IJCSMS International Journal of Computer Science & Management Studies, Vol. 11, Issue 01, May 2011
ISSN (Online): 2231 –5268
www.ijcsms.com

"SAFE & SECURE DATA COMMUNICATION IN MOBILE AD-HOC NETWORK - BY USING IPSEC PROTOCOL"

NIDHI KANDHIL[1], Dr. ANIL KUMAR[2]
[1]nidhikandhil@gmail.com-Rohtak, Haryana (India)
[2]**Asstt. Professor & Head, Dept. of Computer Science & Applications,**
Pt. N.R.S. Govt. College, Rohtak (India)

Abstract

Ad-hoc networks are a new paradigm in wireless communication due to its high significance in various sensitive and emergency operations. An Ad-hoc Network is a multi hop wireless network. Typically network nodes are interconnected through wireless interfaces and unlike traditional networks lack specialized nodes i.e. routers, that handle packet forwarding. Ensuring secure route doesn't guarantee a secure path for data communication in this wireless network. Any node within the secure route might be compromised at any time and become malicious to launch attack. So security for data packet should be introduced to defend against these attacks. This part of the research proposed model to implement IP Security or IPSec to for secure data transmission after route establishment in ad-hoc network paradigm.

Key words: Ad-hoc, wireless network, IPSec, TCP/IP

I. INTRODUCTION

Ad-hoc wireless network provides mobile communication capability to satisfy a need of a temporary nature and without existence of any well-defined infrastructure. Detail analysis of ad-hoc network reveals that ensuring security is a major concern for researchers of this network. Ad-hoc networks are wireless networks where nodes communicate with each other using multi-hop links. There is no stationary infrastructure or base station for communication. Each node itself acts as a router for forwarding and receiving packets to/from other nodes. Routing in ad-networks has been a challenging task ever since the wireless networks came into existence. The major reason for this is the constant change in network topology because of high degree of node mobility. A number of protocols have been developed for accomplish this task. Some of them are DSDV and AODV routing protocols.

An ad-hoc network is a multi hop wireless network. A node communicates with another distant node (i.e. out of its radio range) by hop-by-hop basis where every node acts as a router.
There are some unique and attractive features of mobile ad-hoc network (MANET) as such:

1. No fixed infrastructure and centralized administration
2. Automatic self-configuration and maintenance
3. Quick deployment
4. No predefined topology

IPSec is a set of open standard protocols that govern the secure exchange of data across public networks. IPSec works on Layer 3 and above for TCP/IP and the Network layer of the OSI layer model. By running on Layer 3, IPSec is able to function transparently for applications running on application layer. So it is transparent for all application. The application does not require any knowledge of IPSec in order to use it. IPSec protocol provides an end user to end user traffic with ensuring authenticity and confidentiality of data packet.

The basic services that IPSec provides are:-

1. Access Control How should the load on the visited Web sites be minimized?
2. Connectionless integrity
3. Origin authentication
4. Replay protection
5. Rejection of replayed packet

All these services provide greater security to the data communication in any network, That's why the research proposed for secure data

communication in ad-hoc network by IPSec protocol.

Internet Protocol Security (IPSec) is a protocol suite for securing Internet Protocol (IP) communications by authenticating and encrypting each IP packet of a data stream. IPSec also includes protocols for establishing mutual authentication between agents at the beginning of the session and negotiation of cryptographic keys to be used during the session. IPSec can be used to protect data flows between a pair of hosts, between a pair of security gateways (e.g. routers or firewalls), or between a security gateway and a host. IPSec is a dual mode, end-to-end, security scheme operating at the Internet Layer of the Internet Protocol Suite or OSI model Layer 3. Some other Internet security systems in widespread use, such as Secure Sockets Layer (SSL), Transport Layer Security (TLS) and Secure Shell (SSH), operate in the upper layers of these models. Hence, IPSec can be used for protecting any application traffic across the Internet. Applications need not be specifically designed to use IPSec. The use of TLS/SSL, on the other hand, must typically be incorporated into the design of applications.

IP sec is a successor of the ISO standard Network Layer Security Protocol (NLSP). NLSP was based on the SP3 protocol that was published by NIST, but designed by the Secure Data Network System project of the National Security Administration (NSA).

IPSec is officially specified by the Internet Engineering Task Force (IETF) in a series of Request for Comments addressing various components and extensions, including the official capitalization style of the term.IPSec define encryption, authentication and key management routines for ensuring the privacy, integrity and authenticity of data in a VPN as the information traverses public IP networks. Because IPSec requires each end of the tunnel to have a unique address, special care must be taken when implementing IPSec VPNs in environments using private IP addressing based on network address translation. Fortunately, several vendors offer solutions to this problem. However, they add more management complexity.

II. ROUTING IN AD-HOC NETWORKS

A good number of routing protocols are proposed for ad-hoc network, which are broadly classified into two categories. One is Reactive routing or Table Driven and another is Proactive routing or Source Initiated on Demand. In reactive approach routing information is stored and maintained before the actual transmission begins. From the application perspective it has the advantage of minimum initial delay as the desired route is already established. Destination-Sequenced Distance-Vector Routing (DSDV), Wireless Routing Protocol (WRL) is examples of reactive routing. The proactive routing or 'source initiated on-demand' routing protocols create routes only when a source needs to communicate with another node whose path is not known to the source. Ad-hoc On-Demand Distance Vector (AODV), Dynamic Source Routing (DSR) are examples of this type of routing. Some routing protocols applied the combination of both reactive and proactive routing. Zone Routing Protocol is such a protocol.

AODV ROUTING PROTOCOL

Ad-hoc On-Demand Distance-Vector (AODV) routing protocol is specifically designed for mobile ad-hoc wireless network. It provides very quick and efficient route establishment between communicating nodes. In most of the protocols the overhead is incurred by the fact that each transmitted packet contains the source route to the destination information.

AODV protocol eliminates this problem by maintaining only the next hop information to reach a particular destination. So routing message does not have an increasing size. A monotonically increasing sequence number is used to prevent replay attacks and to ensure loop free routing among the nodes.

Two mechanisms are used to secure the AODV messages: digital signatures to authenticate the non mutable fields of the messages, and hash chains to secure the hop count information.

SAODV ROUTING PROTOCOL

The Secure Ad hoc On-Demand Distance Vector Routing Protocol (SAODV) is an extension of the AODV routing protocol that can be used to protect the route discovery mechanism providing security features like integrity, authentication and non-repudiation. SAODV assumes that each

ad hoc node has a signature key pair from a suitable asymmetric cryptosystem. Further, each ad hoc node is capable of securely verifying the association between the address of a given ad hoc node and the public key of that node. Achieving this is the job of the key management scheme.

III. Previous Works

This section describes some previous works in the literature including various strategies and techniques revised by various authors who have been worked on security issues provide in mobile Ad-hoc network.

Manel Gerrero Zapata and N. Asokan [4] gives a solution for security in AODV routing protocol, called as Secure AODV (SAODV). A route request single signature extension (RREQ-SSE) is included with the RREQ packets. Based on the maximum diameter of the network the initiator estimates the maximum hop count, and generates a one-way hash chain of length equal to the maximum hop count plus one. Two signatures are used before sending the packet, one for RREQ packet and another one for the hash chain. Both signatures are included in the RREQ-SSE. Hop count is also used in the SAODV proposal. It is termed as hop-count authenticator. For instance, if the chain of hash values h0, h1, h3,……,hn are generated such that hi=H[hi+1] then the hop-count authenticator hi represents the hop count of N-i. To forward a RREQ packet in SAODV a node first authenticates the RREQ to check that each field is valid. Then it increments the value of hop count field and computes the hash value of hop count authenticator. Finally it rebroadcasts the RREQ along with the RREQ-SSE extensions. When the RREQ reaches the destination, it validates the RREQ-SSE extensions and returns a RREP if the authentication is successful. In order to prevent false route error message (RERR), SAODV employs hop-to-hop signature generation scheme.

Arun Kumar Bayya, Siddhartha Gupta, Yogesh Kumar Shukla, Anil Garikapati[11] focuses on three areas of ad-hoc networks. They are: key exchange and management, routing, and intrusion detection. They introduce secure aware ad hoc routing (SAR) by making use of the trust level and a negotiable secure association between source and destination. Every node in the network also acts as an IDS agent and runs independently to monitor intrusion in this wireless network. Every IDS agent consists of local data collection, local detection engine and cooperative detection module.

Manel Guerrero Zapata [14] of MANET working group proposed secure AODV routing protocol. Details of the work are highlighted in chapter 4. Mainly the research introduces digital signature and hash function to overcome different types of attack possible in AODV routing protocol. David Cavin, Yoav Sasson, Andre Shipper make an interesting comparative study among three different simulators i.e. OPNET, NS-2, GloMoSim. The result of their comparative simulation encourages our research to simulate the proposed IPSec implementation by NS-2.

Zhou Lindong and Zygmunt J. Hass [15] discuss ad-hoc networks and their different security aspects. All challenging issues such as key management secure routing and secure models of ad-hoc networks also discussed by the authors. The authors of this research introduce the threshold cryptography concept by distributing trust level among different nodes in the network. Here a threshold number of node can participate in the cryptographic operation, so if any node is compromised it does not hamper the cryptographic operation of the network. All nodes participating in the cryptographic operation must achieve a certain level of trust among themselves.

IV. RESEARCH METHODOLOGY

The research methodology spreading into four phases such as phase1; phase2; phase3; phase4; objectives of the study.

PHASE-1

The research initially carries out through literature survey. At the initial stage extensive study in the area of existence routing protocol, limitations of the existence network infrastructure of ad-hoc network and related work in this area has been employed.

This phase also cover literature survey for simulation environment for ad-hoc network. In order to carry out the activity the research chose NS-2 simulator and initiate attempt to simulate

existence ad-hoc environment by this simulator. The primary goal in this phase is to identify and establish concrete boundary in the related work.

PHASE-2

This phase attempt to determine the possible advantages and disadvantages of the existing ad-hoc networks and routing protocols. A brief study of AODV routing protocol and SAODV
.Security aspect of ad-hoc networks is also analyzed in this phase.

PHASE-3

The research proposed a secure data communication model in this phase. Details of IPSec are also analyzed for secure data communication in ad-hoc networks. Some parameters of IPSec and working principal are also elaborated in this phase.

PHASE-4

The parameters and working principal introduced in phase 3 will simulate in the NS-2 environment in this final phase of the research. Data collected from the NS-2 simulation environment analyzed in this phase. A comparison between two different protocols of IPSec implementation has been also made in this phase for determine the feasibility of implementing the proposed model in ad-hoc networks.

OBJECTIVES OF STUDY

Main objectives and motivation of the research are:-

i. Ensuring secure data communication in ad-hoc networks
ii. Proposal to implement IP Sec in ad-hoc network.
iii. Simulate the proposed IP Sec implementation model by using NS-2 simulator.
iv. Compare results for two IP Sec protocols for secure data communication in ad-hoc networks.

LIMITATION OF STUDY

i. The main limitations of the present study are as under:
ii. The sample of study is restricted to only wireless mobile ad-hoc network..
iii. Primary data collected through the sample survey is not efficiently for secure data communication because no pre-deployed infrastructure such as centrally administered routers or strict policy to support end to end routing.
iv. So to implement secured routing in AODV protocol in a network environment with dynamic topology, limited computational Abilities as well as strict power constraints is a really a challenging task.

V. PROPOSED ARCHITECTURE OF IPSEC PROTOCOL

Ensuring secure route doesn't guarantee a secure path for data communication in this wireless network. Any node within the secure route might be compromised at any time and become malicious to launch attack. So security for data packet should be introduced to defend against these attacks. Besides, IP packets have no inherent security. It is relatively easy to forge the addresses of IP packets, modify the contents of IP packets, replay old packets as well as inspect the contents of IP packets during transit. So no guarantee can be given that IP data grams received are (1) from the claimed sender means source address in the IP header (2) that it contain the original data that the sender placed in them
(3) that the original data was not intercepted by a third party while the packet was being sent from source to destination. This part of the research proposed model to implement IP Security or IPSec to for secure data transmission after route establishment in ad-hoc network paradigm.

IPSec is a set of open standard protocols that govern the secure exchange of data across public networks. IPSec works on Layer 3 and above for TCP/IP and the Network layer of the OSI layer model. By running on Layer 3, IPSec is able to function transparently for applications running on application layer. So it is transparent for all application. The application does not require any knowledge of IPSec in order to use it. IPSec protocol provides an end user to end user traffic with ensuring authenticity and confidentiality of data packet.

The basic services that IPSec provides are:-

1. Access Control How should the load on the visited Web sites be minimized?
2. Connectionless integrity
3. Origin authentication
4. Replay protection
5. Rejection of replayed packet

VI. IPSec Implementation

IPSec can be implemented and deployed in the **end hosts** or in the **gateways/routers** or in both. Where in the network IPSec is deployed depends on the security requirements of the users.

Host Implementation

The proper definition of a host in this context is the device where the packet is originating. The host implementation has the following advantages:

- Provides security end to end
- Ability to implement all modes of IPSec security
- Provides security on a per flow basis
- Ability to maintain user context for authentication in establishing IPSec connections

Host implementations can be classified into:

1 Implementation integrated with the operating system (OS). We call it host implementation (for lack of a better term!).

2 Implementation that is a shim between the network and the data link layer of the protocol stack. This is called the "Bump in the Stack" implementation.

Router Implementation

The router implementation provides the ability to secure a packet over a part of a network. For example, an organization may be paranoid about the Internet and not its own private network. In this case, it may want to secure only those packets destined to the geographically distributed branch as these packets traverse the Internet to build its VPN or intranet. The IPSec implementation provides security by tunneling the packets.

The router implementation has the following advantages:

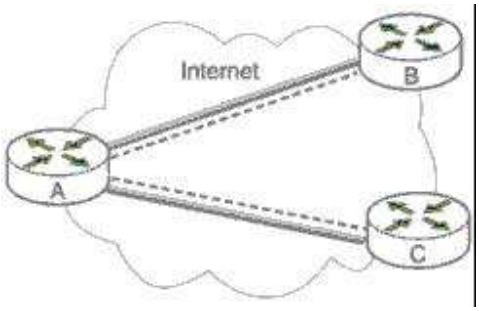
- Ability to secure packets flowing between two networks over a public network such as the Internet.
- Ability to authenticate and authorize users entering the private network. This is the capability that many organizations use to allow their employees to telecommute over the Internet to build its VPN or intranet. Previously, this was possible only over dial-ups (dialing through modem directly into the organization).

There are two types of router implementation:

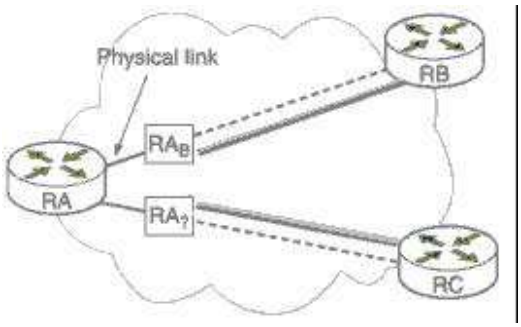
1 Native implementation: This is analogous to the OS integrated implementation on the hosts. In this case, IPSec is integrated with the router software.

2 Bump in the Wire (BITW): This is analogous to BITS implementation. In this case, IPSec is implemented in a device that is attached to the physical interface of the router. This device normally does not run any routing algorithm but is used only to secure packets. BITW is not a long-term solution as it is not viable to have a device attached to every interface of the router.

The network architectures for these implementations are shown in below figure.



Native Implementation deployment architecture



B BITW deployment architecture

VII. CONCLUSION & FUTURE WORK

Due to various emergency and sensitive applications, data packet security needs to be achieved in ad-hoc networks, but guaranteeing complete security in such a network may be impossible if the nodes are too mobile and suddenly compromised. The proposed IPSec implementation attempts to ensure data communication security. Sending and receiving data packets with IPSec needs more time as compared to sending data packets without IPSec.

There are ongoing modifications of AODV to fulfill the security requirements. The security proposal of this research is just the beginning of work in the area of data communication security in ad-hoc networks. Implementation of Encapsulating Security Payload and Authentication Header of IPSec ensure confidentiality, authenticity of data and as a result security will be further improved. The proposed implementation in this research is simulated using NS-2 simulator. If the proposal can be implemented in real wireless network environment then result can be more accurate. The research also does not provide any mechanism to detect intrusion in ad-hoc networks. So implementation of the proposal in real wireless networks and detection of intrusion may be a future direction for this research work.

REFERENCES

[1] Ilyas M. (2003), the Handbook of Ad-Hoc Wireless Networks. CRC Press, Florida.

[2] Charles P. Pfleeger, Shari Lawerence Pfleeger (2003), Security in Computing, Pearson Education, Singapore.

[3] Crawley, E., Nair, R. Rajagopalan, B., and Sandick, H. (Aug. 1998), A Framework for QoS-Based Routing in the Internet, Internet IETF RFC2386.

[4] Manel Guerrero Zapata (2001), Secure Ad hoc On-demand Distance Vector (SAODV) Routing draft-guerrero-manet-saodv, Nokia research center, Mobile Ad Hoc Networking Group, Internet Draft.

[5] Behrouz A. Forozan (2004), Data Communication and Networking, Tata McGraw- ill.

[6] A. Tanenbaum, Computer Networks (2003), (4th ed.), New Jersey, Prentice Hall PTR.

[7] William stalling, Network Security Essentials, Application and standard.

[8] William stalling, Cryptography & Network security, Principles & practice, (3 rd Ed.).

[9] Francisco J. Ros, Pedro M.Ruiz (2004), Implementing a New Manet Unicast Routing, Protocol in NS2, Department of Information and Communication technology, University of Munich, December.

[10] C. Perkins and E. Royer (2003), Ad-hoc On-Demand Distance Vector (AODV) Routing, RFC 3561.

[11] Arun Kumar Bayya, Siddhartha Gupta, Yogesh Kumar Shukla, Anil Garikapati, Security in ad-hoc networks, Computer science department, University of Kentucky.

[12] NS Simulator for beginners, Lecture notes, University de Los Andes, merida, Venezuela and ESSI, Sophia-Antipolis, France, December 2003.

[13] The network simulator, http: // www.isi.nsnam/ns

[14] M. Guerrero Zapata , N. Asokan, *Securing* Ad Hoc Routing Protocols. Proc. ACM Workshop on Wireless Security (WiSe), ACM Press, 2002, pp. 1–10

[15] Zhou Lindong, Zygmunt J. Hass, Securing Ad Hoc networks, Department of Computer Science, Cornell University, Ithaca, NY 14853.

[16] David Cavin, Yoav Sasson, Andre Schiper, On the accuracy of MANET simulators, Distributed Systems laboratory, Ecole Polytechnique Federale de Lausanne (EPFL), CH-1015 Lausanne.

[17] Bhajandeep Singh, Future of Internet Security – IPSec, http://www.securitydocs.com/library/2926

[18] Daniel Clark, Vulnerability's of IPSEC, A disc ussion of possible weakness in IPSEC implementation and protocols, SANS Institute 2002, Version 1.3