International Journal of Computing and Corporate Research
ISSN (Online) : 2249-054X
Volume 4 Issue 4 July 2014
International Manuscript ID : 2249054XV4I4072014-26

PERFORMANCE EVALUATION OF ROUTING PROTOCOL WITH IPSEC IN MOBILE AD HOC NETWORKS

Amit Sharma
Research Scholar
Punjab Technical University
Jallandhar, Punjab, India

Dr. S. N. Panda
Director Research
Chitkara University
Rajpura, Punjab, India

Dr. Ashu Gupta
Assistant Professor
Apeejay Institute of Management Technical Campus
Jallandhar, Punjab, India

ABSTRACT

A mobile ad hoc network represents a system of wireless mobile nodes that can freely and dynamically self-organize into arbitrary and temporary network topologies, allowing people and devices to seamlessly internetwork in areas without any preexisting communication infrastructure. To this end, mobile nodes must cooperate to provide the routing service. Routing in mobile environments is challenging due to the constraints existing on the resources (transmission bandwidth, CPU time, and battery power) and the required ability of the protocol to effectively track topological changes. An ad hoc network has certain characteristics, which imposes new demands on the routing protocol. The most important characteristics is dynamic network topology, which is consequence of node mobility. Nodes can change position quite frequently, which means we need a routing protocol that quickly adapts to topology changes. Many Routing protocols including multi layered security aspects have been developed for accomplishing this task. In this research work, an empirical methodology of network infrastructure is proposed and implemented that makes use of IPSec Protocol. Internet Protocol Security (IPSec) is specialized protocol suite for securing the Internet Protocol (IP) communications by the usage of authenticating and encrypting each IP packet of a communication sessions. This protocol IPSec makes use of and implements the protocols for establishing the mutual authentication between agents at the beginning of the session and negotiation of cryptographic keys to be used during the session.

International Journal of Computing and Corporate Research
ISSN (Online) : 2249-054X
Volume 4 Issue 4 July 2014
International Manuscript ID : 2249054XV4I4072014-26

IPSec is also used in protecting data flows between a pair of hosts (host-to-host), between a pair of security gateways (network-to-network), or between a security gateway and a host (network-to-host). In this research work, the comparative analysis and deep investigation of the methodology is implemented with and without the usage of IPSec. This research work highlights assorted factors in the IPSec for improving the security and integrity of the network.

INTRODUCTION

Wireless communication is becoming more popular among the users now a days and this is mainly due to the technological revolution in the field of mobile phones, laptops, PDA, wireless LAN and modems. It provides communication among a network of disconnected users; these users may be mobile or stationary. The use of wireless technology has become a ubiquitous method to access the Internet or connect to the local network whether in a corporate, educational, or private setting. Practically all laptop computers are currently sold with a built-in wireless adapter. In handheld units like PDAs, wireless adapters have also become standard and are now being introduced in some types of mobile phones. It is much easier and inexpensive to deploy a wireless network compared to a traditional wired network, as the required effort and cost of running cables are negligible. Furthermore, additional devices can be added to the network at no extra cost.

In order for a wireless equipped device to access other computers on the (wireless) local network or connect to the Internet it must associate with a wireless access point. A wireless access point is a device that allows devices equipped with wireless adapters to be linked together in a local area network (LAN) and to connect to a pre-existing wired LAN and via a gateway to get access to the Internet. Such networks are called wireless local area networks (WLANs) as the wireless access point is linking wireless devices without wires. Because of the convenience of not having to rely on wires, WLANs have become immensely popular. When devices equipped with wireless adapters are part of a WLAN and are managed by a wireless access point, their coordination is controlled by a centralized entity. The devices rely on the presence of a fixed infrastructure, i.e., wireless access points to work. Laptop computers must be within the range of a wireless access point to connect to other devices because the laptops must communicate via the access point.

There are two different approaches to establish the communication among a number of hosts:

a) First approach is to use an existing cellular hierarchy which carries data as well as voice; in the cellular network, there is a centralized administration or a fixed base station which handles routing and resource management procedures, since all the routing decisions are made in a centralized manner. Therefore these networks are also called Infrastructural based networks. But the main problem here is handoff between two areas when user moves from one cell to other. It becomes an important to transfer data without any delay while handoff. Another main problem is that it is limited to the area where network is present.

International Journal of Computing and Corporate Research
ISSN (Online) : 2249-054X
Volume 4 Issue 4 July 2014
International Manuscript ID : 2249054XV4I4072014-26

b) In the second approach we can form an ad hoc network among all users who wants to communicate with each other. This means all the users in the ad hoc network must be willing to forward data packets to make sure that the packets are delivered from the source to destination. This form of networking is smaller than the cellular approach and only limited in the range by the individual nodes transmission range. This system has its own advantages over cellular system and these are:

i) On demand setup

ii) Fault tolerance

iii) Unconstrained connectivity

A mobile ad hoc network (MANET) are defined as the category of wireless networks that utilize multi-hop radio relaying and are capable of operating without the support of any fixed infrastructure, hence they are also called Wireless infrastructure less networks. Basically it is a collection of nodes, which have the possibility to connect on a wireless medium and form an arbitrary and dynamic network with wireless links. That means that links between the nodes can change during time, new nodes can join the network, and other nodes can leave it. A MANET is expected to be of larger size than the radio range of the wireless antennas, because of this fact it could be necessary to route the traffic through a multi-hop path to give two nodes the ability to communicate. There are neither fixed routers nor fixed locations for the routers as in cellular networks. It consists of mobile nodes that use a wireless interface to communicate with each other. As all the routing decisions are made by the nodes itself. Therefore, in an ad hoc network the mobile nodes serve as both hosts and routers so they can forward packets on behalf of each other. A MANET is highly dynamic. Links and participants are often changing and the quality of the links as well. In this, asymmetric links are also possible. MANET is very useful in areas where no network exists and also in the remote location, especially for disaster management.

FEATURES

Mobile Ad hoc network has the following features:

1. AUTONOMOUS AND INFRASTRUCTURE-LESS

MANET does not depend on any established infrastructure or centralized administration. Each node operates in distributed peer-to-peer mode, acts as an independent router and generates independent data. Because of this any of the node can acts as a Host.

2. DISTRIBUTED OPERATION

As there is no background network available for the central control of the network operations, the control and management of the network is distributed among the terminals. The nodes involved in a mobile ad hoc network should collaborate amongst themselves and each node acts as a relay as needed, to implement functions e.g. security and routing. Also due to this feature any node can enter and leave the network at any time.

3. MULTI-HOP ROUTING

International Journal of Computing and Corporate Research
ISSN (Online) : 2249-054X
Volume 4 Issue 4 July 2014
International Manuscript ID : 2249054XV4I4072014-26

As in Infrastructure network nodes can communicate only in one hop wireless link to the base station and Multi Hop is not possible. But in MANET no default router available, every node acts as a router and forwards each other's packets to enable information sharing between mobile hosts. Here the multiple routes could be used. In case one route is not working, other routes are always available.

4. DYNAMIC NETWORK TOPOLOGY

Since the nodes are mobile, the network topology may change rapidly and unpredictably and the connectivity among the terminals may vary with time. The mobile ad hoc network should adapt to the traffic and propagation conditions as well as the mobility patterns of the nodes. The mobile nodes in the network dynamically establish routing among themselves as they move about forming their own network on fly.

5. VARIATION IN LINK AND NODE CAPABILITIES

Each node may be equipped with one or more radio interfaces that have varying transmission/receiving capabilities and operate across different frequency bands . This heterogeneity in node radio capabilities can result in possibly asymmetric links. In addition, each mobile node might have a different software/hardware configuration, resulting in variability in processing capabilities.

6**. Light-weight terminals**

Since In wireless infrastructure less network, all the nodes require portability, therefore nodes are having a size and weight constraints with less CPU processing capability, small memory size, and low power storage. If the battery size and processing capability increases then nodes becomes bulky and are not portable. So the routing protocols should optimally manage these resources. Such devices need optimized algorithms and mechanisms that implement the computing and communicating functions.

CHALLENGES

Regardless of the attractive applications, the features of MANET introduce several challenges that must be studied carefully before a wide commercial deployment can be expected. These include

1. Routing: Since the topology of the network is constantly changing, the issue of routing packets between any pair of nodes becomes a challenging task. Most protocols should be based on reactive routing instead of proactive. Multicast routing is another challenge because the multicast tree is no longer static due to the random movement of nodes within the network. Routes between nodes may potentially contain multiple hops, which is more complex than the single hop communication.

2. Security and Reliability : In addition to the common vulnerabilities of wireless connection, an ad hoc network has its particular security problems due to nasty neighbor relaying packets. The feature of distributed operation requires different schemes of authentication and key management. Further, wireless link characteristics also introduce reliability problems, because of limited wireless transmission range, broadcast nature of the wireless medium (e.g.

International Journal of Computing and Corporate Research
ISSN (Online) : 2249-054X
Volume 4 Issue 4 July 2014
International Manuscript ID : 2249054XV4I4072014-26

hidden terminal problem), and mobility-induced packet losses and data transmission errors.

3. Quality of Service (QOS): Every routing protocol has some quality of service incorporated within. So, Providing different quality of service levels in a constantly changing environment will be a challenge. The inherent stochastic feature of communications quality in a MANET makes it difficult to offer fixed guarantees on the services offered to a device. .

4. Power Consumption: For most of the light-weight mobile terminals, the communication-related functions should be optimized for lean power consumption. Conservation of power and power-aware routing must be taken into consideration

SECURING IP COMMUNICATIONS USING IPSEC -Internet Protocol Security (IPSec) is a protocol suite for securing Internet Protocol (IP) communications by authenticating and encrypting each IP packet of a communication session. IPSec 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 in protecting data flows between a pair of hosts (host-to-host), between a pair of security gateways (network-to-network), or between a security gateway and a host (network-to-host).

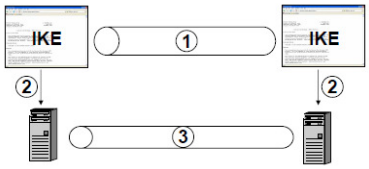

Figure 1 - IPSec Architecture

(1) Authentication, key establishment and negotiation of cryptographic algorithms

Protocols: ISAKMP, Internet Key Exchange (IKE), IKEv2

(2) Set keys and cryptographic algorithms

(3) Secure channel, which provides

Data integrity: using the Authentication Header (AH) protocol or the Encapsulating

Security Payload (ESP)

Confidentiality using ESP

ESP can provide both data integrity and encryption while AH provides only data

Integrity

IPSEC SECURITY OBJECTIVES

• It is not possible to send an IP datagram with neither a masqueraded IP source nor destination address without the receiver being able to detect this

• It is not possible to modify an IP datagram in transit, without the receiver being able to detect the modification

• Replay protection: it is not possible to later replay a recorded IP packet without the receiver being able to detect this

CONFIDENTIALITY

• It is not possible to eavesdrop on the content of IP datagrams

• Limited traffic flow confidentiality

SECURITY POLICY

Sender, receiver and intermediate nodes can determine the required protection for an IP packet according to a local security policy

Intermediate nodes and the receiver will drop IP packets that do not meet these requirements

Internet Protocol security (IPSec) uses cryptographic security services to protect communications over Internet Protocol (IP) networks. IPSec supports network-level peer authentication, data origin authentication, data integrity, data confidentiality (encryption), and replay protection.

IPSec is an end-to-end security scheme operating in the Internet Layer of the Internet Protocol Suite, while some other Internet security systems in widespread use, such as Transport Layer Security (TLS) and Secure Shell (SSH), operate in the upper layers of the TCP/IP model. Hence, IPSec protects any application traffic across an IP network. Applications do not need to be specifically designed to use IPSec. Without IPSec, the use of TLS/SSL must be designed into an application to protect the application protocols.

PROBLEM IN EXISTING SYSTEM

- The classical approach is not security and integrity efficient in terms of the implementation to any network scenario
- In specialized cases of static Network, the nodes may crash for assorted reasons
- The network may split into two or more disconnected partitions.
- The classical approach deteriorates or damage or even nullify the usefulness and effectiveness of the network.
- For these reasons, repairing partitions is a priority.
- The classical approach can be improved and enhanced to repair network partitions by using mobile nodes.
- By reasoning upon the degree of connectivity with neighbors, a mobile node finds the proper position where to stop in order to reestablish connectivity.
- Factors influencing the method performance are singled out and criteria for their selection are discussed.
- Using simulated environment, the proposed method can be proved efficient and effective not withstanding packet loss.

PROBLEM FORMULATED

The existing approaches of using secured and trusted protocols for any kind of network infrastructure. The IPSec protocols are needed in almost every network infrastructure to keep the data channel and transmission secured.

ADVANTAGES OF THE IPSEC PARADIGM

- Access control
- Connectionless integrity
- Data origin authentication
- Rejection of replayed packets
- A form of partial sequence integrity
- Confidentiality (encryption) In a firewall/router provides strong security to all
- Traffic crossing the perimeter
- Resistant to bypass
- Below transport layer, hence transparent to Applications
- Can be transparent to end users

International Journal of Computing and Corporate Research
ISSN (Online) : 2249-054X
Volume 4 Issue 4 July 2014
International Manuscript ID : 2249054XV4I4072014-26

- Can provide security for individual users if desired

ADVANTAGES OF THE PROPOSED SYSTEM

- The proposed system is generating efficient results in terms of the optimal solution when executed using IPSec.
- The proposed technique is efficient also in terms of the Jitter and Throughput despite of the number of iterations
- The limitations may be included regarding the proposed work in terms of its further enhancement using assorted metaheuristics.

The proposed system may give better results in executed using simulated annealing that is one of the prominent metaheuristic techniques

OUTPUT SCREENSHOTS AND RESULTS

Figure 3 – The Data Transmission Rate in Existing and Proposed Techniques

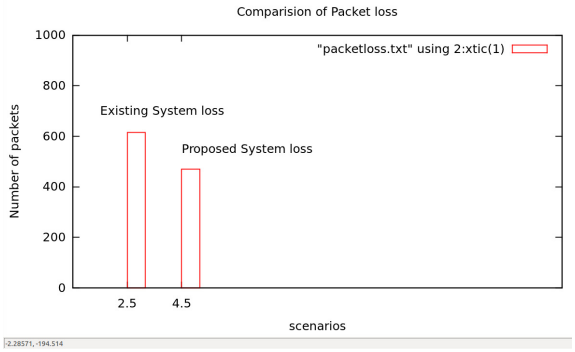

Figure 2 – Comparative Analysis of Packet Loss Rate in Existing and Proposed Approach

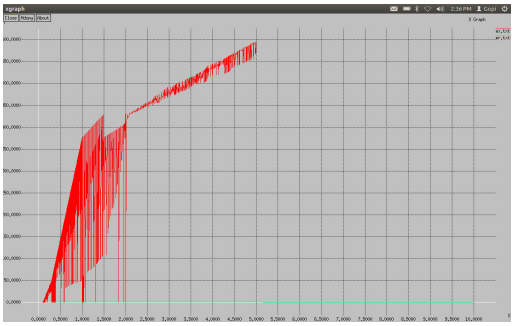

Figure 3 – Comparative Analysis of Packet Loss Parameter in Existing and Proposed Approach

CONCLUSION

Ad-hoc networking is a need of time and a very hot concept in computer communications. This field of research is a state-of-the-art and ongoing topic which many papers are still conducting to highlight and review different existing routing protocols. The importance of this type of research is proven by increasing number of survey researches which try to compare different protocols on the basis of various metrics so that the network can properly utilized at minimum resources. Till date the researchers have only focused on the routing protocols. More routing protocols can be taken into consideration and can

analyze the performance by varying the different parameters. A very important issue that needs to be considered is the security in an ad-hoc network. Routing protocols are prime targets for impersonation attacks. Because ad-hoc networks are formed without centralized control, security must be handled in a distributed fashion. Due to limited availability of resources, the routing protocols have to optimally manage these resources with the efficient utilization of the network. This is related to where the networks actually will be used for, connecting ad-hoc networks to the Internet through access points. This research work concentrates on securing the network scenarios from attacks and intrusions. In this work, the implementation of IPSec based protocol is done. For the future scope of work, the techniques can be associated with metaheuristic techniques.

REFERENCES

[1] Network Security Protocols and Defensive Mechanisms John Mitchell, 2009

[2] Network Security Chapter 4 The IPSec Security Architecture Network Security, WS 2009/10

[3] White Paper IPSec and SSL VPN Decision Criteria A Technology White Paper by Juniper Networks

[4] The IPSec Security Architecture for the Internet Protocol IPSec Architecture Security Associations AH / ESP IKE

[5] IP SECURITY (IPSEC) PROTOCOLS, Official WhitePaper

[6] Internet Security Protocols Bart Preneel February 2011

[7] APNIC eLearning: IPSec

[8] IRACST – International Journal of Computer Networks and Wireless Communications (IJCNWC), ISSN: 2250-3501 Vol.2, No6, December 2012 717 Internet Protocol Security(IPSec)

[9] Imperatives and Issues of IPSEC Based VPN, International Journal of Science and Modern Engineering (IJISME) ISSN: 2319-6386, Volume-1, Issue-2, January 2013 Miteshkumar Shaileshbhai Parmar, Arvind D Meniya

[10] PGP, IPSec, SSL/TLS, and Tor Protocols “Computer and Network Security”, 2014