COSMOS: Journal of Engineering & Technology
A Refereed Research Journal
Vol 4 / No 1 / Jan - Jun 2014 ISSN: 2231-4210

THE DISCUSSION ON SECURE ROUTINE PROTOCOLS

Cosmena Mahapatra[1]

Abstract

The present paper deals with the Secure Routing protocol only counters malicious behavior that targets the discovery of topological information .It does not address the protection of data transmission which is handled separately by Secure Message Transmission Protocol. SRP provides the correct routing information regarding a pair of nodes

provided they have prior security association. A Security Association (SA) exists between the source node and destination node. One way of establishing this SA is negotiating a shared secret key by the knowledge of the public key of the other end. The existence of the SA is justified, because the end hosts choose a secure communication scheme and consequently should be able to authenticate each other.

Keywords: Secure Routine, Public Key.

Introduction

This is a very important requirement of Ad hoc networks, thus some of the important characteristics of secure routing protocols are: They must be able to create a route between source destination pair of nodes. They must possess the ability to detect the misbehaving nodes and report such nodes to all other nodes n the network. Misbehaving nodes initially agree to forward the packets and then fail to do so. There must be the ability to build a trust hierarchy among member nodes to prevent any kind of blackmail attacks against the legitimate nodes by a malicious node. These should be able to maintain confidentiality of network topology from malicious nodes.

Some of the Routing Protocols with these Characteristics are:

Security-Aware Ad-hoc Routine (SAR)

It makes use of trust levels (security attributes assigned to nodes) to make informed, secure routing decision. Current routing protocols discover the shortest path between two nodes. But SAR can discover a path with desired security attributes (E.g. a path through nodes with a particular shared key).105 A node initiating route discovery sets the sought security level for the route i.e. the required minimal trust level for nodes participating in the query reply propagation. Nodes at each trust level share symmetric encryption keys. Intermediate nodes of different levels cannot decrypt in-transit routing packets or determine whether the required security attributes can be satisfied and drop them. Only the nodes with the correct key can read the header and forward the packet. So if a packet has reached the destination, it must have been propagated by nodes at the same level, since only they can decrypt the packet, see its header and forward it. The drawback of SAR is the lack of scalability in case of multiple trust levels, where, multiple keys need to be generated and distributed.

Secure Routing Protocol

Secure Routing protocol only counters malicious behavior that targets the discovery of topological information .It does not address the protection of data transmission which is handled separately by Secure Message Transmission Protocol. SRP provides the correct routing information regarding a pair of nodes

provided they have prior security association. A Security Association (SA) exists between the source node and destination node. One way of establishing this SA is negotiating a shared secret key by the knowledge of the public key of the other end. The existence of the SA is justified, because the end hosts choose a secure communication scheme and consequently should be able to authenticate each other. The SA would be established by any of group key exchange schemes. SRP sends the route request to the trusted destination and replies are sent strictly through the same route. This minimal trust prevents the black hole attack. It is required that the end nodes be able to use non-volatile memory to maintain state information regarding relayed queries, so that previously seen route requests are discarded.

Authenticated Routing for Ad-hock Networks (ARAN)

[1] *Research Scholar, Sai Nath University, Ranchi*

ARAN consists of a preliminary certification process followed by route instantiation process that guarantees end to end authentication. Route discovery in ARAN is accomplished by a broadcast route discovery message from a source node that is replied to by the destination node. The routing messages are authenticated end-to-end and only authorized nodes participate at each hop between source and destination.

Watchdog and Path Rater

These components run on each node to detect the malicious nodes in the network. Watchdogs enables the nodes to listen to the transmissions of their one hop neighbors therefore a node can keep track of packets that were successfully transmitted by subsequent nodes and the packets that were not. Thus, a node dropping all the packets is considered malicious. Path rater maintains the rating for every other node in the network. The Path rater assigns rates to the nodes between 0 and 1 with 0.5 being neutral. A node always rates itself with an. Also when a node in the network becomes known to the network Path rater assigns it neutral rating only active nodes are assigned rates. Path rater continuously increments the rating of the node on the active route these ratings aroused as metrics while selecting the path for data transmission. The rating of the path is calculated as the average of the nodes in the path. A path with the highest rating is always selected.

Secure Message Transmission Protocol (SMT)

Secure message transmission protocol (SMT) safeguards pair wise communication across dynamic network, possibly in the presence of adversaries. For a given topology view of the network, source node determines a set of diverse paths connecting the source and destination nodes. This set is called active path set (APS). The protocol introduces limited transmission redundancy across the path; by breaking the message into N fragments so that successful reception of M out of N fragments allow the resurrection of the message at the destination. Each fragment is transmitted across a different path and also its header carries the MAC so that it allows the destination to authenticate and verify its integrity. The source receives authentic acknowledgements that tell it that the data fragments have been received safe and sound to the destination. The SMT protocol combines four elements: end-to-end secure and robust feedback mechanism, dispersion of transmitted data, simultaneous usage of multiple paths and adaptation to the network changing conditions. This protocol requires security associations between two nodes and hence does not require the cryptographic protection at the intermediate nodes. Approaches to secure MANE There are basically two approaches for securing MANET: proactive and reactive. The proactive method attempts to prevent the security threats through various cryptographic schemes. The reactive approach on other hand, seeks to detect the attack or intrusion and react accordingly. Cryptographic Techniques for message authenticationH.MAC (Hashed Message Authentication Code):It says that two nodes sharing the same key KS can efficiently generate and verify message authenticator HK using cryptographic one way hash function. One way Hash functions are the functions that are generally impractical to invert. Here if pair wise keys are used, (n-1)/2 keys will be required to be maintained for n inputs. Digital Signatures: These require mathematically more complete signing and verification as these require asymmetric cryptography. Any node can verify the digital signature given. That it knows the public key of the signing nodes.

References

1. Culler, D. E and Hong, W., Wireless Sensor Networks, Communication of the ACM, Vol. 47, No. 6, June 2004, pp. 30-33.
2. Akyildiz, I. F., Su, W., Sankara Subramaniam, Y, and Cayirci, F., Wireless Sensor Networks: A Survey, Computer Networks, 38, 2012, pp. 3 93-422.
3. Dai, S, Jing, X, and Li, L, Research and analysis on routing protocols for wireless sensor networks, Proc. International Conference on Communications, Circuits and Systems, Volume 1, 27-30 May, 2005,pp. 407-411.
4. Pathan, A-S. K., Islam, H. K., Sayeed, S. A., Ahmed, F. and Hong, C. S., A Framework for Providing E-Services to the Rural Areas using Wireless Ad Hoc and Sensor Networks, to appear in IEEE Icnews 2006.
5. Undercoffer, J., Avancha, S., Joshi, A., and Pinkston, J., Security for Sensor Networks, Cadip Research Symposium, 2002, available at, http://www.cs.sfu.ca./angiezIpersonalIpaper/sensor-ids.pdf.Saleh, M. and Khatib, I. A., Throughput Analysis of Wep Security in Ad hoc Sensor Networks, Proc. The Second International Conference on Innovations in Information Technology (IIT 05), September 26-28, Dubai, 2005.
6. Kurak, C and McHugh, J, A Cautionary Note on Image Downgrading in Computer Security

Applications, Proceedings of the 8th Computer Security Applications Conference, San Antonio, December, 1992, pp. 153-159.

7. Mokowitz, I. S., Longdon, G. E., and Chang, L., A New Paradigm Hidden in Steganography, Proc. of the 2000 workshop on New security paradigms, Ballycotton, County Cork, Ireland, 2001, pp. 41-50.
8. Kim, C. H., 0, S. C., Lee, S., Yang, W. I., and Lee, H-W., Steganalys is on BPCS Steganography, Pacific Rim Workshop on Digital Steganography (Steg'03), July 3-4, Japan, 2003.
9. Younis, M., Akkaya, K., Eltoweissy, M., and Wadaa, A., On handling QOS traffic in wireless sensor networks, Proc. of the37th Annual Hawaii International Conference on System Sciences, 2004, 5-8 January, 2004, pp. 292-301.
10. Orihashi, M., Nakagawa, Y., Murakami, Y., and Kobayashi, K., Channel synthesized modulation employing singular vector for secured access on physical layer, IEEE Globecom 2003,Volume 3, 1-5 December, 2003, pp. 1226-1230.
11. Zhou, L. and Haas, Z. J., Securing ad hoc networks, IEEE Network, Volume 13, Issue 6, Nov.-Dec. 1999, pp. 24-30.
12. Strulo, B., Farr, J., and Smith, A., Securing Mobile Ad hoc Networks A Motivational Approach, BT Technology Journal, Volume 21, Issue 3, 2003, pp. 81 – 89.