indukarthik2009@yahoo.in

DR. G. M. KADHAR NAWAZ

DIRECTOR, DEPARTMENT OF M.C.A.

SONA COLLEGE OF TECHNOLOGY
SALEM TAMIL NADU INDIA
nawazse@yahoo.co.in

Abstract. Protection against covert security breaches across mobile ad hoc networks is hard to achieve due to the dynamic and decentralized topology of these networks. The covert channels in wireless involves complicated manipulations to convey covert information. Since they are decentralized the style of operations each node has to be handled individually. The routing algorithms had to be designed to dynamically adapt to network topology changes providing correct routes between communicating users in a timely and efficient manner. The paper investigates ad-hoc wireless networks' susceptibility to covert channels that can be formed through manipulating the network protocols which is otherwise very difficult to eliminate or even detect these covert channels. The work also analyses concept of covert channels and investigates susceptibility aspects of some of the ad hoc routing protocols to find out the possible countermeasures.

Keywords: Covert channel, ad hoc protocol, communication models

1. Introduction

As people become increasingly dependent on cell phones and other wireless communicate on links, the development of efficient and economic routing protocols has gained greater focus. The relative capabilities of these protocols is based on their ability to withstand malicious attacks. Protection against covert security breaches across mobile ad hoc networks is hard to achieve due to the dynamic and decentralized topology of these networks. The difficulty of this task is compounded by the inability of an ad-hoc architecture to implement a predefined security architecture or authentication system for the expansion and shrinking of the network. The lack of built-in defense mechanisms raise multiple vulnerability concerns. This work analyses concept of covert channels and investigates susceptibility aspects of some of the ad hoc routing protocols to find out the possible countermeasures.

2. Covert Channel

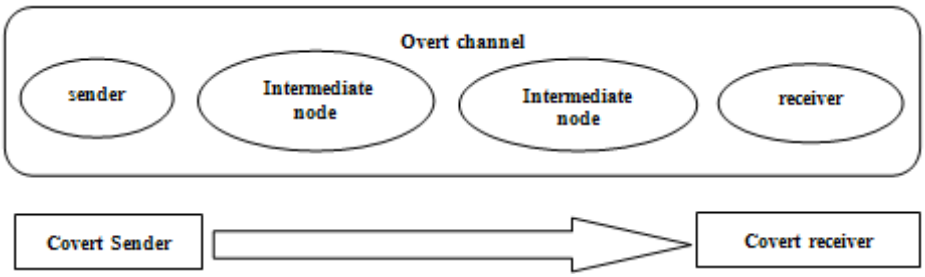
3.1. Covert Channel: Also a Communication Channel!!

A covert channel is defined as any communication channel that can be exploited by a process to transfer information in a manner that violates the system's security policy. In simple, a covert channel is the transfer of data between two processes that are not permitted or not known to be in touch with each other. To set up the channel, the sender and receiver communicate covertly over normal ports, exchanging secret messages using the standard procedure without tipping off neighbor nodes or security monitors as to their behavior. Covert channels are classified into covert storage channels and covert timing channels. Communication in a covert storage channel allows the sender to write the hidden data into a storage location which is not meant for communication which is extracted by the receiver. Communication in a covert timing channel requires that the sender modulates its own system resources such that the manipulation affects the response time observed by the receiver.

3.2. Communication Models

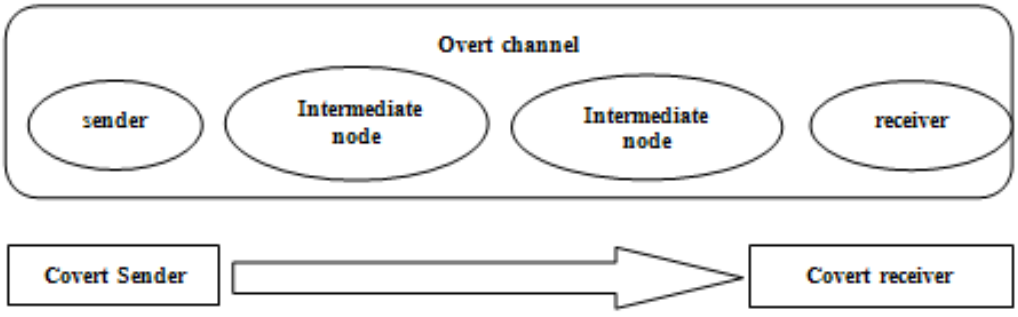
There are a number of scenarios for covert communication between the nodes depending on whether a covert node is a sender or a receiver or acting as an intermediate node manipulating the overt channel between innocent nodes.

- If the sender of the overt channel can also be a sender of the covert channel, and similarly the receiver of the overt channel can also be the receiver of the covert channel. In this case the underlying overt channel is manipulated by the sender and later extracted by the receiver. This is shown in fig-1.



(Fig– 1)

- If the sender has to send some covert data but could not create a new overt channel for this purpose it acts as an intermediate node and embeds its covert channel in to the existing overt channel and transmits the data. But the amount of information that could be sent depends on the maximum capacity of the existing overt channel. But again here the covert receiver can be a middleman where the covert channel is extracted and the overt channel is transmitted to the innocent overt receiver. Here the covert receiver should possibly remove the covert channel preventing possible detection by the receiver or any other intermediate nodes. This is shown in Fig-2.



Covert Channel

(Fig – 2)

3. Covert Channels In Adhoc Networks

The covert channels in wireless involves complicated manipulations to convey covert information. Since they are decentralized the style of operations each node has to be handled individually. The routing algorithms had to be designed to dynamically adapt to network topology changes providing correct routes between communicating users in a timely and efficient manner. The paper investigates ad-hoc wireless networks' susceptibility to covert channels that can be formed through manipulating the network protocols which is otherwise very difficult to eliminate or even detect these covert channels.

3.1. DSR as a adhoc protocol

The Dynamic Source Routing Protocol adopts an on-demand approach of source routing to forward the packets. Each packet sent over DSR carries a header with an ordered source list of the nodes to traverse to reach its destination. Since packets already contain the routing path, intermediate nodes do not need to maintain a current map of the network infrastructure. The packets are left to be loop-free without the usual frequent updates or route advertisements from neighbours. The two most prominent features of DSR are route discovery and route maintenance. Route discovery is initiated through route request packets from a sender to a destination. This on-demand feature allows DSR to be completely self-organizing and self-configuring, making changes only to the routes requested by sending nodes. It has proven useful in eliminating the flood of update messages due to the frequent addition or departing of nodes as in mobile wireless networks. The DSR protocol guarantees that neighbor nodes can safely transfer packets without excessive storage or forwarding overhead, but it does not provide complete informational security.

- During route discovery, the method of covert encryption can be applied to the compromised data is in the route **request identification number**. Each route request message identifies the initiator and target of the Route Discovery, and also contains a unique request identification number (sometimes two), determined by the initiator of the Request. This code number modulo an agreed upon key K could be a code word used to indicate encrypted data.
- The number of **hop limits** could be altered or informative numbers can be added to the hop limit to denote encrypted data.
- The covert data is transmitted through altering the clock times of the data. That is, a message might be sent with a **clock time** several milliseconds off what it should be and this difference can be a significant covert data to the covert receiver.
- With some prior agreement on an algorithm the packets could be sent in a wrong order to convey a covert information.
- All all packets can **piggyback data** onto the message through the options header so that the encoded data could be tripped off by the receiver message without any other nodes noticing.

3.2. AODV as a ad hoc protocol

AODV aims to reduce the amount of route protocol traffic on ad-hoc wireless networks by using on-demand route queries. When a node has to deliver a message, it initiates a route discovery procedure and broadcasts this request to the ad-hoc network. The route request propagates through the network until it reaches the destination node or some intermediate nodes that can provide the reply, provided the network is connected. The route will remain cached in intermediate node routing tables as long as the source continues to send messages. The protocol is susceptible to subversion because the route discovery requests are sent on-demand, at the discretion of the source. As long as the source and destination agree on a covert communication protocol, the source can transmit hidden information at will. There are four covert channels immediately obvious in the use of AODV.

- The first is a classic covert timing channel achieved by timing the requests at an agreed upon interval. For example, two requests sent in a short interval can represent a 1 and a long pause between requests could represent a 0.
- The second channel is implemented by manipulating the source sequence number, which is intended to help establish the route back from the intermediate node to the source. One can either embed the covert character into to sequence number of one route request or increment the sequence number by a specific value in a series of requests in an agreed upon time frame.

- The third channel is the lifetime entry in the routing table indicates when is the last time that the route was used. Receivers of this route reply may derive extra information through looking into how recently the route was used by its constructor.
- The fourth channel is implemented by embedding a covert message in the destination identifier. This covert channel does not require synchronization between the covert transmitter and receiver. Order of reception is enabled through the source sequence number contained in the route request. Plus, the covert information is carried by the route requests which are broadcast in the network.

4. Counter Measures

A timestamp method of pruning would prohibit this situation for the manipulation of cache data by a malicious user from occurring. In addition, downed links known from overhearing transmitted packets should be aggressively pruned from the cache. These methods provide for a greater house-cleaning of the cache and serve to protect a node as well as to make it more efficient.

The most effective way to ensure security is to monitor and enforce the respect of security policy. In ad hoc mobile networks, the detection of protocol deviances must be handled by the neighbors of a node. Nodes may learn from observed behavior of their neighbors to watch for misbehavior such as the dropping of packets, unusual traffic attention or unnecessary route salvaging. This monitoring system could also learn from a neighbor's behavior, and report its experiences with other neighbors thus allowing for greater of dynamic adjustments and autonomous learning methods for the network as a whole. This also prevents against nodes flooding the network with endless streams of trivial data.

Though Securing hosts cannot remove covert network channels it can prevent their exploitation in some application scenarios. If hosts were secured from being hacked, the installation of Trojans, and the modification of software or the network stack would be impossible, thus hackers could not exploit covert channels.

One approach to counter covert channels is to block protocols/

ports that are susceptible. Especially in a closed network protocols prone to covert channels could be blocked, or replaced by versions with fewer or limited covert channels. The leakage of classified information from a high security system to a low security system (the classic covert channel) can be prevented by a network design where only hosts on the same security level are allowed to communicate. But this approach might not prove to be practical for all sorts of networks but can be applied wherever possible.

Networks can be secured against wiretapping. Securing routers against compromise prevents some covert channel scenarios in which covert senders or receivers act as middlemen.

Unused or reserved bits and padding can be set to zero and the unknown header extensions can be removed. The checksums had to be ensured to correct and updated always

5. Conclusion And Future Work

The huge amount of data and vast number of different protocols in the Internet makes it ideal as a high-bandwidth vehicle for covert communications. The capacity of covert channels in computer networks has greatly increased because of new high-speed network technologies, and this trend is likely to continue. Even if only one bit per packet can be covertly transmitted, a large Internet site could lose 26GB of data annually. Many existing covert channels in network protocols follow the obscure approach to security and their detection or elimination is straightforward. Though there are a number of countermeasures, industry products still lack methods to deal with covert channels. And since some proposed countermeasures significantly reduces overt channel performance they cannot be recommended in real high-speed networks. But the race of developing new covert channels with improved stealth and capacity and developing more effective detection and elimination techniques will continue. The future work will involve identifying the possible covert channels during protocol design by intergrating better security management methods

6. References

[1] R. A. Kemmerer, “A Practical Approach to Identifying Storage and Timing Channels,” Proc. IEEE Symp. Security and Privacy, Apr. 1982.

[2] I. S. Jacobs and C. P R. Tsai, V. D. Gligor, and C. S Chandersekaran. A Formal Method for the Identification of Covert Storage Channels in Source Code. *lEEE Transactions on Software Engineering*, 16:6, pp. 569-580, June 1990.

[3] Robert Nitzel and Charles Benton. Exploiting Dynamic Source routing to Enable Undersea Networking over an Ad-hoc topology. AUSNET 2002.

[4] John P. Wack, Lisa J. Carnahan. Computer Viruses and Related Threats: A Management Guide. 1989

[5] David B. Johnson, David A. Maltz. Dynamic Source Routing in Ad Hoc Wireless Networks , *Mobile Computing*, 1996.