A Security Design combining the advantages of Cryptanalysis and Anonymous routing protocol to achieve data secrecy and anonymity

Varsha Waingankar , Swetha S.
{MTech 4th semester} {Asst.Professor}

Department of Information Science and Engineering
R.V College of Engineering

ABSTRACT

Since internet is widely used these days , users privacy has become the main concern. Privacy is related to anonymity .Basic requirement for anonymity is to unlink the user's identity to specific activities such as in a untraceable e-cash system and P2P payment systems. To provide anonymity various techniques are made use of such as identity based cryptography, blind messages, pseudonyms and ticket based protocol. But only the use of cryptography will not provide with the existence of confidential communication so anonymous routing protocol used along with cryptography helps to achieve better anonymity. With the use of anonymous routing protocol multiple packets cannot be linked to have originated from the same client . Hence the real network identity will be concealed making it difficult to find the client and the confidential relationship between the parties involved in communication.

Keywords: ***anonymity, privacy, routing protocol, onion routing, cryptography, and pseudonym.***

1. INTRODUCTION

MANET's are more prone to attacks [1]. (both active as well as passive) because wireless transmission are easier to capture. Hence providing security in MANET's is a difficult task. Providing anonymity in MANET's is important because the users may want to hide his/her identity while making use of a particular service or communicating with other users. Also anonymity is very important in the case where the user wants to hide location information so that the adversary finds it very difficult to attack, as he won't be able to identify and locate the nodes within that particular network.

2. BACKGROUND STUDY

Every time a mail is being sent or a web page is being visited or chat facility is made use of, the packets of data is sent across the internet. This data contains information about where the data is to be sent and to whom should it be sent .i.e, basically the IP address. [2]These data packets are transmitted through several nodes from the source to the destination so any person keenly observing that link can roughly identify the person involved in the communication based on the information that is present in the packet. The addresses of source and destination are visible in the packet's IP header, even though the packet data is encrypted.

The system is considered to be a collection of clients, servers in a communication network. The client and the servers exchange information using a communication channel most popularly being the internet. The client and servers act as nodes, whereas the communication channels act as links. Anonymity systems provide unlinkability between sent messages and their true recipients.

Pseudonyms are another important aspect of security. But pseudonyms are different from anonymity as in, actions of sending and receiving message are linked to a particular identifier that is not the true identity of that person. Even though anonymity and pseudonymity are different concepts, they are inter related. A pseudonym can be used to link a series of transactions over an anonymity system.

2.1 PROPERTIES OF THE ADVERSARIES

Passive/active adversaries: An adversary that is able to monitor and record the traffic on the network links, entering and exiting the clients and servers in an anonymous network is known to be passive adversary. It can also record data such as packet lengths and arrival times. [3]

An adversary that has all the capabilities of a passive adversary and is also able to manipulate network traffic by controlling one or more network links and by operating a node in the anonymity network is known as an active adversary. This adversary can modify and drop traffic in parts of the network , as well as insert his own traffic or even replay the previously recorded legitimate traffic.

Global/Local adversaries : A powerful observer that has access to almost all the network links between the clients and the server in an anonymous network is known as a global adversary

An adversary that is only capable of monitoring the links that enter and exit a particular node in a networks or related subsets of these nodes are known as local adversary. The visibility of an adversary determines how much of the network he is able to passively monitor or actively manipulate

Static/Adaptive Adversaries: An adaptive adversary is one that does not contain large scale infrastructures that is required for monitoring all clients and servers in an anonymity network at the same time. And hence he selects some subsets of the network that he wants to monitor based on the previously acquired information.

An adversary that is able to monitor some subsets of the network, but not able to change which subset he observes at will is known as a static adversary.

2.2 THE PROBLEM: CRYPTOGRAPHY ALONE WILL NOT HIDE THE EXISTENCE OF CONFIDENTIAL COMMUNICATION RELATIONSHIPS

In addressing the privacy and anonymity issues over the internet Dingledine [4] argues over the fact that cryptography alone cannot sufficiently hide the existence of confidential communication relationships. Hence cryptography must be combined along with appropriate routing protocol such as TOR to achieve better anonymity from the security point of view. Tor is intended to provide online anonymity. Tor is basically internet software that is used to route internet traffic through a worldwide volunteer network of servers in order to conceal a user's location or usage from anyone conducting network surveillance or traffic analysis. Usage of Tor makes it more difficult to trace Internet activity, including "visits to Web sites, online posts, instant messages and other communication forms", back to the user and is intended to protect users' personal freedom, privacy, and ability to conduct confidential business by keeping their internet activities from being monitored.

Onion routing was conceived in 1996 by David.M.Goldschlag, Michael.G.Reed and Paul.F.Syverson for the Naval Research Laboratory’s research group in high assurance system [5]. It lives just beneath the application layer and is designed to interface with a wide variety of unmodified internet services by means of proxies. Onion routing is the mechanism in which the sender (initiator) and the receiver (responder) nodes communicate with each other anonymously by means of some anonymous intermediate nodes called as onion routers. It protects against traffic analysis and makes it very hard for an eavesdropper to determine who is talking to whom over the network. It concentrates on encrypting the packet header in such a way that only the intended destination understands that the packet is meant for him. Instead of making a socket connection directly with the destination machine, the sender makes a connection to an onion proxy on a remote machine. This onion proxy then randomly selects a set of onion routers up to the destination and builds an anonymous connection to the destination via them. It then constructs a special data structure called as an onion and routes it through this established connection

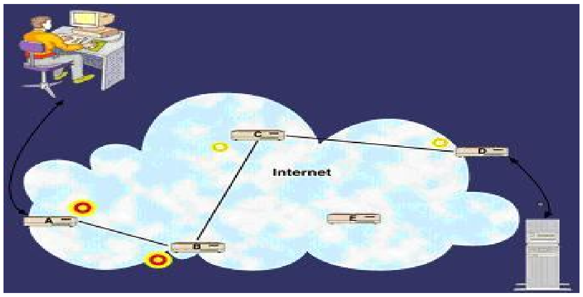

Figure 1: Transfer of data using encryption

3. OVERVIEW: SOLUTION

Anonymous routing as in wired networks make use of MIX-NETS [4], wherein the packets that are sent from the source to destination must pass through a series of mixes. A mix basically re-orders and re-encrypts the incoming data for forwarding, thereby preventing the correlation of incoming and the outgoing flows. Mix was modified in the onion routing that allows the routing information to be encoded in a set of the encrypted layers. TCP based onion router (tor) adds forward secrecy and incremental path building.

3.1 Network Infrastructure:

As shown in the figure the network infrastructure consists of onion routers that carry traffic between the initiator and the responder (via the intermediate onion routers). Each onion router has a single connection to each of its neighboring onion routers. The job of a onion router is to decrypt an incoming packet using its private key and pass it to the next onion router mentioned in the onion packet. It may also apply padding to maintain the size of the onion thus making traffic analysis more difficult

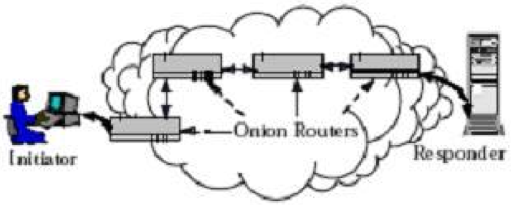

Figure 2 : use of many onion router that carry traffic

3.2 Proxy interfaces:

The proxy links the initiator to the anonymous connection (node W) on the initiator end and at the responder end it links the anonymous connection to the responder (node Z).e.g.: When the initiator sends a request for say a particular URL; instead of directly connecting to the server where the URL content is stored, it connects to an onion proxy W. This proxy then randomly chooses a set of onion routers say X-Y-Z. It then encrypts the packet with Y's, X's and Z's public key and their addresses and sends it to the first onion router on the desired root. The data then moves along the route and is transmitted by Z to the responder. Z also acts as a proxy because it passes data from the responder to the anonymous connection. Each onion proxy maintains a list of onion routers on the network and their IP addresses. There are also directory servers where active routers register with. So onion proxies can query directory servers from time to time in order to get an up-to-date list of servers on the network

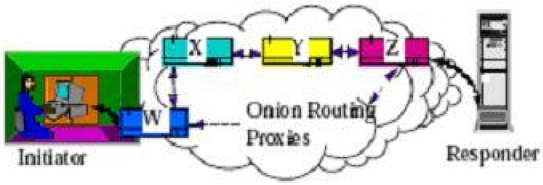

Figure3 : use of proxy router for traffic analysis between source and destination node for increased security

Onion routing consists of the following steps: Defining a route, constructing an anonymous connection, moving data through an anonymous connection and destroying the anonymous connection.

The protocol used here basically focuses on achieving anonymous routing directly to the needs of the dynamic and unpredictable MANET's. This approach combines the use of Identity based cryptography (IBC), use of node pseudonyms, and also a simple symmetric key cryptography by eliminating the burden of public key certificate management by using the identity of the node as its public key The private key is known only to the node with the appropriate identity. All these features combined together make this algorithm more robust and efficient compared to the existing ones. The advantages of this approach include

1. Eliminating the use of the public key certificate and the certificate management infrastructure by exploiting the power of asymmetric key cryptography.

2. Low costs of the cryptographic operations

3. Exploiting the fact that there are no links in a wireless network that make that make messages untraceable. This provides strong anonymity in MANET's

The design focuses on providing guarantee of data secrecy between the communicating nodes. The design ensures the following:

1. Identity anonymity: A node that sends or receives packet cannot be identified by its neighbor.

2. Route anonymity: A node that is responsible for forwarding packets must be unable to determine the identities of other nodes participating in the routing protocol.

3. Location anonymity: It should not be possible for any node even to determine other nodes approximate location.

- The target environment needed to ensure that the protocol is robust and light weighted
- Protocol should limit the use of asymmetric key cryptography in order to prevent compute intensive operations such as certificate management.
- The protocol should prevent the flooding attack.

3.3. DATA STRUCTURES FOR NODES Each node maintains a set of data structures.

3.3.1. Token table for route request

In this table each entry consists of a route request token. This consists of a two-byte nonce and a timestamp that corresponds to the tokens last reference. This token uniquely identifies a single route request packet and also prevents the excessive rebroadcast of a route request by a single node

3.3.2 Table for maintaining the pseudonyms

Nodes make use of a list of pseudonyms to identify it self. Each route request that visits a node has an unique pseudonym. Each entry in the table contains information about the pseudonym and the timestamp associated with that pseudonym as to when it was last referenced.

3.3.3. Data table used for Routing

The information about all the active routes that are present between the source to the destination are maintained in this table that holds the next hop for each destination and related parameters.

Destination id : The public identity of the destination node

Source node nonce: The symmetric key material generated on this node and used as a part of the session key between this node and the destination id

Destination node nonce : The symmetric key material that is generated by the destination and used as apart of the session key material.

Initialization vector: Is made use for encryption and decryption using the session key

Encrypted initialization vector: The initialization vector encrypted using the session key used to reduce the decryption attempts.

Pseudonym List : The list of node pseudonyms for this

Table1: parameters used for route request

3.3.4 Route Reply packet Data table

Information about the recent replies passing through the node are stored in this table. This table ensures each packet reaches its intended destination by re-broadcasting it periodically until the node receives an acknowledgment.

Route reply token: Only if this is not disabled there exists an entry.

Route reply packet uid: A set of bytes acting like a trap door basically used to determine the intended destination.

Encrypted route reply data : Data that is encrypted with a nonce sent by a source contains a fresh nonce generated by the destination along with the source and destination identities.

Time until broadcast: before attempting to broadcast the time required to hold the route reply

Timestamp: time when the entry was inserted into the table

rebroadcast_disabled: the route reply was re-broadcasted by a neighbor is indicated using a true value.

route pseudonym : list pseudonym list for this reply’s route

Table 2: Parameters used for route reply

3.3.5. Table for data packet

The information about the recent data packets that have passed through the nodes are stored her. The route reply gets periodically re-broadcasted until the entry is disabled.

data token: unique token of the stored data packet.

data packet uid: the trapdoor for the data packet

encrypted data: application level data to be transmitted; encrypted with the session key generated cooperatively by the source and destination

Table3 : Parameters used for data packet and transfer

The other parameters such as timestamp, time until broadcast, rebroadcast disabled and route pseudonym list are also included.

3.3.6. Route Request, Route Reply and Data packet structure

To ease the processing of control packets, CARP (certificate free anonymous routing protocol) structures them in a common form:[6]

[packet type_, TTL, packet_token, other blocks of bytes that are specific to the packet],

where packet_type can be RREQ, RREP, or DATA for route request, route reply and data packets. The TTL (time to live) is decremented at each hop. The packet_token is a two-byte nonce that uniquely identifies each packet and is used to prevent broadcast storm

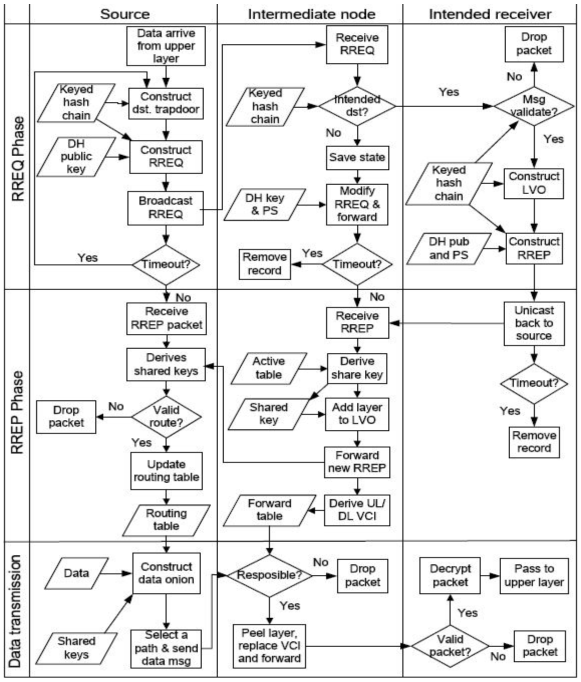

Figure 4. operational flowchart [References:*www.nicta.com.au/__data/assets/pdf_file/0004/.../Paper_-_Taro.pdf*]

4. RESULTS

This paper provides a better security design at the protocol level. This process give detailed insights about the need of the routing protocol, the adversaries and the attacks, different types of anonymity leading to the design of the protocol and the various steps involved in the design. For example, if the users are communicating through the means of an wireless medium, although encryption is used to protect data from being read by unintended recipients it still does not ensure complete safeness. The reason being that information can be gathered by an eavesdropper by indirect inferences like traffic analysis etc. The onion is constructed in such a way that it prevents any eavesdropper from gaining information about the parties involved in the communication or the nature of their data exchange. The result of this paper being a more efficient security architecture with IBE's use to route discovery i.e; certificate free anonymous routing protocol.

5. CONCLUSION

The anonymous protocol presented in this paper provides with strong anonymity and guarantees major advantages over the competing methodologies. CARP exploits the strong security guarantees of an asymmetric key cryptography scheme IBE, but eliminates the use of public key certificates and certificate management there by reducing the cost. CARP exploits the lack of links in an ad hoc network to provide strong anonymity guarantees, such as identity, routing and location identity anonymity for nodes on an ad hoc network.

6. REFERENCES

[1] Jinyuan Sun, Member, IEEE, Chi Zhang, Student Member, IEEE, Yanchao Zhang, Member, IEEE, and Yuguang Fang, Fellow, IEEE "SAT: A Security Architecture Achieving Anonymity and Traceability in Wireless Mesh Networks

[2] On Anonymity in an Electronic Society: A Survey of Anonymous Communication Systems . Matthew Edman ACM Journal Name, Vol. V, No. N, Month 2008, Pages 1{39.

[3] Attacks on Anonymity Systems: The Theory Roger Dingledine http://freehaven.net/

[4] R Dingledine, N Mathewson, and P Syverson. Tor: The Second Generation Onion Router. InProceedings of the 13th USENIX Security Symposium, pages 303–320, August 2004

[5] Michael G. Reed, Paul F. Syverson, David M. Goldschlag. "Proxies for anonymous Routing". Naval Research Laboratory, Washington DC.

[6]TARo: Trusted Anonymous Routing for MANETs Jiefeng (Terence) Chen National ICT Australia Roksana Boreli ,National ICT Australia , Vijay Sivaraman School of Electrical Engineering and Telecommunications , University of New South Wales , Australia.