Young Scientist- Tomorrow's Science Begins Today
Vol. 1, Issue – 2015
ISSN: 2581-4737

HASHING ROUTING

PUSHPANKAR SHEKHARI, ANUPAM PANDEY

ABSTRACT

A recent trend in ad hoc network routing is the reactive on-demand philosophy where routes are established only when required. Mostly work has been concentrated on routing aspect. Most of the protocols in this category are not incorporating proper security features. Security is one of the most important concepts in ad hoc networks. It has been observed that different protocols need different strategies for security. The study here proposes a theory in this paper based on Hashing as a tool. This scheme can make most of the on demand protocols secure. The study should help in making protocols more robust against attacks and standardize parameters for security in routing protocols.

KEYWORDS: Security, ad hoc networks, MANET, Hashing.

INTRODUCTION

Wireless Ad Hoc networks have been an interesting area of research for more than a decade now. What makes ad hoc networks interesting and challenging is its potential use in situations where the infrastructure support to run a normal network does not exist. Some applications include a war zone, an isolated remote area, a disaster zone like earthquake affected area and virtual class room etc. In ad hoc networks all nodes are responsible of running the network services meaning that every node also works as a router to forward the networks packets to their destination. It is very challenging for researchers to provide comprehensive security for ad hoc networks with the desired quality of service from all possible threats. Providing security becomes even more challenging when the participating nodes are mostly less powerful mobile devices. In this paper an effort has been made to evaluate various security designs proposed.

SECURITY REQUIREMENTS

In any fixed or wireless network, the security is incorporated at three stages: prevention, detection and cure. Key parts of prevention stage are authentication and authorization. The authentication is associated with authenticating the participating node, message and any other meta-data like topology state, hop counts etc. Authorization is associated with recognition. Where detection is the ability to notice misbehavior carried out by a node in the network, the ability to take a corrective action after noticing misbehavior by a node is termed as cure. Different possible attacks on ad hoc networks are eavesdropping, compromising node, distorting message, replaying message, failing to forward message, jamming signals etc. The

ISSN: 2581-4737

central issues behind many of the possible attacks at any level of security stage are authentication, confidentiality, integrity, non repudiation, trustworthiness and availability. There are several proposals available to solve these issues, but are not comprehensive in nature as they target specific threats separately. Therefore there is a strong need to have an efficient security regime which can take care of all the aspects of security.

SECURITY THREATS

The two broad classes of network attacks are active attacks and passive attacks.

PASSIVE ATTACK

An attack in which an unauthorized party gains access to an asset and does not modify its content (i.e., eavesdropping). Passive attacks can be either eavesdropping or traffic analysis (sometimes called traffic flow analysis). These two passive attacks are described as Eavesdropping: The attacker monitors transmissions for message content. An example of this attack is a person listening into the transmissions on a network topology between two workstations or tuning into transmissions between a wireless handset and a base station.

ACTIVE ATTACK

An attack whereby an unauthorized party makes modifications to a message, data stream, or file. It is possible to detect this type of attack but it may not be preventable. Active attacks may take the form of one of four types masquerading, replay, message modification, and denial-of-service (DoS). These attacks are summarized as:

- **Masquerading:** The attacker impersonates an authorized user and thereby gains certain unauthorized privileges.
- **Replay:** The attacker monitors transmissions (passive attack) and retransmits messages as the legitimate user.
- **Message modification:** The attacker alters a legitimate message by deleting, adding to, changing, or reordering it.
- **Denial-of-service:** The attacker prevents or prohibits the normal use or management of communications facilities. The consequences of these attacks include, but are not limited to, loss of proprietary information, legal and recovery costs, tarnished image, and loss of network service. Some of the issues associated are given below.
    - Ad Hoc networks primarily being wireless have limited band-width in comparison to wired networks. Smaller packets are available to transfer data and it further constraints to use. lesser number of bits for security purposes. It has been expected that this limitation will be eased with the advancement of hardware in future.
    - The participating nodes of an Ad Hoc networks usually are mobile devices which have limited capabilities in terms of processing power, memory size and battery backup. It makes the use of digital signature, as a security measure less suitable as

ISSN: 2581-4737

digital signatures are computation intensive. The use of digital signatures may also consume considerable memory if digital signatures are appended by each node that forwards the packet to its destination.

SECURE ROUTING

The routing protocols with in ad hoc networks are more vulnerable to attacks as each device acts as a relay. Any tampering with the routing information can be compromise the whole network. An attacker can introduce rogue information with in routing information or replay old logged or stored information.

The aim is to protect any information or behaviour that can update or cause a change to the routing tables on cooperating nodes involved in an ad hoc routing protocol. For completeness, timeliness and ordering are added to the list of desirable security properties that can eliminate or reduce the threat of attacks against routing protocols. Techniques that can be used to guarantee these properties are described in Table I.

Table I.

Properties	**Techniques**
Timeliness	Timestamping, Slotted Time
Ordering	Sequence Numbering
Authenticity	Password, Certificate
Authorization	Credential
Integrity	Digest, Digital Signature
Confidentiality	Encryption
Non-Repudiation	Chaining of Digital Signature

The following properties can be integrated into routing protocol messages to prevent attacks that exploit the vulnerability of unprotected information in transit:

TIMELINESS

Routing updates need to be delivered in a timely fashion. Update messages that arrive late may not reflect the true state of the links or routers on the network. They can cause incorrect forwarding or even propagate false information and weaken the credibility of the update information. Most ad hoc routing protocols have timestamps and timeout mechanisms to guarantee the freshness of the routes they provide.

ORDERING

Out-of-order updates can also affect the correctness of the routing protocols. These messages may not reflect the true state of the network and may propagate false information. Ad hoc routing protocols have sequence numbers that are unique within the routing domain to keep updates in order.

ISSN: 2581-4737

AUTHENTICITY

Routing updates must originate from authenticated nodes and users. Mutual authentication is the basis of a trust relationship. Simple passwords can be used for weak authentication. Each entity can append a public key certificate, attested by a trusted third party to claim its authenticity. The certifying authority can implement a password based login or a challenge-response mechanism to authenticate the identity in the first place. The receiving node can then verify this claim by examining the certificate. One of the problems in ad hoc networking is the absence of a centralized authority to issue and validate certificates of authenticity.

AUTHORIZATION

An authenticated user or node is issued an un-forgeable credential by the certificate authority. These credentials specify the privileges and permissions associated by the users or the nodes. Currently, credentials are not used in routing protocol packets, and any packet can trigger update propagations and modifications to the routing table.

INTEGRITY

The information carried in the routing updates can cause the routing table to change and alter the flow of packets in the network. Therefore, the integrity of the content of these messages must be guaranteed. This can be accomplished by using message digests and digital signatures.

NON-REPUDIATION

Routers cannot repudiate ownership of routing protocol messages they send. A major concern with the updates is the trust model associated with the propagation of updates that originate from distant nodes. Ad-hoc nodes obtain information from their neighbours and forward it to their other neighbours. These neighbours may forward it to other neighbours and so on. In most existing protocols, nodes cannot vouch for the authenticity of updates that are not generated by their immediate neighbours. In order to preserve trust relationships, it becomes necessary to form a chain of routers (using signatures to protect integrity) and authenticate everyone in turn, following the chain to the source. This is necessary because trust relationships are not transitive. Alternative solutions that avoid chaining include the path attribute mechanism developed for Secure BGP and secure distance vector routing.

CONFIDENTIALITY

In addition to integrity, sometimes it may be necessary to prevent intermediate or non-trusted nodes from understanding the contents of packets as they are exchanged between routers. Encrypting the routing protocol packets themselves can prevent unauthorized users from reading it. Only routers that have the decryption key can decrypt these messages and

ISSN: 2581-4737

participate in the routing. This is employed when a node cannot trust one or more of its immediate neighbors to route packets correctly, etc.

Each of these desirable properties has a cost and performance penalty associated with it. Some options such as enforcing access control to routing tables using credentials and providing non repudiation by chaining signatures are extremely expensive and impractical to implement and enforce in a generalized routing protocol.

PROPOSED SOLUTION

The solution proposed stresses upon applying hashing techniques not only in prevention stage in the form of message and routing information authentication, but also in different stages of securing ad hoc networks. The efforts can be made in the direction of improving hash functions to avoid collisions, using stronger hash keys by making them dependent on additional parameters like biometric credentials, passwords, IP addresses etc. The hash techniques can also be tried for keeping the link status of the network.

HASHING TECHNIQUES

Hash Function: Hashing techniques available are based on the concept of a hash function that transforms a given input of arbitrary length to a value of a fixed length, called the hash value. The transformation is done in a manner that it is computationally infeasible to transform the hash value to the original value. Hash functions are very efficient as they do not involve heavy computations and hence are applied in the area of security for message authentication and integrity checks.

The problem with hash functions is collision. Collision is a situation where a hash function generates the same hash value for more than one different input values. Collisions are possible in a hash function due to the fact that it transforms an input of any length to an output of fixed length, meaning a mapping from a larger set to a smaller set. The solution to this problem is achieved through the adoption of appropriate collision resolution or avoiding techniques. There can be three ways in which the collisions can be handled: first by selecting a hash function that is more and more collision resistant, second by putting the processing in an environment to minimize the chance of collisions and third by resolving when the collision really takes place. The choice of a hash function,its implementation and its associated collision resolution technique depends on problem area that is being solved.

The popular examples of hashing functions found to be used in different places are HMAC, MD5, SHA-1.

One way hash chain: A unique way of using hash functions is 'one way hash chain'. This concept was firstly used to provide one time password authentication and later for one time use of digital cash. One way hash chain is the list of values that are generated by applying a hash function on an initial value repeatedly. Every value, except the initial one, is therefore

ISSN: 2581-4737

generated by applying hash function to its previous value exactly one time. This way, any value from that list can be authenticated by providing the previous value in the sequence as a key. Therefore the values of a chain can be used in the reverse order of their generation.

The problem with hash chain is to synchronize the authentication process with the revealing of the validating keys. A message will be incorrectly invalidated if time duration in which the validating key (the previous hash value from the hash chain) is being advertised is missed

Many of the implementations of one way hash chains in ad hoc network are based on TESLA protocol which was initially developed for authenticating broadcast messages.

Hash Trees: Hash tree is a tree of hash values that has been built up on a set of some initial values. The lowest layer of the tree comprise of the initial values as the leaf nodes, In the next layer of the tree the initial values are individually converted to their corresponding hash values while in the subsequent layers, the hash values are computed by utilizing more than one values of the lower layer. Eventually we have a top hash value representing the root of the tree. The top hash value can be used to authenticate any of the values within the tree.

RELATED WORK

Most of the work done around using Hashing techniques is around authenticating messages and route table entries. Bayya et al demonstrate the use of hashing as part of password based authenticated key exchange. The problems given in this protocol are :

- The need of a strong shared secret.
- The need to constantly change the shared secret which in turn may prove to be computationally expensive.

Adrian et al used symmetric cryptography to secure ad hoc networks by using one way hash chains or Markle hash tree as part of SEAD protocol for proactive routing. In this protocol the elements of hash chain are used directly to authenticate the sequence number and other metric in each entry. The problems identified with SEAD protocol are:

- No provision of a secure initial key distribution.
- Count-to-infinity problem where the routing table update of one node forces the routing table update in another node which in turn forces the update in the first node and so on.
- Observes greater network traffic.

Adrian et al, in one of the variants of their routing protocols named 'Secure On-Demand Routing Protocol' based authentication on TESLA which in turn depends on using hashing in the form of MAC for authenticating messages. TESLA also takes care of constantly changing keys with the help of one-way key chains which are published on a time synchronization pattern. The problem associated with Adrian is strict time synchronization. Zapata in its proposed protocol, SAODV uses a new one-way hash chain for each Route Discovery to

ISSN: 2581-4737

secure the metric field in an RREQ packet. It also uses asymmetric cryptography to initially authenticate participating nodes. Adding two issues to create security will demand more mathematics and slow down causing end to end delay. Maintenance of PKI infrastructure is always a problem in case of asymmetric primitives being used. Cheung and Hauser et al. describe symmetric-key approaches to the authentication of updates in link state protocols, but neither work discusses the mechanisms for detecting the status of these links.

CONCLUSION

In this paper, the security threats for an ad hoc network has been analysed and presented with the security objectives that need to be achieved. The paper represents the first step of research to analyse the security threats, to understand the security requirements for ad hoc networks, and to identify existing techniques, as well as to propose new mechanisms to secure ad hoc networks. Hashing has been used as one of the tools. More skilled technical work has to be done to deploy these security mechanisms in an ad hoc network and to investigate the impact of these security mechanisms on the network performance.

REFERENCES

1. W. Stallings," Network and Internetwork Security Principles and Practice", Prentice Hall, Englewood Cliffs, NJ, 1995.
2. NIST, Fed. Inf. Proc. Standards, "Secure Hash Standard," Pub. 180, May 1993.
3. Bayya, Arun. Security in Ad-hoc Networks, Computer Science Department. University of Kentucky.
4. B. J. Yih-Chun Hu, Adrian Perrig. Ariadne: A secure on-demand routing protocol for ad-hoc networks. In Proceedings of the Eighth Annual International Conference on Mobile Computing and Networking (MobiCom 2002), Sept. 2002.
5. Y. Hu, D. Johnson, and A. Perrig, "Sead: Secure Efficient Distance Vector Routing for Mobile Wireless Ad Hoc Networks," IEEE WMCSA, 2002.
6. Diane Tang. Resource Discovery in Ad-Hoc networks, Computer System Laboratory , Stanford University Stanford, California 1998
7. Kai Inkinen. New Secure Routing in Ad Hoc Networks: Study and Evaluation of Proposed Schemes, Helsinki University of Technology.
8. Hao Yang, Haiyun Luo et al. Security in Mobile Ad Hoc Networks: Challenges and Solutions, UCLA Computer Science Department.
9. Manel Guerrero Zapata. Secure Ad hoc On-Demand Distance Vector (SAODV) Routing. IETF MANET Mailing List, Message-ID: 3BC17B40.BBF52E09@nokia. com, Available at ftp://manet.itd.nrl.navy.mil/pub/manet/2001-10.mail, October 8, 2001.
10. Manel Guerrero Zapata, N. Asokan. Securing Ad Hoc Routing Protocol. WiSe 2002
11. Po-Wah Yau, Chris J. Mitchell. Security Vulnerabilities in AdHoc Networks. Royal Hollway, University of London.
12. Young Ho PARK et el. Secure Route Discovery Protocol for Ad Hoc Networks. IEICE Trans. Fundamentals, Vol.E90-A, No.2 Feb, 2007.

