Security Issues and Challenges (SIC) of Ad-hoc Networking

Hoshiyar Singh Kanyal
PhD Research Scholar, IFTM, University Moradabad, India.
e-mail :hkanyal1@rediffmail.com

Prof. (Dr.) S. Rahamatkar
PhD Supervisor, IFTM University & Principal, Shree Rayeshwar Institute of Engineering & Information Technology, Shiroda India
e-mail :rahamatkar_s@rediffmail.com.

Dr .B.K Sharma
PhD Co-supervisor, IFTM University and Professor, Ajay Kumar Garg Engineering College Ghaziabad, India
e-mail: bksharma888@yahoo.com

***Abstract*—** As the approach of ad hoc networking varies from traditional networking approaches, the security aspects that are valid in the conventional wired networks are not fully applicable in the context of ad hoc networks. While the basic security requirements such as confidentiality and authenticity remain, the ad hoc networking approach restricts the set of applicable security mechanisms to be used since the level of security and the performance are related to each other and must be carefully balanced.

The security goals and challenges that the field of ad hoc networking faces are explored in more detail. An overview of the most important active attacks is included. Some of the most important security schemes are presented in order to illustrate common approaches that are currently followed to ensure network security in infrastructure less networks. The protected resourceful Ad hoc Distance vector routing protocol (SEAD)[2] employ the use of hash chains to substantiate hop counts and sequence numbers. SEAD[2] is based on the design of the proactive ad hoc routing protocol DSDV[9]. The final secure routing protocol to be presented is the Secure Routing Protocol (SRP).

***Keywords*-*SEAD,DSDV,SRP*.**

*****

I. Introduction

Security is a key concern for ad hoc networks particularly for the more security-aware applications used in military and decisive networks. An ad hoc network can be measured secure if it holds the subsequent attribute [3] :

Accessibility: Ensures that the network manages to grant all services even though denial of service (DoS) attacks. A denial of service attack can be launch at any coating of an ad hoc network [4]. On the substantial and media access control layer a wicked user can employ congestion in order to hold up with signals in the physical layer. On the network layer, a wicked user can interrupt the normal operation of the routing table in different ways. Finally, on the higher layer, a wicked user can bring downward high-level services such as the key management service.

Discretion: Ensures that definite information is in no way disclosed to not permit users. This attribute is typically preferred when transmit responsive information such as military and tactical data. Routing information must also be top secret in some cases when the user's position must be kept secret.

Reliability: Guarantee that the communication that is transmitted reaches its target without being changed or dishonored in any way. Communication fraud can be caused by either a wicked attack on the network or because of broadcasting propagation collapse.

Validation: Enables a node to be confident of the individuality of the peer with which it communicates. When there is no verification scheme node can impersonate as some other node and gain illegal access to resources.

Non-denial: Ensures that the inventor of a communication cannot decline sending this message. This attribute is helpful when trying to sense isolated compromised nodes.

*Access and usage control***:** Access control ensures that access to information is controlled by the adhoc network .Usage control ensures that the information resource is used correctly by the authorized node having the corresponding rights.

II. Security Challenges

The prominent features of ad hoc networks pose both challenges and opportunities in achieving the proposed security goals. One of the main challenges that ad hoc networking [2] faces are related to the use of wireless links [8].

Due to the use of wireless medium an ad hoc network is vulnerable to link attacks ranking from inactive eavesdrop to dynamic masquerade message repeat and message fraud. An adversary can easily eavesdrop network traffic by placing a wireless enabled device within the range of the ad hoc network and capture routing and application packets. By eavesdropping the malicious node can gain access to secret information and violate the confidentiality requirement Passive attacks like eavesdropping are very hard to detect since they do not present any significant pattern [6, 12] or impact in the performance of the network.

Active attacks may allow a malicious node to delete or inject to the network traffic erroneous messages, modify messages and impersonate as another node, hence violating availability, integrity, authentication and non-repudiation. As opposed to passive attacks, active attacks can be detected and limited with the utilization of various schemes.

Attacks against the ad hoc network can be launched from within the network by compromised or malicious nodes. In order to be able to claim high availability in such an environment, an ad hoc network should have distributed protection architecture with no central entities.

Due to the dynamic nature of an ad hoc network both its topology and membership can change arbitrarily. This fact prevents the establishment of long-lived trust relationships among the participating nodes. Unlike other wireless mobile networks [4], like mobile IP, nodes in ad-hoc networks may dynamically become affiliated with different administrative domains. Thus, any security solution with static configuration will not be sufficient. It is desirable for a security mechanism to become accustomed on the dash to these changes.

To conclude, an ad hoc network is not limited to a specific number of participating nodes. Even though it has not been practically attempted, ad hoc networks theoretically can be composed of hundred or even thousands of nodes. Therefore a security mechanism in order to be able to sufficiently accomplish its tasks has to be scalable and able to handle arbitrarily networks.

III. Types of Attack in Ad-hoc Network

Attack is defined as **"**To initiate to act upon violently, to begin to destroy expose, alter, or disable. Attacks in ad-hoc network are:

A. Passive Eavesdropping

An attacker can snoop to any wireless network [8] to know what departure is on in the network. It first listens to manage communication to gather the network topology to recognize how nodes are communicating with another. Thus, it can get together smart information about the network before attacking. It may also listen to the in sequence that is transmitted using encryption though it should be secret belong to upper layer applications.

Eavesdrop is also a hazard to location privacy .An unconstitutional node can notice a wireless network that exists inside a physical area, just by detect radio signals.

B. Discriminating Existence (Selfish Nodes)

This wicked node which is also known as selfish node and which is not participate in the network operations, use the network for its advantage to develop arrangement and save its own resources such as power. To accomplish that, selfish node puts onward its survival whenever personal cost is occupied so these selfish node behaviors are known as discriminating existence attacks. For example, selfish nodes do not still send any HELLO mail and fall all packets even if they are sent to it, providing it does not set up the transmission. When a selfish node wants to begin a link with another node, it performs route detection and then sends the essential packets. When the node no longer wishes to use the network, it returns to the "quiet mode" subsequent to a while, neighboring nodes overthrow their own route entries to this node and selfish node becomes undetectable on the network.

C. Gray Hole Attack (Routing Misconduct)

Gray hole attacks is an energetic attack type, which lead to plummeting of messages. Violent node first agrees to onward packets and then fails to do so. Primarily the node behaves suitably and replay true RREP messages to nodes that begin RREQ [6] message. This mode, it takes over the transfer packets. Afterwards, the node immediately drops the packets to initiate a (DoS) denial of service attack.

If adjacent nodes that attempt to send packets over attacking nodes drop the link to destination then they may desire to determine a route again, broadcasting RREQ messages. Violent nodes establish a route, transfer RREP messages. This progression goes on until wicked node succeeds its aim. This attack is well-known as routing misbehavior.

D. Black Hole Attack

The differentiation of Black Hole Attacks compare to Gray Hole Attacks is that wicked nodes never send proper control messages initially. To bring out a black hole attack, wicked node waits for adjacent nodes to send RREQ messages. When the wicked node receives an RREQ message, without scrutiny its routing table, instantaneously sends a false RREP [7] message giving a route to target over itself, passing on a high sequence number to patch up in the routing table of the wounded node, before other nodes send a true one. Consequently requesting nodes imagine that route discovery method is completed and disregard other RREP [7] messages and begin to send packets over wicked node.

E. Impersonation

Due to lack of validation in ad-hoc networks, just MAC or IP addresses exclusively identify hosts. These addresses are not satisfactory to validate the sender node. Consequently non-repudiation is not providing for ad-hoc network protocols. MAC and IP spooling are the simplest methods to make up as another node.

Wicked nodes achieve impersonation only by altering the source IP address in the control message. An additional cause for impersonation is to argue nodes to change their routing

tables pretend to be a forthcoming node, such as attacks aligned with routing table. One of the attractive impersonations is Man-in-the-middle attack. Malicious (wicked) node performs this attack by combine spoofing and plummeting attacks. Physically, it must be located as the only node within the range for target, in the center of the route must be prevented from receiving any other route information to the target. Malicious (wicked) node may furthermore change the routing tables of the wounded node to redirect its packets, using attacks adjacent to the routing table. At this position, malicious (wicked) node waits for an RREQ message to the target node from basis node. When basis node sends an RREQ message, malicious (wicked) node drops the RREQ and replays a spoofed RREP message to basis node as if it is upcoming from the target node. At the similar time, malicious (wicked) node sends a RREQ message to the target node and drops the RREP message from the target node. By doing this; malicious (wicked) node manages to set up a route both to the basis and the target node and attacker controls the announcement between the basis and target. If the communication is encrypted an authentication as to MAC or IP address, malicious (wicked) node can easily get the up layer communication.

F. Modification Attack

Control messages are used to set up the shortest and true path between two nodes. But malicious (wicked) nodes desire to route packets to the track that they want, modifying content of the control messages (e.g. RREQ, RREP and RERR). Amendment means that the message does not bring out its normal functions.

Direction information such as hop count, sequence number, life time etc. are carried along with control messages. This sequence has a big role in establishing a true route. Modifying these fields in the control messages, malicious node can perform its own attacks. Masquerade is not one of these kinds of attacks; masquerade is only performed by modifying basis address to pretend as another node in the network. But shifting route information in control messages is performing to give the wrong impression about the intermediate node and this modification is normally against the replay messages. For example: by shifting hop count in the RREP messages, malicious (wicked) node wants to change route information of intermediate node. In this attack type; wicked node decreases its hop count in the RREP message, first capturing it, and lastly sending it to the claimed node. When intermediate node receives this fake message it chooses the costly route in the network. Malicious (wicked) node intends to perform this attack to affect the network performance. This attack can be performed by adding a number of virtual nodes and decreasing hop count field of the RREP messages. Such attack is called as detour attack.

G . Attacks against the Routing Tables

Every node has its individual routing table to get other nodes easily in the network. At the identical time, this routing table draws the network topology for each node for a period. (Maximum of 3 second duration of ACTIVE_ROUTE_TIMEOUT constant value of AODV protocol [9]). If wicked node attacks against this table, attacked nodes do not locate any route to other nodes that it needs to link. Such attack is always performed by fabricating a new control message. So it is also called fabricating attack.

Presently there are a lot of attacks against routing tables. Each one is completed by fabricating false control messages. For example; to attempt a black hole attack, wicked node first invade into the routing table of the victim, transport false RREP [7] message. Malicious(wicked) node also spreads false RERR messages into the network so that suitable working links are marked as broken .an added attack type against the routing table is to create lots of route entries for non-existent nodes with RREQ[6] messages. As a end result, routing table of the attacked node is complete and does not have enough ingress to create a new one. This is known as routing table overflow attack. Attacks beside the routing tables also have an effect on the network integrity, varying the network topology established in the routing tables. Erroneous control messages are distributed quickly in the network due to route discovery method and influence the network integrity in a broad area. So attacks against the routing table are known as Network Integrity.

IV . SECURITY SCHEMES

There are two main approaches in securing ad hoc environments currently utilized. The first is the intrusion detection [5,10] approach that aims in enabling the participating nodes to detect and avoid malicious behavior in the network without changing the underlined routing protocol or the underling infrastructure. Although the intrusion detection field and its applications are widely researched in infrastructure networks it is rather new and faces greater difficulties in the context of ad hoc networks. The second approach is secure routing [2] that aims in designing and implementing routing protocols that have been designed from scratch to include security features.

Mainly the secure protocols that have been proposed are based on existing ad hoc routing protocols similar to DSR and DSR but redesigned to include security features. In the following sections we briefly present the two approaches in realizing security schemes that can be employed in ad- hoc [13] networking environments.

A. Intrusion Detection System [11]

Intrusion is defined as "any set of actions that attempt to compromise the reliability secrecy, or accessibility of a resource" [1, 12].Target protection techniques works as the first line of justification. However, intrusion protection unaided is not enough since there is no ideal security in any system, especially in the field of ad hoc networking due to its elementary vulnerabilities. So, intrusion recognition can work as the second line of defense to capture audit data and perform traffic analysis to detect whether the network or a specific node is below attack. On one occasion an intrusion has been detected in an untimely stage, measures can be taken to minimize the damages or even gather evidence to inform other legitimate nodes for the trespasser and maybe initiate countermeasures to minimize the effect of the dynamic attacks.

Target detection [5, 10] system can be classified as network-based or host-based according to the review data that is used. In general, a network-based intrusion detection [5, 10] system (IDS) runs on a gateway of a network. Obviously this approach is not suitable for ad hoc networks since there is no central point that allows monitoring of the whole network. A host-based IDS [10] relies on capturing local network traffic to the specific host. This data is analyzed and processed locally to the host and is used either to secure the activities of this host, or to notify another participating node for the malicious action of the node that performs the attack.

B. Secure Routing

This approach attempts to design secure routing protocols [2,3] for ad hoc networks. These protocols are moreover entirely new stand-alone protocols into existing protocols like AODV and DSR. Generally the existing secure routing protocols that have been proposed can be broadly classified into two categories, those that use hash chains, and those that in order to operate require predefined trust relationships.

C. *Approaches to IDS.* The following approaches to intrusion detection[14]:

Arithmetical anomaly detection: Involves the gathering of data relating to the performance of legitimate users over a period of time. Then statistical tests are functional to observed performance to establish with a high level of confidence whether that behavior is not legitimate user behavior.

Rule-based detection: Involves an effort to describe a set of rules that can be used to make a decision that a given behavior is that of an intruder.

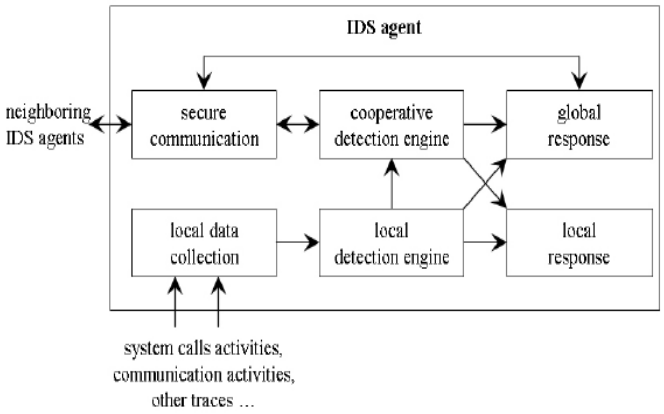

Figure: A Model for an IDS Agent

V. CONCLUSION.

In this, safety measures solution, different vulnerabilities and feasible attacks to Ad-hoc network have been discussed and illustrated. At MAC layer, significant threats contain eavesdrop of management messages, masquerading, management message modification. a few of these issues have been fixed with the acceptance of recent amendments and safety solutions in IEEE 802.16 but some silent exist and need to be measured carefully

Most MANET routing protocols seem to handle the rapid changes to the networking environment rather well. As the routing protocol is responsible for specify and maintain the essential *r*outing fabric for the nodes, protocol must be protected from any attack against confidentiality, authenticity, integrity, non-repudiation and availability.

REFERENCES

[1] S.Madhavi "Intrusion Detection in Mobile Adhoc Networks". In Proceedings of International Conference on Information Security and Assurance, vol 8, July2008, IEEE.

[2] Anand Patwardhan, Anupam Joshi, Jim Parker, Michaela lorga; Secure Routing and Intrusion Detection in Adhoc Networks. In the Proceedings of the 3rd International Conference on Pervasive Computing and Communications (PerCom 2005), Kauai Island, Hawaii, July 2005.

[3] L. Zhou, Z.J. Haas, "Securing Ad hoc Networks", IEEE, Networks Magazine,Vol. 13, no 6, November/Dec 1999.

[4] S. Buchegger and J. L. Boudec. Performance Analysis of the CONFIDANT protocol: Cooperation of nodes Fairness in dynamic ad- hoc Networks. In Proceedings of IEEE/ACM Symposium on Mobile AdHoc Networking and Computing (MobiHoc), Lausanne, CH, June 2005.

[5] M. Roesch. Snort: Lightweight intrusion detection for networks. In Proceedings of the 1999 USENIX LISA Systems Administration Conference, November 1995.

[6] S. Wu and U. Manber. A fast algorithm for multi-pattern searching. Technical Report TR-94-17, UniversiAho and M. Corasick, VolNo 18,Jan 1994

[7] Fast pattern matching: an aid to bibliographic search.Commun. ACM, 18(6):333-340, June 1994.

[8] E. Royer, C-K Toh, "A Review of Current Routing Protocols for ad- hoc Mobile Wireless Networks", IEEE personal communications, Vol. 6, no 2, pp.46-55 April 1994.

[9] C. E. Perkins, P. Bhagwat, "Highly Dynamic Destination-Sequenced Distance-Vector Routing (DSDV) for Mobile Computers", in Proceedings of the SIGCOMM '94 Conference on Communications Architectures, Protocols and Applications, August 1994.

[10] K. G. Anagnostakis, E. P. Markatos, S. Antonatos, and M. Polychronakis, E2xB: Adomain-specific string matching algorithm for intrusion detection. In Proceedings ofthe 18th IFIP International Information Security Conference (SEC2003), May 1993.

[11] S.Antonatos, K. G. Anagnostakis, and E. P. Markatos, Generating realistic workloads fornetwork intrusion detection systems. SIGSOFT Software. Eng. Notes,29(1):207-215, 1992.

[12] R. Boyer and J. Moore, A fast string searching algorithm. Commun. ACM,20(10):762-772, October 1991.

[13] Y. –C. Hu, A. Perrig, D. B. Johnson, "Ariadne: A Secure On-demand Routing Protocol for Ad hoc Networks", in Proceedings of the 8th ACM International Conference on Mobile Computing and Networking (MobiCom'02), pp. 12-23,September1990.

[14] D.E Denning "An Intrusion Detection Model", IEEE Trans. Software Engg, Vol. Se-13, No 2,Feb 1987, pp 222-232