International Journal of Computing and Business Research (IJCBR)

ISSN (Online) : 2229-6166

Volume 4 Issue 3 September 2013

PERFORMANCE EVALUATION OF SECURITY SCHEMES FOR AD HOC NETWORKS

Ashok Kumar,

Electronic Science Dept.,

DAV College,

Ambala City (Haryana),India

Abstract: A recent trend in Ad Hoc network routing is the reactive on-demand philosophy where routes are established only when required. Most of the protocols in this category are not incorporating proper security features. In this paper areas have beenidentified where work needs to be done to incorporate security mechanisms into the routing protocols for ad hoc networks. It has been observed that different protocols need different strategies for security. The study will help in making protocol more robust against attacks and standardizing parameters for security in routing protocols.

1. INTRODUCTION

A wireless Ad hoc network is a collection of different nodes in vicinity with each other and making a network on the fly, without centralized infrastructure. Each member node communicates with each other via radio range using other nodes. In such Ad hoc networks, nodes keep on moving around and may leave or join the network. In this paradigm the traditional wired routing protocols cannot be implemented. In Ad hoc networks the density of nodes, number of nodes and the mobility of these hosts may vary. As there are no stationary infrastructures, each node acts a router which transmits data packets to other nodes. Thus the choice of effective and robust routing protocol is very important [1, 2]. Main aim of routing is to minimize delay, maximize network throughput, maximize life time and maximize energy efficiency. On the basis of routing information update mechanism Ad hoc network routing protocols can be divided into three categories namely

- Table –driven or Proactive routing protocols.
- On demand or Reactive routing protocols.
- Hybrid routing protocols.

1.1Table -driven or proactiveroutingprotocols: In this routing protocol, each node maintains one or two tables containing network topology information which periodically exchanges with other nodes in the network. Path finding algorithm on this topology maintains path of destination. In small networks, this can be efficient as normal communication does not involve any delay in the route setup. With the increase in size of the network this scheme becomes quite complicated. The maintain Nance of routing tables requires large storage space, network bandwidth and processing time. All these are in scarcity in Mobile Ad hoc networks. The main problem of the proactive routing is that if the topology of network changes or a new

node enters or old node leaves the network, a node that moves to new location must make its presence known to all neighboring nodes; this causes a huge overload and potential delay in the network. Some of the table-driven Ad hoc routing protocols are Destination-sequenced Distance –vector (DSDV), Wireless Routing Protocol (WRP)

1.2 On demand or reactive routing protocols: Such protocols do not maintain network topology information. Here the routes are created as and when required. With the onset of transmission from source to destination, the required path is obtained by using connection establishment process. Protocols falling in this category do not exchange routing information periodically. Some of the existing reactive protocols are Dynamic Source Routing (DSR) [3, 4], Ad hoc On Demand Distance-Vector Routing (AODV) [2] and Temporary Ordered Routing Protocol (TORA). Due to the reactive nature the nodes do not have to announce their arrival or departure from the network. The intended recipient might already have left the network when the sender wants to initiate transmission. A route request still has to be transmitted throughout the whole network, consuming resources of all nodes.

1.3 Hybrid routing protocols: Protocols of this group combines the best features of the Proactive and reactive protocols. Nodes with a certain distance from a particular node under observation are taken as within the routing zone of the given node. For routing within zone Proactive approach is used and for routing with nodes which are located outside the routing zone of the given node Reactive protocol is used. Protocols belonging to this category are: Core Extraction Distributed Ad hoc Routing (CEDAR), Zone Routing Protocol (ZRP) [7] etc.

2. Security against attacks in Ad-Hoc networks:

The use of wireless link makes an Ad-hoc network prone to link attacks of wide range like passive eavesdropping to activate impersonating, message replay and message distortion. By means of eavesdropping attacker may have an access to secret information and on the other hand the active attacks may delete some message or introduce erroneous messages [6, 7, and 8]. These attacks ultimately lead to violating availability, authentication, integrity and non repudiation. Ad hoc networks should have distributed architecture for high survivability. The trust relationship among individual nodes also keep on changing (especially when some nodes are found to be compromised) due to dynamic nature of Ad hoc network. There are various types of Ad hoc networks which are as below

2.1Black *Hole*: In this attack malicious node injects false route replies to the route requests which it receives, advertising itself as having the shortest path to a destination. Such fake replies are fabricated to divert network traffic through the malicious node for eavesdropping, or simply to attract all traffic to it in order to perform a denial of service attack by dropping the received packets.

2.2*Blackmail*: This attack is relevant for those routing protocols which use mechanisms for the identification of malicious nodes and propagate messages that try to blacklist the offender. An attacker may fabricate such messages and try to isolate authentic nodes from the network. The security property of non-repudiation can prove to be useful in such cases since it binds a node to the messages it has generated.

2.3*Breaking the neighbour relationship*: In this an intelligent filter is placed by an intruder on a communication link between source and destination (in the Information system) to modify or change information in the routing updates or even intercept traffic belonging to any data session.

2.4*Denial of Service*: Denial of service attacks aim at the total disruption of the routing function and therefore the entire operation of the Ad hoc network. Particular instances of denial of service attacks include the routing table overflow and the sleep deprivation torture. In a routing table overflow attack the malicious node floods the network with bogus route creation packets in order to consume the resources of the participating nodes and disrupt the establishment of legitimate routes. The sleep deprivation torture attack aims at the consumption of batteries of a specific node by constantly keeping it engaged in routing decisions.

2.5*Masquerading:* During the neighbor acquisition process, a outside intruder could masquerade an nonexistent or existing IS by attaching itself to communication link and illegally joining in the routing protocol domain by compromising authentication system. The threat of masquerading is almost the same as that of a compromised IS.

2.6*Location Disclosure*: Location disclosure is an attack that aims at the privacy requirements of an Ad hoc network. By the use of traffic analysis techniques, or with simpler probing and monitoring approaches, an attacker is able to discover the location of a node, or even the structure of the entire network.

2.7*Replay*: An attacker that performs a replay attack enters into the network routing traffic which has been captured earlier. This attack usually targets the freshness of routes, but can also be used to undermine poorly designed security solutions.

2.8*Routing Table Poisoning*: Routing protocols maintain tables that hold information regarding routes of the network. In such attacks the malicious nodes generate and send fabricated signal, or modify authentic messages from other nodes to create false entries in the tables of the participating nodes. For example, an attacker can send routing updates that do not correspond to actual changes in the topology of the Ad hoc network. Routing table poisoning attacks may result in the selection of non-optimal routes, the creation of routing loops, bottlenecks and even portioning certain parts of the network.

2.9*Rushing Attack*: Rushing attack lands the network in denial-of-service when used against all previous on-demand Ad hoc network routing protocols. For example, DSR, AODV, and secure protocols based on them, such as Adriane, ARAN and SAODV are unable to discover routes longer than two hops when subject to this attack. To develop Rushing Attack Prevention (RAP), a generic defense against the rushing attack for on-demand protocols that can be applied to any existing on-demand routing protocol to allow that protocol to resist the rushing attack.

2.10*Passive Listening and traffic analysis*: In this intruder can passively collect exposed routing information. Such attack cannot effect the operation of routing protocol, but it is sort of breach of user trust to the routing protocol. Thus, sensitive routing information should be protected. However, the confidentiality of user data is not the responsibility of routing protocol.

2.11*Wormhole:* The wormhole attack is one of the most powerful one since it involves the cooperation between two malicious nodes that participate in the network. One attacker, e.g. node A, captures routing traffic at one point of the network and tunnels them to another point in the network, to node B, for example, which shares a private communication link with A. Node B then

selectively injects tunneled traffic back into the network. The connectivity of the nodes which have established routes over the wormhole link is completely under the control of the two collaborating attackers.

3.0 This paper deals with survey and comparison of various security Protocols such as ARAN, ARIADNE and SRP.Basic features of these protocols are as below.

3.1Authenticated Routing for Ad hoc Networks (ARAN)

The ARAN secure routing protocol is an on-demand routing protocol that detects and protects against malicious actions carried out by third parties and peers in the Ad hoc environment [9]. ARAN introduces authentication, message integrity and non-repudiation as part of minimal security policy for the Ad hoc environment and consists of a preliminary certification process, a mandatory end to-end authentication stage and an optional second stage which provides secure shortest paths. ARAN requires the use of a trusted certificate server (T) before entering in the Ad hoc network, each node has to request a certificate signed by T. The certificate contains the IP address of the node, its public key, a time stamp indicating when the certificate was created and time at which the certificate expires along with the signature by certificate server. All nodes are supposed to maintain fresh certificates with the trusted server and must know T's public key. The aim of the first stage of the ARAN protocol is for the source to verify that the intended destination was reached. As with any secure system based on cryptographic certificates, the key revocation issue has to be addressed in order to make sure that the expired or revoked certificates do not allow the holder to access the network. In ARAN, when a certificate needs to be revoked, the trusted certificate server T sends a broadcast message to the Ad hoc group that announces the revocation. Any node receiving this message rebroadcasts it to its neighbors. Revocation notices need to be stored until the revoked certificate would have expired normally. Any neighbor of the node with the revoked certificate needs to reform routing as necessary to avoid transmission through the now un-trusted node. This method is not failsafe. In some cases, the un-trusted node that is having its certificate revoked may be the sole connection between two parts of the Ad hoc network. In this case, the non- trusted node might not forward the notice of revocation for its certificate, resulting in a partition of the network, as nodes that have received the revocation notice will no longer forward messages through the un-trusted node, while all other nodes depend on it to reach the rest of the network. This only lasts as long as the un-trusted node's certificate would have otherwise been valid, or until the un-trusted node is no longer the sole connection between the two partitions. At the time that the revoked certificate should have expired, the un-trusted node is unable to renew the certificate, and routing across that node ceases. Additionally, to detect this situation and to hasten the propagation of revocation notices, when a node meets a new neighbor, it can exchange a summary of its revocation notices with that neighbor; if these summaries do not match, the actual signed notices can be forwarded and re-broadcasted to restart propagation of the notice.

Advantages of ARAN

- The ARAN protocol protects against exploits using modification, fabrication and impersonation.

Disadvantages of ARAN

- The ARAN protocol uses of asymmetric cryptography which makes it a very costly protocol to use in terms of CPU and energy usage.
- ARAN is not immune to the wormhole attack.

3.2A Secure On-Demand Routing Protocol for Ad hoc Networks(ARIADNE)

ARIADNE is an on-demand secure Ad hoc routing protocol based on DSR that withstands node compromise and relies only on highly efficient symmetric cryptography [10]. ARIADNE guarantees that the target node of a route discovery process can authenticate the initiator, that the initiator can authenticate each intermediate node on the path to the destination present in the RREP message and that no intermediate node can remove a previous node in the node list in the RREQ (Route Request) or RREP (Route Replay) messages. As for the Secure Routing Protocol (SRP), protocol ARIADNE needs some mechanism to bootstrap authentic keys required by the protocol. In particular, each node needs a shared secret key is the shared key between a source S and a destination D with each node it communicates with at a higher layer, an authentic TESLA key for each node in the network and an authentic "Route Discovery chain" element for each node for which this node will forward RREQ messages.

Advantages of ARIADNE

- ARIADNE copes with attacks performed by malicious nodes that modify and fabricate routing information, with attacks using impersonation and with the wormhole attack.
- It is protected also from a flood of RREQ packets that could lead to the cache poisoning attack.
- It is immune to the wormhole attack only in its advanced version: using an extension called TIK (TESLA with Instant Key disclosure) that requires tight clock synchronization between the nodes; it is possible to detect anomalies caused by a wormhole based on timing discrepancies.

3.3Secure Routing Protocol (SRP)

The Secure Routing Protocol (SRP) has been designed as an extension compatible with a variety of existing reactive routing protocols [11]. SRP combats attacks that disrupt the route discovery process and guarantees the acquisition of correct topological information. It allows the initiator of a route discovery to detect and discard bogus replies and relies on the availability of a security association (SA) between the source node (S) and the destination node (T). The SA could be established using a hybrid key distribution based on the public keys of the communicating parties. S and T can exchange a secret symmetric key (KS, T) using the public keys of one another to establish a secure channel. S and T can then further proceed to mutual authentication of one another and the authentication of routing messages.

Advantages of SRP

- It copes with non-colluding malicious nodes that are able to modify (corrupt), replay and fabricate routing packets.
- Neighbor discovery mechanism maintains information on the binding of the medium access control and the IP addresses of nodes, SRP is proven to be essentially immune to IP spoofing.
- In case of the Dynamic Source Routing (DSR) protocol, SRP requires including a 6-word header containing unique identifiers that tag the discovery process and a message authentication code (MAC) computed using a keyed hash algorithm.

Disadvantages of SRP

- The basic version of SRP suffers from the route cache poisoning attack.
- SRP suffers from the lack of a validation mechanism for route maintenance messages
- It is not immune to the wormhole attack: two colluding malicious nodes can misroute the routing packets on a private network connection and alter the perception of the network topology by legitimate nodes.

4. Proposed plan:

The study is limited in many ways in ad hoc network. Some of the issues that have not been properly addressed, there are many additional issues which have not been addressed for the proper security of ad hoc network. We have proposed the solution for authenticated broadcasting such as data authentication, data confidentiality, data integrity, data freshness, non-repudiation; these are security goal for any application to be achieved. For our security measures, we proposed to implement μTESLA due to its distributed nature, if these are implemented in ad hoc network the routing protocol will be more secure as these provides semantic security some other facility for securing ad hoc network. Some of the measures that can be incorporated are:

4.1Virtual Private Networks (VPN) This offers a solid solution to many security issues, where an authenticated key provides confidentiality and integrity for IP (Internet Protocol) data grams. Software is available to implement VPNs on just about every platform [12, 14]. Authentication depends upon three factors as password, Fingerprints and a security Token. Using two factors is desirable and using all three is most secured. VPN only support IP suite so it cannot be solution for all

environments.

4.2Encryption: Encryption is a technique used for many years for passing information from one place to other in a secured manner [2, 13]. A message in its original shape is referred to as a plaintext (or Text) and a message used to conceal original message is called Cipher text (or Cipher). The process of changing plaintext into cipher text is called Encryption and the reverse process is called decryption. There are many algorithms available for these processes. Some of them are Data Encryption Standard (DES), International Data Encryption algorithm (IDEA) and Public key algorithm (RSA) these are based on key based algorithms. There is one popular key algorithm as Digital signature algorithm. In Digital signature, Signer encrypts the message with key, this is sent to recipient, the message is then decrypted with sender's public key. In case of ad hoc networks this may not be the best method as it uses a lot of space and is also slow.

4.3One Way Hash Function: There is another algorithm called one way hash Function: it is like checksum of a block of text and is secure in that it is impossible to generate the same hash function value without knowing the correct algorithm and key [14, 15]. It accepts a variable size message and produces an affixed size tag as output. This algorithm can be combined with encryption to provide an efficient and effective digital signature.

4.4Digital Signature: External attacks can be checked using Confidentiality of the routing information and also by authentication and integrity assurance features [16]. Encryption can be solution to this. Digital signatures and one way functions can be applied. Permian used complex robustness to protect routing data from compromised nodes. It is ability to continue correct operation in presence of arbitrary nodes with complex failures.

5. Conclusion:

In this paper, security relevant issues with in ad hoc networks are identified. Several issues have been suggested to achieve goal of security. There are some aspects which we are trying to cover as Overhead caused by adding security parameters. Speed of data transmission, which will be affected due to added size. Also medium of transmission is to be taken care of, which can be dense or sparse. The problems of information through covert channels are not addressed in this paper. Efforts are on to incorporate the security parameter as "key encryption" to existing routing protocols and see the effect of it. The major issue to be considered is overhead and speed of data transmission.

Acknowledgement: Special Thanks to DrAshwani Kush, Head, Dept of comp science, University College, Kurukshetra University for his valuable suggestions and guidance.

6. REFERENCES:

1. L.Zhou and Z.J.Haas, "Secure Ad hoc Networks", IEEE Networks,13(6):24-30, Nov/Dec 1999

2. C.E.Perkins and Elizabeth Royer,"Ad hoc on-demand distance vector routing.", In IEEE WMCSA'99, Pages (90-100) February 1999

3. D. Johnson and D.A. Maltz and J. Broch," The dynamic source routing protocol for mobile Ad hoc networks (internet-

draft),” In Mobile Ad hoc network (MANET) Wprlemg group, IETF, PVTPNER 1999

4. D.B. Johnson and D.A. Maltz.”, Dynamic Source Routing in ad-hoc wireless network.”, In Mobile Computing,1996
5. Z.j. Haaas and M. Perlman.,” The Zone Routing Protocol (ZRP) for ad-hoc networks”, (Internet-Draft).1998
6. Preetida,”Security within Ad-hoc networks”Position paper, PAMPS Workshop, Sept 2002, London
7. B.Kumar. ,“Integration of security in network routing protocols” , SIGSAC reviews 11(2):18-25, 1993.
8. A.Kush, C.Hwang, P.Gupta, “Secured Routing Scheme for Ad hoc Networks” International Journal of Computer Theory and Engineering (IJCTE). Volume 3. pp 1793-1799. May 2009.
9. B. Dahill, B.N Levine, E.Royer and C.Shields,” A Secure Routing Protocol for Ad-hoc networks.”Technical Report UM-CS-2001-037, University of Massachusetts, Dept of computer science August2001.
10. Y.C Hu, A.Perrig and D.Johnson ,”Ariadne: A secure on demand routing protocol for ad-hoc networks.”Technical report TR01-383, Rice university, December 2001.
11. P Papadimitratos and Z.J Haas,” Secure routing for mobile Ad hoc networks,”SCS Communication Network and Distributed System Modeling and Simulation Conference (CNDS 2002) January2002
12. S. Vassilaras, D. vogistzis and G.yovanof ,”Security and co-operation in clastered mobile ad-hoc networks with centralized superversion,”IEEE journal on selected areas in communication, 24(2), February 2006.
13. M.g Zapata,”Secure ad-hoc On-Demand Distance Vector(SAODV) routing’” IETE MANET List, Available at draftguerrero-manet saodv-03.txt.March 18,2005.
14. H.Luo and S.Lu,” Ubiquitous and Robust Authentication services for ad hoc wireless network,” In Proceeding of seventh IEEE symposium on computers and communications (ISCC-02), July 2002
15. A.Kush,C.Hwang,”ProposedProtocol for Hash-Secured Routing in Ad hoc Networks”, MASAUM JOURNAL OF COMPUTING (MJC) Volume:1 Issue: 2 Month: Sept. 2009,pages 221-226
16. R. Rivest, A. Shamir, L. Adleman, “A Method of obtaining Digital signatures and public key cryptosystems,” Communications of ACM, 21(2), February 1978 page 120-128