Bulletin of Electrical Engineering and Informatics
ISSN: 2302-9285
Vol. 5, No. 4, December 2016, pp. 469~488, DOI: 10.11591/eei.v5i4.563

Secure Routing Protocol for Integrated UMTS and WLAN Ad Hoc Networks

Shashank Tripathi[1]*, A. K. Jain[2]
[1, 2] Department of Instrumentation and Control Engineering
Dr B R Ambedkar National Institute of Technology Jalandhar, India
*Corresponding author, e-mail: shashankt.ic.12@nitj.ac.in[1], jainak@nitj.ac.in[2]

Abstract

The integrated UMTS and WLAN ad hoc networks are getting more and more popular as they hold substantial advantages by next generation networks. We introduce a new secure, robust routing protocol specifically designed for next generation technologies and evaluated its performance. The design of the SNAuth_SPERIPv2 secure routing protocol takes advantage to the integrated network, maintaining Quality of Service (QoS) under Wormhole Attack (WHA). This paper compares performance of newly developed secure routing protocol with other security schemes for CBR video streaming service under WHA.

Keywords*: integrated UMTS and WLAN Ad Hoc network, QoS, routing, scalability, security, WHA*

1. Introduction

In the trusted environment, inter-domain packet routing in the Integrated Universal Mobile Telecommunications System (UMTS) and Wireless Local Area Network (WLAN) ad hoc multi-hop network [1] is used under the guidance of routing protocols. The development of secure routing protocol to defend against untrusted environment is research issue now a days. Most applications such as online transactions, critical business operations, military networks, etc., that run in untrusted environments wants secure communication and routing to protect network from unhealthy situations. The routing infrastructure of integrated network is vulnerable to a variety of attacks because there are no strong security services built in routing protocols. Most internet routing protocols provide authentication using plain-text password, that is easy for an adversary to make admission to an integrated network of manipulation routing information. We introduce a secure, robust routing protocol, namely SNAuth_SPERIPv2 periodic distance vector routing protocol using secure neighborauthentication for performing routing for untrustworthy environment. The Integrated UMTS and WLAN multi-hop networks support different class of services, namely: conversational, streaming, interactive, and background class service [2], [3], [4]. First two classes are guaranteed QoS classes (highly delay sensitive) and next two are non-guaranteed QoS classes (loss sensitive) [5]. CBR video streaming application is real-time asymmetric guaranteed class of service.

The rest of the paper is organized as follows: Section 2 discusses background: integrated UMTS and WLAN ad hoc networks vulnerabilities and attacks, section 3 introduce related work, section 4 discuses secure routing requirements and design of secure routing protocol for the integrated network and section 5 introduces performance evaluation. Finally, Section 6 concludes this paper.

2. Background: Integrated UMTS and WLAN Ad Hoc Networks Vulnerabilities and Attacks

The WLAN nodes of integrated UMTS and WLAN ad hoc network are capable of operating independently without any fixed infrastructure. The dynamic routing protocols in such network, find routes between these nodes and allowing packets to be sent on to a further destination network node [6]. The integrated network has unstable infrastructure vulnerability due to absence of wired network deployment in ad hoc network [7-8]. In RIPv2, there is several known security vulnerabilities exist because its routing update message contains a vector of pairs (destination distance) [9-10]. Some of attacks are discussed below.

Received June 9, 2016; Revised October 23, 2016; Accepted November 6, 2016

2.1. Router Impersonation

In router impersonation, an unauthorized node can connect easily to a routing domain and take part in routing. This may be trained with the help of IP spoofing. After performing impersonation, an attacker may alter or replay routing messages among legitimate routers. RIPv2 has clear-text password for authentication, which can easily breached. The keyed Message-Digest algorithm 5 (MD5) has been developed to replace this password authentication scheme [11]. Keyed mechanism is better, but also vulnerable due to compromised router which may disclose keying materials of all routers [9-10].

2.2. Prefix Impersonation

In prefix impersonation, an unauthorized or malicious node may claim a zero distance to those routers who does not directly connected to the network subnet (prefix). The MD5 authentication scheme [11] is not enough for this attack. Prefix impersonation can easily launch Denial of Service (DoS) in inter-domain (e.g., BGPv4 [12]) as well as intra-domain routing protocol (e.g., RIPv2) [9-10]. In the ARPANET [13], a similar incident has occurred known as blackhole attack.

2.3. Distance Fraud

In distance fraud, an unauthorized may claim a distance shorter or longer than the actual distance to a specific destination. The short distance fraud may be used to attract traffic to float different passive attacks e.g., session hijacking, eavesdropping etc. Whereas, long distance fraud can be used to avoid traffic and preserve its resources which may lead to unfair utilization of network links and cause network congestion due to consistency check of routing updates by routers. The long distance fraud is an active threat and may lead to launch a DoS attack on the network. The RIPv2 with MD5 authentication scheme is not enough for this attack [9-10].

2.4. Wormhole Attack (WHA)

WHA is a powerful active attack that may have severe consequences on distance vector routing protocols by showing shortest path for routing packets. The active WHA may be considered with passive eavesdropping threat [8], [14]. The eavesdropping threat has the capacity to intercept wireless traffic (breach confidentiality of the network) without altering and dropping of packets. In WHA, attacker developed a high bandwidth and low latency wireless tunnel between two malicious nodes. Attackers intercept packets at one location in the network and tunnel them to another location, and then replay (potentially altered) all tunneled packets into the network [8], [14], [15]. It works in two modes, namely: transparent mode and participant mode. In the transparent mode, wormhole malicious nodes are not victim network members. Where in participant mode, these nodes are the part of the victim network [16].

3. Related Work

This section focuses our study on the approaches proposed in literature that protect internet routing protocols (e.g. RIP, BGP, etc.) against active attacks. Several works already have been done to secure intra-domain distance vector routing (e.g. RIPv2 [17]) and inter-domain path vector routing protocol (e.g. BGPv4 [18]) using public-key digital signatures or Message Authentication Code (MAC) cryptographic approaches [9], [10], [19] and [20]. The related works of several researchers have reviewed below.

Hu et al. [8] introduced the severe WHA against wireless ad hoc network routing protocols, and proposed a new packet leashes mechanism for detecting and defending against this attack. A multi-hop wireless network is more vulnerable from this attack. Packet leashes (which can be either temporal or geographic leashes) are used to restrict the maximum transmission distance of routing packet for avoiding next hop fraud. The temporal leashes has implemented by TIK (TESLA with Instant Key disclosure) protocol based on a message authentication code (symmetric cryptographic primitives) which is an extension of the TESLA broadcast authentication protocol.

Hu et al. [21] proposed security mechanisms using efficient one-way hash functions and authentication trees for Secure Efficient Ad Hoc Distance Vector Routing protocol (SEAD) e.g. RIP against active attack. Their approach is one of the first robust approaches against multiple

uncoordinated attackers creating an incorrect routing state in victim nodes or compromising nodes in the network and may prevent shorter and same distance fraud. Limitation of the work is that it does not take up long distance fraud.

Hu et al.[22] proposed various security mechanisms using hash tree chain, tree-authenticated one-way chains and a one-way Merkle-Winternitz (MW) chain (new cryptographic mechanism) for distance vector routing protocol and cumulative authentication mechanism for path vector routing protocol against DoS attack. The distance vector (e.g. RIP) and path vector (e.g. BGP) use in the internet and can be applied to multi-hop wireless ad hoc networking.

Sanzgiri et al. [23] proposed a secure routing protocol for ad hoc network known as Authenticated Routing for Ad hoc Networks (ARAN) and successfully work against active tunnelling attacks which enable DoS attacks. It provides authentication using predetermined cryptographic certificates that guarantee end-to-end authentication to secure shortest path attack.

Hu et al. [24] proposed a secure distance vector routing protocol for ad hoc network known as Rushing Attack Prevention (RAP) protocol against rushing attacks which enable DoS in network. This is secure neighbor authenticated multipath distance vector routing protocol and developed by generic approach. Due to route discovery techniques, the protocol has higher overhead, but performs well and provides a usable route against the active attack. They also propose to integrate different secure distance vector routing protocols with a secure neighbor authentication scheme to enhance security.

Hu et al. [25] proposed an on-demand secure ad hoc routing, called Ariadne against active attack. It can authenticate the routing message using highly efficient symmetric cryptographic primitives.

Wan et al. [10] proposed a secure distance vector routing protocol (S-RIP) which can be significantly applied to the non-trustworthy environment like ad hoc network and inter-domain routing.

Babakhouya et al. [9] proposed a secure distance vector routing protocol (S-DV) to detect malicious routing update for long or short distance fraud. This scheme proposed Distance Reply (DR) authentication mechanism for S-DV routers, which reduces overhead and scalability of S-DV routing protocol.

4. Secure Routing Requirements and Design of Secure Routing Protocol for the Integrated Network

In integrated UMTS and WLAN ad hoc network, the multi-hop WLAN ad hoc network is a routing attack prone region. This can make overall integrated network insecure. The security of vulnerable domain is maintained by a secure routing protocol. Most routing protocols provide authentication using plain-text password, which is easy for an adversary to make admission to an integrated network of manipulation routing information. For proper detection and authentication against WHAs on the integrated network, a Secure Neighborhood Authenticated Strict priority Equal-cost multipath RIPv2 (SNAuth_SPERIPv2) distance vector routing protocol is designed and for further enhancement of security in integrated network, integrate the secure distance vector routing protocol with different layer security schemes.

4.1. Design of SNAuth_SPERIPv2 routing protocol

The SNAuth_SPERIPv2 periodic distance vector routing protocol is the integration of secure neighbor authentication schemes with strict priority load balancing or equal-cost multipath RIPv2 routing protocol. That makes basic RIPv2 more robust and provides load balancing by spreading traffic along multiple equal cost paths.

4.1.1. The secure neighbor authentication (SNAuth) schemes

SNAuth schemes work with symmetric as well as asymmetric cryptography. In the SNAuth [24] with symmetric cryptography, the authentication variant is based on 16 byte pair-wise shared secret key [26] variant between sender and receiver nodes which is hidden from remaining users. Authentication variant in SNAuth with asymmetric cryptography is based on certification. In the SNAuth based on pair-wise shared secret variant, every sender node broadcasts its identity (SNAuth-HELLO) packets periodically after completing a previous session key and a neighboring receiver node of SNAuth-HELLO packet pre-shares this key with

the sender node and perform three-way challenge-response handshake to authenticate the sender node [27]. The challenge-response messages use a common secret key to encrypt and decrypt their nonce. Here, nonce is the 128 bit random number that may only be used once with particular authentication message. The Figure1 illustrates three way handshake based on pair-wise shared secret variant.

The second neighbor authentication method has slightly different challenge-response scheme where the receiver does not pre-share a master secret key with the sender. In the SNAuth based on certificate variant, the sender node broadcasts its certificate with a certified HELLO message and all neighboring receiver nodes of certified HELLO message perform two-way challenge-response handshake to authenticate sender node [28]. The challenge certificate messages uses, its own certificate and a common public key encrypted cipher-text signed by its own private key. The public key cryptosystem uses an Elliptic Curve Cryptosystem (ECC) [29] which has shorter certificate length and cipher-text length and offers less communication overhead. The response messages use a secret session key to encrypt and decrypt their nonce. The Figure2 illustrates two way handshakes based on certificate variant.

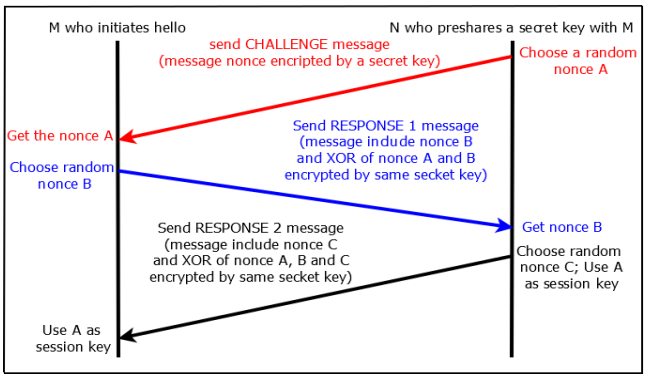

Figure 1. The Pair-Wise Shared Secret Variant of SNAuth

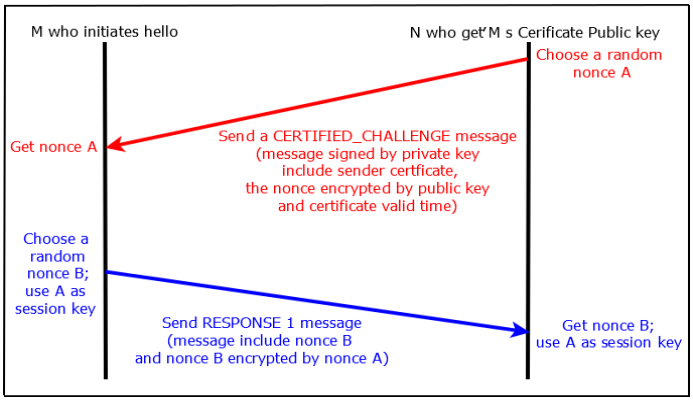

Figure 2. The SNAuth Variant based on Certification

4.1.2 Strict Priority Equal-cost multipath RIPv2 (SPERIPv2)

Routing Information Protocol version2 (RIPv2) is used for intra-domain distance vector routing. RIPv2 is classless dynamic routing protocol works on Bellman Ford algorithm. It is used by medium and small organizations (IP networks of moderate size) because it's limited hop-count (15 hops per packet) and a value of hop count metric = 16 is considered as destinations network unreachable. For extension of coverage area up to 64 hops, the WLAN ad hoc network is integrated with UMTS network. This integration support RIPv2 routing protocols to send their

packets to ubiquitous locations by the support of Gateway GPRS Support Node (GGSN) with GPRS tunnelling protocol (GTP).

RIPv2 is an extension of RIPv1. It is a UDP based protocol that means each router that uses this routing process will send and receive datagram on a UDP port. RIPv2 packet format is given in Figure 3. In Figure3 (a), command is 8 bit field that indicated the type of message. RIPv2 router uses two types of message to transmit and receive, namely: request and response for completing routing table. Address Family Identifier (AFI) is used for message authentication. In RFC-2453, RIPv2 support 20 byte plain text password for authentication which can easily breached. In RFC-2082, the keyed 16 byte MD5 has been developed to replace this password authentication scheme as shown in Figure3 (b). The unsigned 8 bit authentication data length present in field permits other authentication algorithms to be substituted by MD5. The Route Tag (RT) field is provided a method of separating internal intra-domain route provided by an Interior Gateway Protocol (IGP) from external inter-domain route by Exterior Gateway Protocol (EGP). RIPv2 has Variable Length Subnet Mask (VLSM) of the destination prefix specified in "IP Address", which support RIPv2 for Classless Inter-Domain Routing (CIDR) [30]. The next hop field is an advisory field which is used to eliminate extra hops in the packet being routed. If a packet routing is done by the originator of advertisement or received next hop is not directly reachable, then hop IP address is represented as 0.0.0.0. The RIPv2 message has an IP multicast address used for periodic broadcast in every 30 second by the regular routing update.

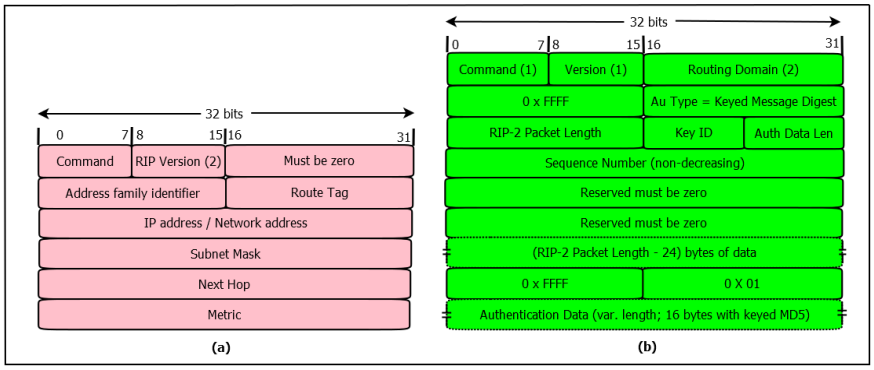

Figure 3. RIPv2 Message Format (a) with a Plain Text Password (b) Keyed MD5

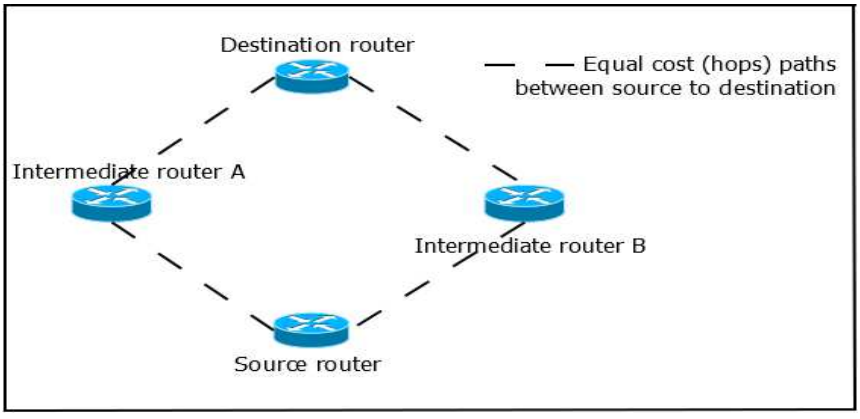

Figure 4. Equal Cost Path in RIPv2

Most of internet applications want more than one route to the destination. Hence, it is advantageous if a RIP router may learn equal cost routes. In RIPv2, the split horizon with poison reverse (techniques to avoid routing loops) may apply for equal cost routes by setting their metrics to infinity. By suitable modification in processing of response messages and correct

implementation of split horizon with poison reverse while advertising the routes to neighbors, up to 16 equal-cost paths in the RIPv2 route table can be implemented [31]. The meaning of equal cost multipath is that more than one equal cost path between the source destination. There should be advertise only one route with a cost of 16 (set metrics to infinity) after completion of poison reverse process, no matter router learns how many equal cost routes [17]. which helps to increase robustness of the routing protocol and provide load balancing by distributing traffic among all routers. Figure4 illustrates the equal cost path in RIPv2 between source and destination based on a Bellman Ford algorithm. The equal cost multiple path routing creates more overhead but makes available better performance in congestion and capacity by its load balancing capability. The strict priority equal cost multiple path routing provides proper and scheduled routes which decrease congestion and increase the network throughput. In this scheme, SNAuth has been performed on the basis of pair-wise shared secret variant. The maximum time interval for which a node waits to do the next neighbor detection handshake (secure-neighborhood expiration timeout) has been specified as 5000 ms [32].

4.2. Integrate the Secure Distance Vector Routing Protocol (SNAuth_SPERIPv2) with Different Security Schemes

The aim of this integration is to make integrated networks with very robust against WHA. The different security schemes are structured in below sub-sections.

4.2.1. SNAuth_SPERIPv2 with Direct Sequence Spread Spectrum (DSSS)

The aim of the integration of SNAuth_SPERIPv2 with DSSS is to provide security services for both routing protocol information and data message signal in an integrated network. In this scheme, SNAuth based on pair-wise shared secret variant has been performed.The DSSS technique offers jamming resistance at the physical layer. It has been implemented in WCDMA and 802.11b for providing secure data message signal in physical layer. A multi-layer wormhole adversary model with the network security models is used as attack model. WHAs on routing protocol produces DoS directly on network layer and indirectly on other layers of network that effect availability and integrity of routing packets. In typical DSSS technique, spreads the modulated signal by spreading signal is generated from a Pseudo-Noise (PN) sequence running periodically at a much higher rate than the original data signal for securing physical layer of the network against jamming DoS attacks [33]. The transmission and reception turnaround latency for UMTS and WLAN radios have been specified as 25µs and 2µs, respectively. In Figure5, DSSS system model has been illustrated.

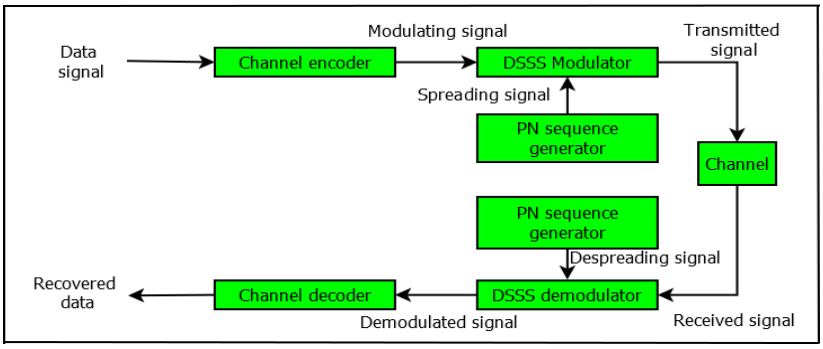

Figure 5. DSSS System Model

4.2.2. SNAuth_SPERIPv2 with Counter Mode Cipher Block Chaining Message Authentication Code Protocol (CCMP) - Advanced Encryption Standard (AES)

The aim of the integration of SNAuth_SPERIPv2 with CCMP-AES is to provide security services for both routing protocol information and data message in integrated network. SNAuth_SPERIPv2 provide routing protocol message authentication, where, CCMP-AES provides confidentiality, integrity and authentication of Media Access Control Protocol Data Unit (MPDU). In this scheme, SNAuth has been performed on the basis of pair-wise shared secret

variant. CCMP-AES is a Robust Security Network (RSN) data confidentiality and integrity protocol. It has been implemented in 802.11i as Wi-Fi Protected Access II (WPA2) for providing secure data frames in data link layer by utilizing the newest and strongest 128-bit AES encryption algorithm [34], [35]. This scheme protects integrated network from eavesdropping, alteration and dropping of data frames from unauthorized users. The processing delay for CCMP 'AES' encryption algorithm with CBC Hash-based Message Authentication Code (HMAC) has been specified as 5µs. CCMP originates cipher text and Message Integrity Code (MIC) for plain text MPDU using MPDU Data, Temporal Key (TK), Additional Authentication Data (AAD) and Nonce. The encrypted MPDU has been formed by combining cipher text and MIC with MPDU and CCMP header as shown in Figure 6(a). The MPDU plain text has been recovered using same keys and sequence number in decryption scheme as shown in Figure 6(b).

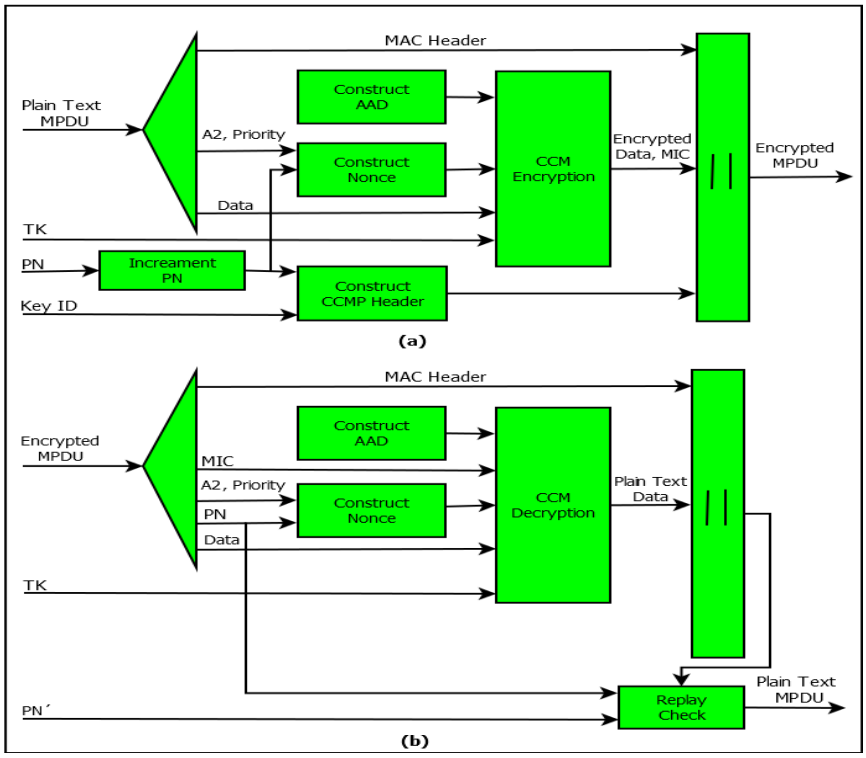

Figure 6. MPDU (a) Encryption (b) Decryption Scheme

4.2.3. SNAuth_SPERIPv2 with Internet Protocol Security (IPSec)

The aim of the integration of SNAuth_SPERIPv2 with IPSec is to provide security services for both routing protocol information and entire IP datagram in integrated network against WHA. SNAuth_SPERIPv2 provide routing protocol message authentication, where, IPSec provides confidentiality, integrity and authentication of an IP datagram. In this scheme, SNAuth has been performed on the basis of pair-wise shared secret variant. The proposed IPSec scheme uses a hybrid version of IPSec protocol that includes both Encapsulating Security Payload (ESP) and Authentication Header (AH) protocols [36], [37], [38] as shown in Figure7. ESP provides confidentiality with optional integrity and authentication by authenticated encryption algorithms.ESP works in two modes, namely: transport and tunnel mode. In tunnel mode, the ESP header is inserted before the original IP header and after the new IP header while protection applies to entire original IP datagram. In transport mode, the ESP header is inserted after the original IP header while protection applies to upper layer protocols. AH is a member of the IPsec protocol suite that provide guaranteed integrity and authentication of the entire original IP datagram including the new IP header. The hybrid version of IPSec has been used with ESP tunnel mode while protecting entire IP datagram with security association using the Internet Security Association and Key Management Protocol (ISAKMP) for protection of a

particular data flow between a pair of hosts of integrated network [39]. Common authentication algorithms have been used in ESP and AH that includes HMAC-MD5, HMAC- Secure Hash Algorithm 1(SHA1), HMAC-MD5-96, and HMAC-SHA1-96 with 10µs cryptographic processing delay. The Data Encryption Standard - Cipher Block Chaining (DES-CBC) encryption algorithm has been used in ESP with 10µs cryptographic processing delay.

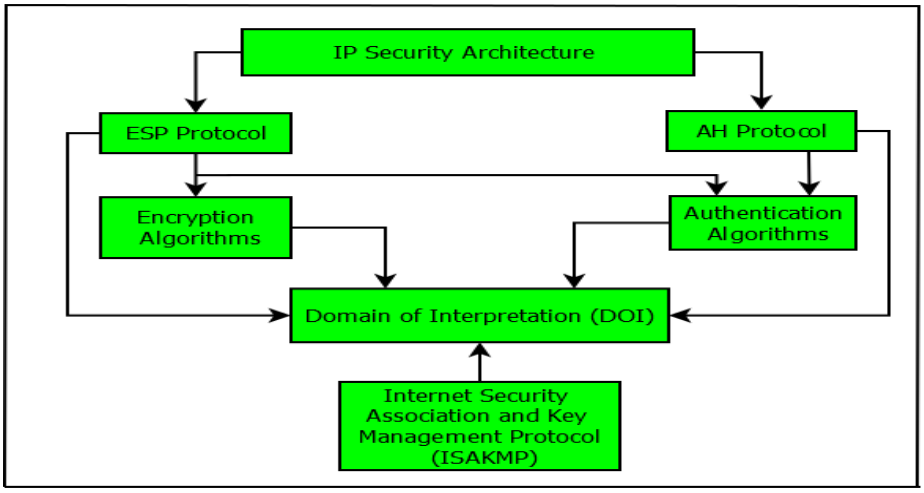

Figure 7. The IPSec Protocol Architecture

4.2.4. SNAuth_SPERIPv2 with Wireless Transport Layer Security (WTLS)

The aim of the integration of SNAuth_SPERIPv2 with WTLS is to provide the complete end-to-end security for routing protocol information, transport and upper layer in an integrated network. SNAuth_SPERIPv2 provide routing protocol message authentication, where, WTLS provides data privacy, authentication and integrity for Wireless Application Protocol (WAP) applications against man in the middle DoS attacks [23], [40], [41], 42]. In this scheme, SNAuth has been performed on the basis of certificate. WTLS security protocol is the security layer of WAP that defines a set of protocols in transport, security, transaction, session, and application layers to enable a creation of the value added mobile services such as online banking and ecommerce, etc. In this scheme, WTLS certificate has been implemented on each IP interface with the IPSec ESP in transport mode for transport and upper layer security. The WTLS uses modern cryptographic algorithms are MD5, SHA1, AES, 3DES, and Elliptic Curve Cryptography (ECC).

5. Performance of Integrated Networks

This section presents the simulation results which have conducted using QualNet to evaluate the performance of security schemes under WHA.

5.1. Configuration of the network including wormhole adversary

The Integrated UMTS and WLAN ad hoc network parameters of the models have been configured according to IEEE802.11g and Third Generation Partnership Project (3GPP) guidelines. Configuration of the integrated network parameters is given in Table1.

A wormhole adversary has been implemented in the vulnerable area of integrated network which can disrupt routing protocols by higher bandwidth and low latency wireless link tunnel as shown in Figure8. The wormhole is working in transparent mode as external adversary and performs DoS attack.

5.2. Performance Metrics

QoS performances of integrated networks under wormhole adversary and different security schemes have been analyzed using following metrics, namely: number of frames

dropped by wormhole (WH), routing overhead, average packet loss, average throughput, average end-to-end delay, average jitter and average hop-count [43].

CBR video streaming traffic has been employed for the QoS performance evaluation of integrated network under WHA. This traffic use network end-to-end delay as a performance metric.

Table 1. Configuration of the Network Parameters

Parameter	UMTS	WLAN
No. of channels (channel frequencies)	02 $\begin{pmatrix} 1.95\ \text{GHz UL} \\ 2.15\ \text{GHz DL} \end{pmatrix}$	01 $(2.4\ \text{GHz})$
Path-loss model	Two-ray	
Shadowing model	Constant without fading	
Antenna model	Omni-directional	
	PHY Layer	
Radio Type	Cellular PHY- UMTS PHY	802.11a/g radio
Maximum transmission power	30dBm	20dBm
User data rate (Offered)	384 Kbps	6 Mbps
Channel access scheme	FDD	CSMA/CA
Channel bandwidth	5 MHz	20 MHz
Modulation scheme	QPSK	OFDM-BPSK
Transmission and reception turnaround time	25 µs	2 µs
	MAC Layer	
MAC protocol	UMTS LAYER 2 – Cellular MAC	802.11
	Wormhole (WH) Adversary	
Wormhole-mode	Threshold	
Wormhole propagation delay	4.25 µs	

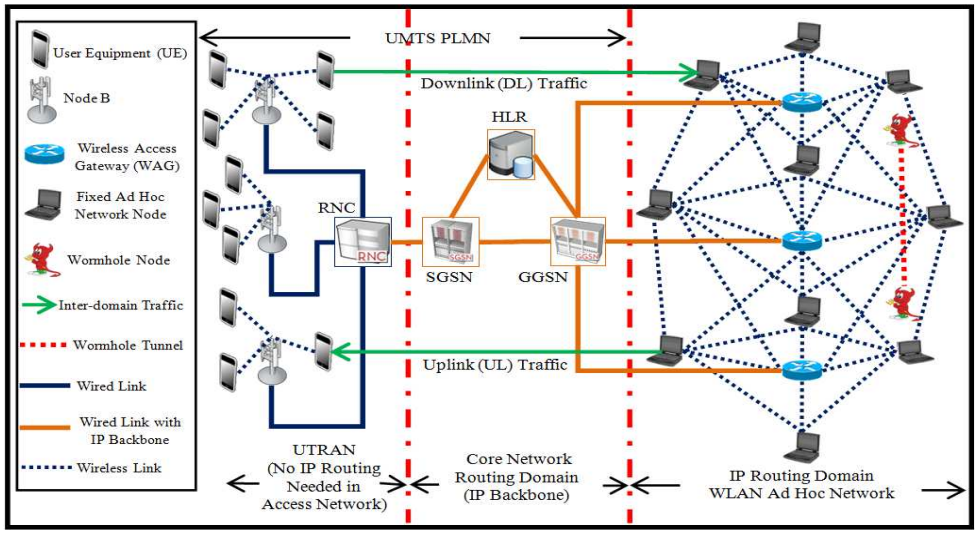

Figure 8.The Integrated UMTS and WLAN Ad Hoc Network with WH Adversary

5.3. Simulation Setup

In order to assess the contribution of proposed secure routing protocol (SNAuth_SPERIPv2) against WHA, simulation has been carried out with and without WHA. Simulations are run for one way video streaming application with Constant Bit-Rate (CBR) traffic. The simulations are performing for two different scenarios under constant traffic load and constant inter-domain traffic ratio. The simulation setup for two different scenarios is given in Table 2.

Table 2. Simulation Setup

Parameter	Scenario-1	Scenario-2
Packet size	512 Byte	512 Byte
Traffic load	25 packets/s	25 packets/s
Maximum number of network nodes	40 nodes (users)	200 nodes (users)
Distance between adjacent ad hoc nodes	100 m	100 m
Number of mobile nodes	zero	zero
Distance between adjacent Node Bs	1 km	2 km
Perturbation	zero	zero
Inter-domain traffic ratio	50% (25% uplink and 75% downlink flow)	25% (25% uplink and 75% downlink flow)
Intra-domain traffic ratio	zero	zero
Total simulation time	1800 s	1800 s
Area	3x3 km2	6x6 km2

Simulation scenario-1 is performed to evaluate the influence of the wormhole adversary on integrated network by increasing network size using an increasing number of fixed nodes from 8 to 40. The distribution of fixed nodes is uniform in 3x3 km^2 area while keeping network density constant. In this scenario, the stationery node does not deviate or move in any direction from their ideal grid position, which indicate perturbation about 0% and integrated network become highly stable. After introducing wormhole adversary, how performance of IP based routing protocols disturb is to be investigated.

Where, simulation scenario-2 is performed to evaluate the influence of the wormhole adversary on integrated network by increasing network size using an increasing number of fixed nodes from 40 to 200. The distribution of fixed nodes is uniform in 6x6 km2 area while keeping network density constant. In this scenario, the stationery node does not deviate or move in any direction from their ideal grid position, which indicate perturbation about 0% and integrated network become highly stable. After introducing wormhole adversary, how performance of IP based routing protocols disturb is to be investigated.

One uplink (from WLAN to UMTS user) flow and one downlink (from UMTS to WLAN user) flow for every user with transmission time interval (TTI) of 40 ms are considered as 100% inter-domain traffic ratio. The CBR streaming traffic has taken only one uplink or only one downlink flow for every user in the first scenario. The last scenario is taken only one uplink or only one downlink flow of every two users. In [44], the authors have investigated that the RAB provide high capacity and low QoS in uplink, and low capacity and high QoS in downlink end users to CN of an integrated network for asymmetric CBR video streaming class of service. Due to this, all simulation scenarios are performed simulation under the 25 % amount of uplink and 75% of downlink flows for this service.

In both scenarios, two external wormhole malicious nodes with a low-latency, high bandwidth link have introduced within ad hoc network routing domains and they are not part of the regular integrated network. The wormhole adversary nodes have the ability to intercept legitimate wireless packets from victim ad hoc network nodes and tunnelled selective packet from one location and replayed to other locations. The external adversary under threshold mode is fulfilled the above requirements and produces denial of service (DoS) in an integrated network. For defending against WHA, it is necessary to drops maximum frames/packets by wormhole tunnel before replayed. In all scenarios, the victim integrated network is counted minimum physical and link layer delay by choosing a suitable victim turnaround time.

A secure neighbor authenticated strict priority equal cost multipath routing information protocol version 2 (SNAuth_SPERIPv2) has been designed to protect an integrated network of wormhole routing attack. In order to evaluate security behavior in terms of QoS of integrated UMTS and WLAN network under WHA with different security scheme are structured in seven phases. In the first phase simulation has performed for RIPv2 routing protocol with MD5 authentication without WHA and in a second phase, simulation is performed under WHA. In the third phase, integration of SNAuth with SPERIPv2 is done and simulation has performed with this robust routing protocol under WHA. Fourth, fifth, sixth and seventh phase SNAuth_SPERIPv2 perform with DSSS, CCMP-AES, IPSec and WTLS, respectively under

WHA. All simulation scenarios are also considered the cryptographic latency used by all security schemes.

5.4. Simulation Results for Scenario -1

5.4.1. The Performance of Integrated Network on a Number of Frames Dropped by WH tunnel under Different Security Scheme while the Numbers of Fixed Network Nodes are Increased

Figure 9(a) shows, Frame dropped by WH is increasing with network size. The security schemes which have maximum number of frames dropped produce minimum DoS in an integrated network. SNAuth_SPERIPv2 routing protocol with IPSec have maximum number of frames dropped in all security schemes where RIPv2 with basic MD5 authentication scheme shows minimum frame dropped than other security protocols.

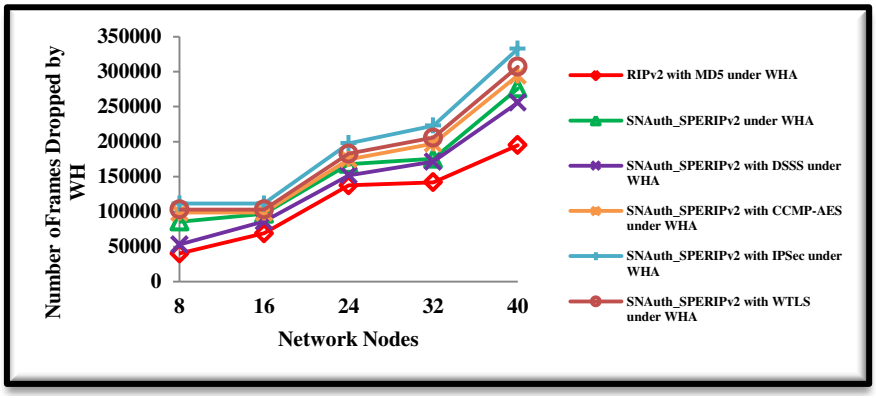

Figure 9(a).Number of frames dropped by WH tunnel versus number of network nodes

5.4.2. The Performance of Integrated Network on Routing Overhead under Different Security Scheme with and without WHA while the Numbers of Fixed Network Nodes are Increased

Figure 9(b) shows the routing overhead is increasing with the network size. The routing overhead of different security scheme with WHA rises as the number of frames dropped by WH tunnel is decreased. The main reason behind this increase in routing overhead is the loss of packets due to WHA. When WHA is more dominant then it intercepts maximum packets from the victim network and replayed them.

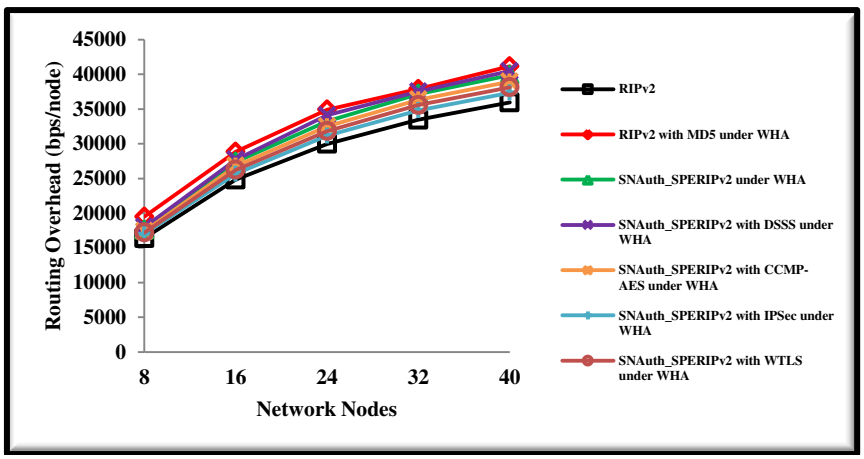

Figure 9(b). Average routing overhead versus number of network nodes

This Figure also shows RIPv2 with MD5 is more affected by WHA and have maximum routing overhead where SNAuth_SPERIPv2 routing protocol with IPSec is less effected by WHA and have minimum routing overhead among them. RIPv2 without WHA have minimum routing overhead from the secure routing protocols with WHA.

5.4.3. The Performance of Integrated Network on Average Packet Loss under Different Security Scheme with and without WHA while the Numbers of Fixed Network Nodes are Increased

Figure 9(c) shows the average packet loss is increasing with the network size. The average packet loss of different security schemes with WHA rises as the number of frames replayed on WH tunnel is increased means number of frame drops by WH tunnel decreased. This Figure also show RIPv2 with MD5 is more affected by WHA and have maximum average packet loss where SNAuth_SPERIPv2 routing protocol with IPSec is less effected by WHA and have minimum average packet loss among them. RIPv2 without WHA have a minimum average packet loss from the secure routing protocols with WHA.

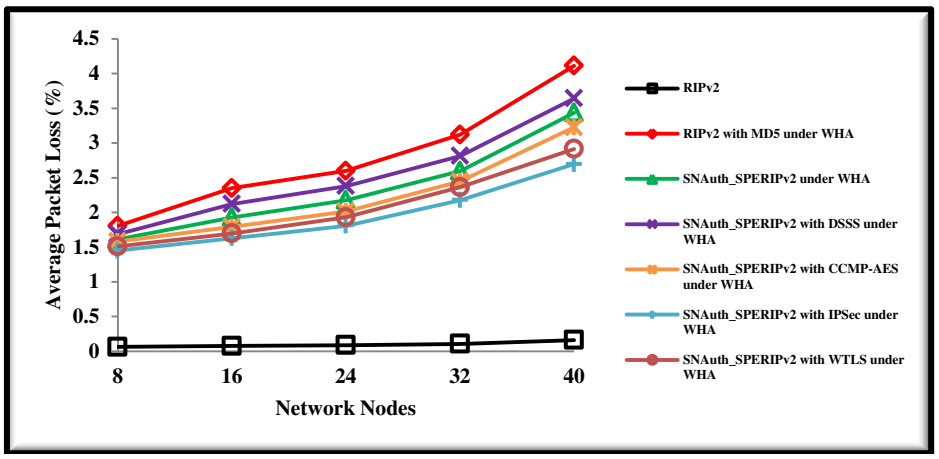

Figure 9(c). Average Packet loss versus Number of Network Nodes

5.4.4. The Performance of Integrated Network on Average Throughput under Different Security Scheme with and without WHA while the Numbers of Fixed Network Nodes are Increased

Figure 9(d) shows the average throughput is decreasing with the network size. The average throughput of different security schemes with WHA decreases as average packet loss is increased. This Figure also show RIPv2 with MD5 is having minimum average throughput where SNAuth_SPERIPv2 routing protocol with IPSec is having maximum average throughput among them under WHA. RIPv2 without WHA have maximum average throughput from the secure routing protocols with WHA.

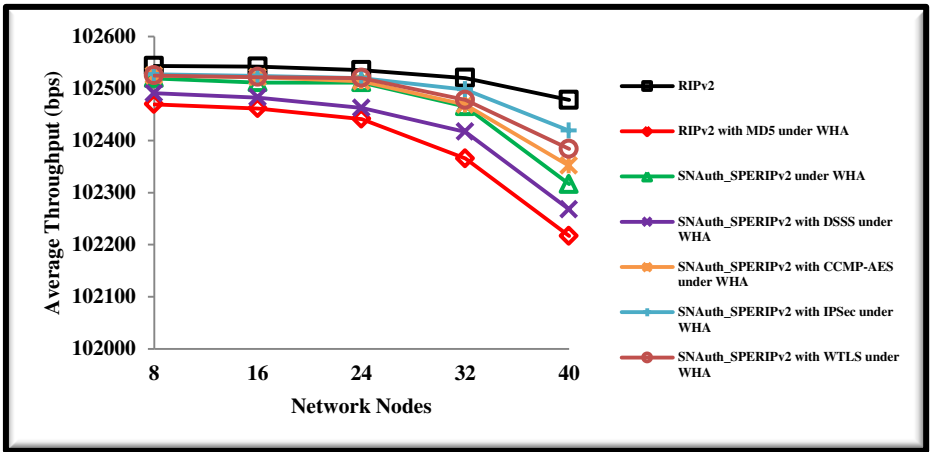

Figure 9(d). Average throughput versus number of network nodes

5.4.5. The Performance of Integrated Network on Average end-to-end Delay under Different Security Scheme with and without WHA while Numbers of Fixed Network Nodes are Increased

Figure 9(e) shows the average end-to-end delay is increasing with the network size. The average end-to-end delay of different security schemes with WHA increases as average packet loss is increased. This Figure also show RIPv2 with MD5 is having a maximum average end-to-end delay where SNAuth_SPERIPv2 routing protocol with IPSec is having a minimum average end-to-end delay among them under WHA. RIPv2 without WHA have minimum average end-to-end delay from the secure routing protocols with WHA.

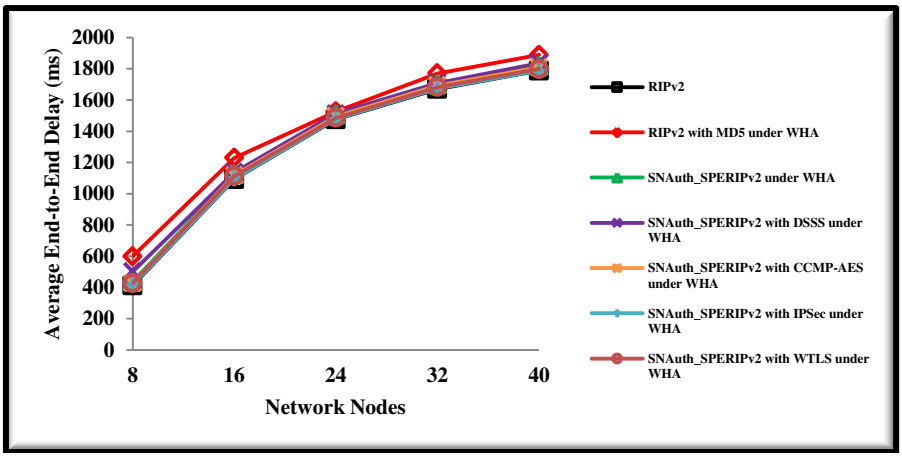

Figure 9(e). Average end-to-end Delay versus Number of Network Nodes

5.4.6. The Performance of Integrated Network on Average Jitter under different Security Scheme with and without WHA while the Numbers of Fixed Network Nodes are Increased

Figure 9(f) shows the average jitter is decreasing with the network size for the streaming service. The average jitter of different security schemes with WHA increases as average packet loss is increased. This Figure also show RIPv2 with MD5 is having maximum average jitter where SNAuth_SPERIPv2 routing protocol with DSSS is having minimum average jitter among them.

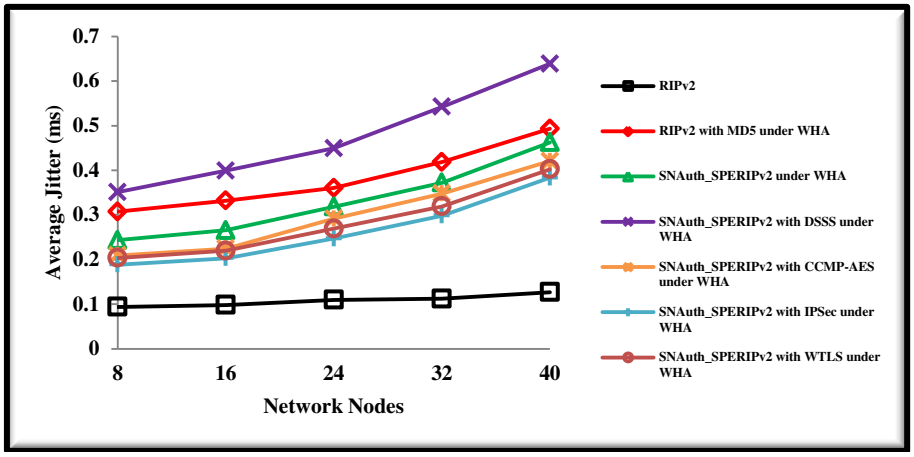

Figure 9(f). Average jitter versus Number of Network Nodes

5.4.7. The Performance of Integrated Network on the Average Hop - Count under Different Security Scheme with and without WHA while the Numbers of Fixed Network Nodes are Increased

Figure 9(g) shows, SNAuth_SPERIPv2 routing protocol is having more hop-count than RIPv2 because SNAuth_SPERIPv2 is multipath routing protocols, and it is more robust than RIPv2. The route selection algorithm favors stability to lower the hop - count. RIPv2 is more stable in sense of routing than SNAuth_SPERIPv2. SNAuth_SPERIPv2 routing protocol with IPSec is having maximum hop-count and minimum packet loss under WHA. Where RIPv2 routing protocol with MD5 is having minimum hop-count and maximum packet loss under WHA. To protect the network from WHA, it is necessary to make routing protocols robust.

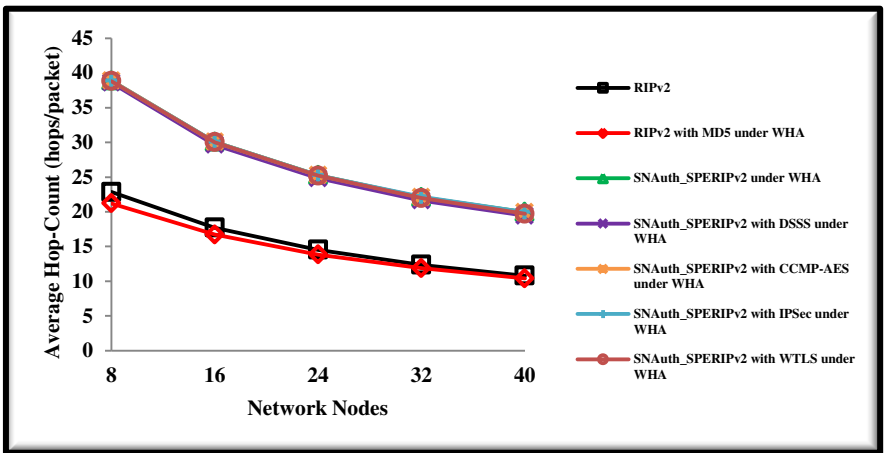

Figure 9(g). Average hop-count versus number of network nodes

5.5. Simulation Results for Scenario - 2

5.5.1. The Performance of Integrated Network on a Number of Frames Dropped by Wormhole Tunnel (WH) under Different Security Scheme while the Numbers of Fixed Network Nodes are Increased

Figure 10(a) shows the frame dropped by WH is increasing with network size. The security schemes which have maximum number of frames dropped produce minimum DoS in an integrated network. SNAuth_SPERIPv2 routing protocol with IPSec have maximum number of frames dropped in all security schemes where RIPv2 with basic MD5 authentication scheme shows minimum frame dropped than other security protocols.

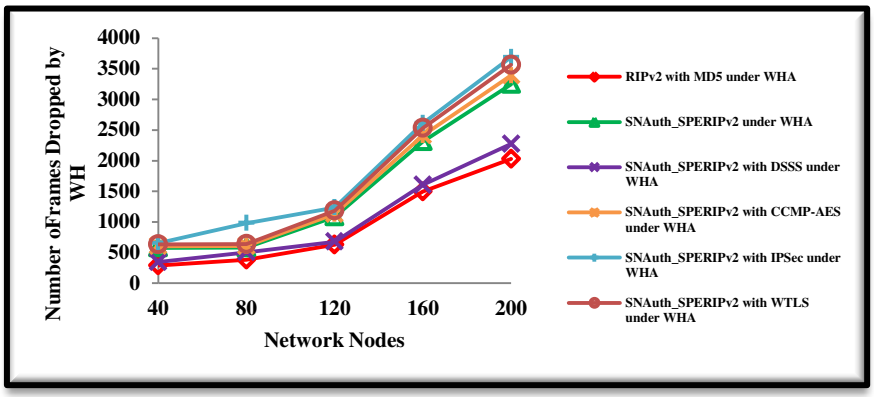

Figure 10(a). Number of frames dropped by WH versus number of network nodes

5.5.2. The Performance of Integrated Network on Routing Overhead under Different Security Scheme with and without WHA while the Numbers of Fixed Network Nodes are Increased

Figure 10(b) shows the routing overhead is increasing with the network size. The routing overhead of different security scheme with WHA rises as the number of frames dropped by WH tunnel is decreased. The main reason behind this increase in routing overhead is the loss of packets due to WHA. When WHA is more dominant then it intercepts maximum packets from the victim network and replayed them. This Figure also shows RIPv2 with MD5 is more affected by WHA and have maximum routing overhead where SNAuth_SPERIPv2 routing protocol with IPSec is less effected by WHA and have minimum routing overhead among them. RIPv2 without WHA have minimum routing overhead from the secure routing protocols with WHA.

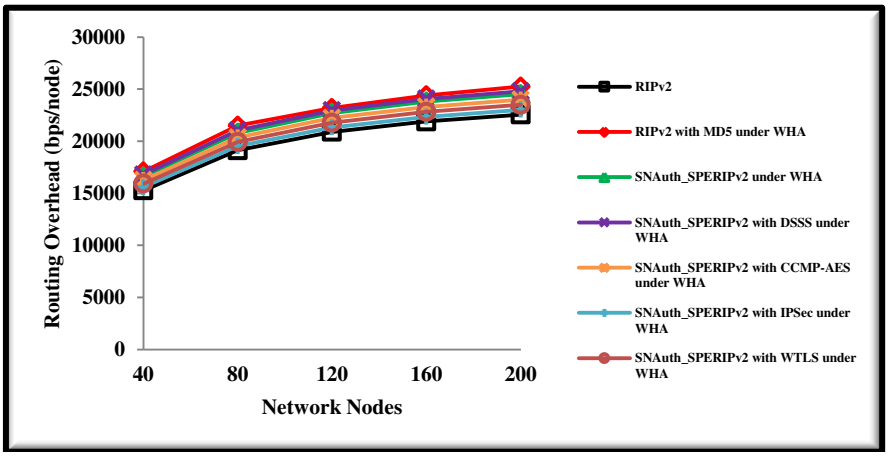

Figure 10(b). Average routing overhead versus number of network nodes

5.5.3. The Performance of Integrated Network on Average Packet Loss under Different Security Scheme with and without WHA while Numbers of Fixed Network Nodes are Increased

Figure 10(c) shows the average packet loss is increasing with the network size. The average packet loss of different security schemes with WHA rises as the number of frames replayed on WH tunnel is increased means number of frame drops by WH tunnel decreased. This Figure also shows RIPv2 with MD5 is more affected by WHA and have maximum average packet loss where SNAuth_SPERIPv2 routing protocol with IPSec is less affected by WHA and

have minimum average packet loss among them. RIPv2 without WHA have a minimum average packet loss from the secure routing protocols with WHA.

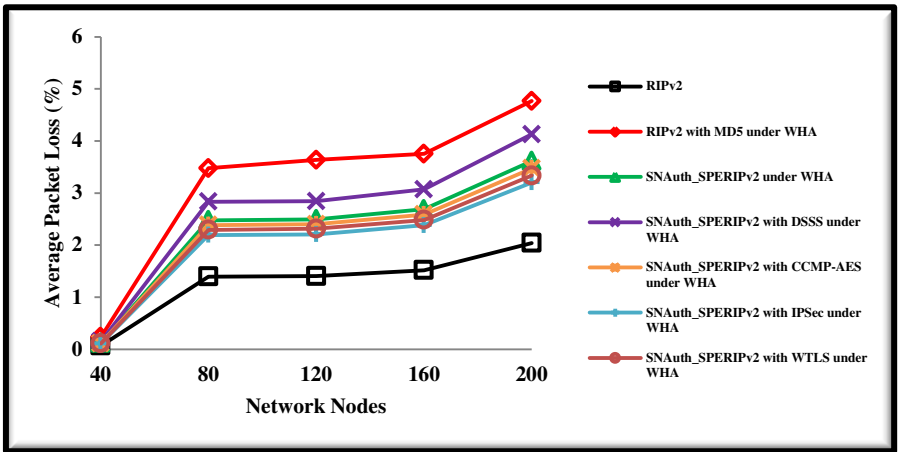

Figure 10(c). Average packet loss versus Number of Network Nodes

5.5.4. The Performance of Integrated Network, on Average Throughput under Different Security Scheme with and without WHA while the Numbers of Fixed Network Nodes are Increased

Figure 10(d) shows the average throughput is decreasing with the network size. The average throughput of different security schemes with WHA decreases as average packet loss is increased. This Figure also show RIPv2 with MD5 is having minimum average throughput where SNAuth_SPERIPv2 routing protocol with IPSec is having maximum average throughput among them under WHA. RIPv2 without WHA have maximum average throughput from the secure routing protocols with WHA.

5.5.5. The Performance of Integrated Network on Average end-to-end Delay under Different Security Scheme with and without WHA while Numbers of Fixed Network Nodes are Increased

Figure 10(e) shows the average end-to-end delay is increasing with the network size. The average end-to-end delay of different security schemes with WHA increases as average packet loss is increased. This Figure Also show RIPv2 with MD5 is having a maximum average end-to-end delay where SNAuth_SPERIPv2 routing protocol with IPSec is having a minimum average end-to-end delay among them under WHA. RIPv2 without WHA have minimum average end-to-end delay from the secure routing protocols with WHA.

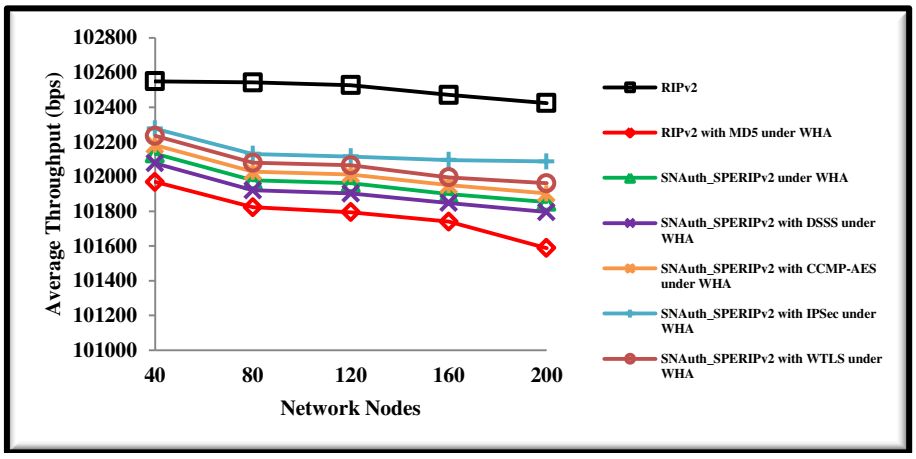

Figure 10(d). Average Throughput Versus Number of Network Nodes

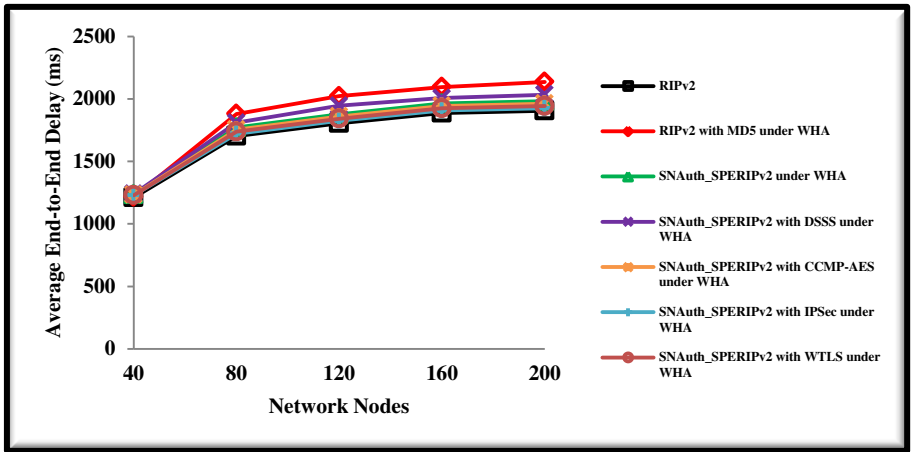

Figure 10(e). Average end-to-end Delay Versus Number of Network Nodes

5.5.6. The Performance of Integrated Network, on Average Jitter under Different Security Scheme with and without WHA while the Numbers of Fixed Network Nodes are Increased

Figure 10(f) shows the average jitter is decreasing with the network size for the streaming service. The average jitter of different security schemes with WHA increases as average packet loss is increased. This Figure also show RIPv2 with MD5 is having maximum average jitter where SNAuth_SPERIPv2 routing protocol with DSSS is having minimum average jitter among them.

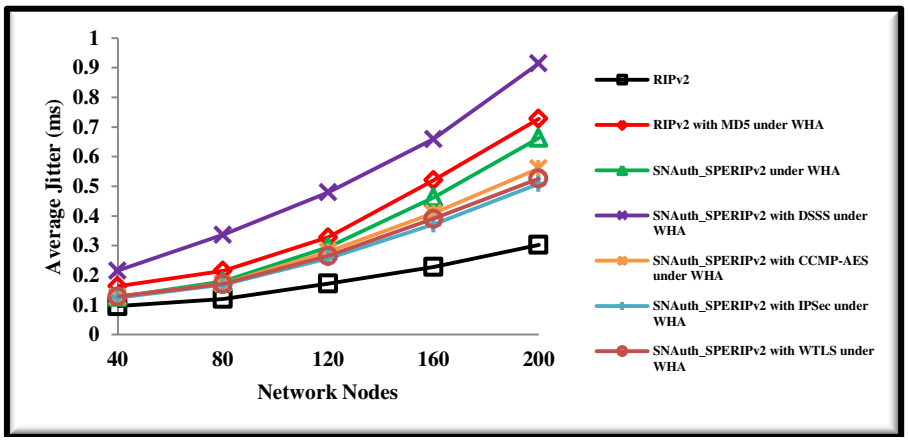

Figure 10(f). Average Jitter Versus Number of Network Nodes

5.5.7. The Performance of Integrated Network on the Average hop - count under Different Security Scheme with and without WHA while the Number of Fixed Network Nodes are Increased

Figure 10(g) shows, SNAuth_SPERIPv2 routing protocol is having more hop-count than RIPv2 because SNAuth_SPERIPv2 is multipath routing protocols, and it is more robust than RIPv2. The route selection algorithm favors stability to lower the hop - count. RIPv2 is more stable in sense of routing than SNAuth_SPERIPv2. SNAuth_SPERIPv2 routing protocol with IPSec is having maximum hop-count and minimum packet loss under WHA. Where RIPv2 routing protocol with MD5 is having minimum hop-count and maximum packet loss under WHA. To protect the network from WHA, it is necessary to make routing protocols robust.

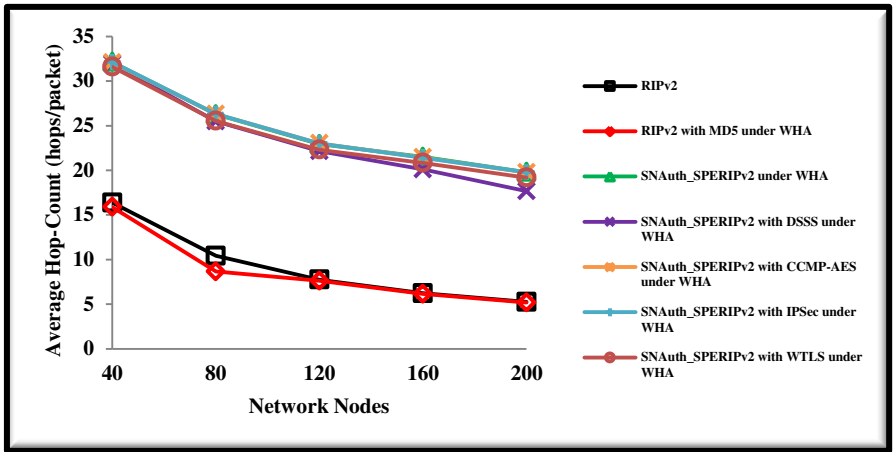

Figure 10(g). Average hop-count Versus Number of Network Nodes

6. Conclusion

Simulation results show that, proposed SNAuth_SPERIPv2 routing protocol with IPSec outperforms existing security schemes for the integrated UMTS and WLAN Ad Hoc networks under WHA, for highly jitter sensitive video streaming traffic under network node scalability. The secure protocol performs best when utilized in most common cellular and ad hoc network scenarios. The impact of WHA on a wireless ad hoc network under SNAuth_SPERIPv2 routing protocol is mitigating. All simulation result collected, are within limits as specified by 3GPP and ITU guidelines.

References

[1] 3GPP TS 23.934. 3GPP system to Wireless Local Area Network (WLAN) Interworking; Functional and Architectural Definition (Release 6). *3GPP TSG SA*, Aug. 2002.

[2] 3G TS22.105v3.9.0 Release 1999. Univarsal Mobile Telecommunications System (UMTS). Service Aspects, Services and Service Capabilities. June 2000.

[3] L Skorin-Kapov, D Huljenic, EN Tesla, D Mikic, D Vilendecic. Analysis of End-to-End QoS Networked Virtual Reality Services in UMTS. Networked Virtual Environ. *IEEE Commun*. Mag. 2004: 49–55.

[4] N Baghaei, R Hunt. Review of Quality of Service Performance in Wireless LANs and 3G Multimedia Application Services. *Comput. Commun. Elsevier B. V.* 2004; 27: 1684–1692.

[5] FC de Gouveia, T Magedanz. Quality of Service in Telecommunication Networks. *Telecommun. Syst. Technol. EOLSS*, 2: 1–8.

[6] B Kannhavong, H Nakayama, Y Nemoto, N Kato, A Jamalipour. A Survey of Routing Attacks in Mobile Ad Hoc Networks. *IEEE Wirel. Commun. Secur. Wirel. Mob. Ad Hoc Sens. Networks*. 2007: 85–91.

[7] MA Mobarhan, MA Mobarhan, A Shahbahrami. Evaluation of Security Attacks on UMTS Authentication Mechanism. *Int. J. Netw. Secur. Its Appl.* 2012; 4(4): 37–52.

[8] Y Hu, A Perrig, DB Johnson. Wormhole attacks in Wireless Networks. *IEEE J. Sel. Areas Commun.* 2006; 24(2): 370–380.

[9] A Babakhouya, Y Challal, M Bouabdallah, S Gharout. SDV: A new approach to Secure Distance Vector routing protocols. *IEEE Secur. /SECCOMW.* 2006: 1–9.

[10] T Wan, E Kranakis, P Oorschot. S-RIP: *A Secure Distance Vector Routing Protocol.* Proc. Appl. Cryptogr. Netw. Secur. 2004: 103–119.

[11] F Baker, R. Atkinson. RIP-II MD5 Authentication. *RFC 2082*, Jan. 1997.

[12] A Heffernan. Protection of BGP Sessions via the TCP MD5 Signature Option. *RFC 2385*, Nov. 1998.

[13] JM McQuillan, G Falk, I Richer. A Review of the Development and Performance of the ARPANET Routing Algorithm. *IEEE Trans. Comm.* Dec. 1978; 26(12): 1802–1811.

[14] A korba Abdelaziz, M Nafaa, G Salim. *Survey of Routing Attacks and Countermeasures in Mobile Ad Hoc Networks.* IEEE UKSim 15th Int. Conf. Comput. Model. Simul. 2013: 693–698.

[15] L Qian, N Song, X. Li. *Detecting and Locating Wormhole attacks in Wireless Ad Hoc Networks*

through Statistical Analysis of Multi-path. IEEE Commun. Soc. / WCNC. 2005: 2106–2111.
[16] I Hbabeh, I Khalil, A Khreishah, S. Bataineh. Performance Evaluation of Wormhole Security Approaches for Ad Hoc Networks. *J. Comput. Sci.*, 9(12); 2013: 1626–1637.
[17] G Malkin. RIP Version2. *RFC 2453*, Nov.1998.
[18] Y Rekhter, T Li. A Border Gateway Protocol4. *RFC 1771*, March.1995.
[19] S Kent, C Lynn, K. Seo. Secure Border Gateway Protocol (Secure-BGP). *IEEE J. Sel. Areas Commun.* April 2000; 18(4): 582–592..
[20] R White. Securing BGP Through Secure Origin BGP. *Internet Protoc. J.* Sept. 2003; 6(3): 15–22.
[21] Y Hu, DB Johnson, A Perrig. SEAD: Secure Efficient Distance Vector Routing for Mobile Wireless Ad Hoc Networks. *Ad Hoc Networks Elsevier B.V.* 2003; 1:175–192.
[22] Y Hu, DB Johnson, A Perrig. *Efficient Security Mechanisms for Routing Protocols*. Proc. NDSS'03. 2003: 1–17.
[23] K Sanzgiri, B Dahill, B Levine, C Shields, E Royer. *A Secure Routing Protocol for Ad Hoc Networks*. 10th IEEE Int. Conf. Netw. Protoc. 2002: 1–10.
[24] Y Hu, DB Johnson, A Perrig. *Rushing Attacks and Defense in Wireless Ad Hoc Network Routing Protocols.* ACM Wirel. Secur. conjunction with MobiCom, Sept. 2003: 30–40.
[25] Y Hu, DB Johnson, A Perrig. Ariadne: A Secure On-Demand Routing Protocol for Ad Hoc Networks. *Wirel. Networks Springer*. 2005; 11: 21–38.
[26] S Zhu, S Xu, S Setia, S Jajodia. *Establishing Pair-wise Keys For Secure Communication in Ad Hoc Networks: A Probabilistic Approach.* Proceedings. 11th IEEE Int. Conf. Netw. Protoc. Nov.2003: 326 – 335.
[27] J Arkko, J Kempf, B Zill, P Nikander. Secure Neighbor Discovery (SEND). *RFC 3971*. March 2005.
[28] R Gagliano, S Krishnan, A Kukec. Certificate Profile and Certificate Management for Secure Neighbor Discovery (SEND). *RFC 6494*. Feb. 2012.
[29] S Blake-Wilson, N Bolyard, V Gupta, C Hawk, B Moeller. Elliptic Curve Cryptography (ECC) Cipher Suites for Transport Layer Security (TLS). *RFC 4492*, May 2006.
[30] V Fuller, T Li. Classless Inter-domain Routing (CIDR): The Internet Address Assignment and Aggregation Plan. *RFC 4632*, 2006.
[31] Configuring RIP. *Cisco Nexus 7000 Ser. NX-OS Syst. Manag. Configure Guid. Release 5.x*, Dec. 2011.
[32] Release 12.2(54)SG. Catalyst 4500 Series Switch Cisco IOS Software Configuration Guide.
[33] T Kang, X Li, C Yu, J Kim. A Survey of Security Mechanisms with Direct Sequence Spread Spectrum Signals. *J. Comput. Sci. Eng.* 7(3), Sept. 2013 : 187–197.
[34] A Samiah, A Aziz, N Ikram. *An Efficient Software Implementation of AES-CCM for IEEE 802.11i Wireless St.* 31st Annu. Int. Comput. Softw. Appl. Conf. July 2007 : 689 – 694.
[35] I Saberi, B Shojaie, M Salleh, M Niknafskermani, SM Alavi. *Improving confidentiality of AES-CCMP in IEEE 802.11i*. Int. Jt. Conf. Comput. Sci. Softw. Eng. 2012: 82 – 86.
[36] S Kent. IP Encapsulating Security Payload (ESP). *RFC 4303*, Dec. 2005.
[37] Y Zhang, B Singh. *A multi-layer IPsec protocol*. SSYM'00 Proc. 9th Conf. USENIX Secur. Symp. Aug. 2000; 9: 1–16.
[38] V Manral. Cryptographic Algorithm Implementation Requirements for Encapsulating Security Payload (ESP) and Authentication Header (AH). *RFC 4305*, April 2007.
[39] D Piper. The Internet IP Security Domain of Interpretation for ISAKMP. *RFC 2407*, Nov. 1998.
[40] Wireless Transport Layer Security, Wireless Application Protocol, WAP-261-WTLS-20010406-a. *(WTLS) WAP Forum*, Apr. 2001.
[41] A Levi, E Savas. *Performance Evaluation of Public-Key Cryptosystem Operations in WTLS Protocol*. Eighth IEEE Int. Symp. Comput. Commun. 2003. (ISCC 2003). Proceedings. July 2003; 2: 1245 – 1250.
[42] S Jormalainen, J Laine. Security in the WTLS. 1999: 1–18. <http://www.tml.tkk.fi/Opinnot/Tik110.501/1999/papers/wtls/wtls.html>
[43] J Jun, ML Sichitiu. MRP: Wireless mesh networks routing protocol. *Comput. Commun. Elsevier B.V.* May 2008; 31(7): 1413–1435.
[44] S Tripathi, AK Jain. Comparative Performance Analysis of Inter-Domain Routing Protocols in Integrated HSDPA and WLAN Ad Hoc Networks with Streaming Traffic. *J. Commun. Eng. Syst.2015;* 5(3): 7–18.

Biographies of Authors

Shashank Tripathi was born in Allahabad, Uttar Pradesh, India on July 30th, 1985. He received B.Tech Degree in Electrical & Electronics Engineering from Skyline Institute of Engineering & Technology, Greater Noida, Uttar Pradesh, India in 2007 and M.Tech Degree in Control & Instrumentation Engineering from Dr. B. R. Ambedkar National Institute of Technology, Jalandhar, Punjab, India in 2010. He was Assistant Professor at Department of Instrumentation and Control Engineering, Dr. B. R. Ambedkar National Institute of Technology, Jalandhar, Punjab, India from August 2010 - July 2012. He is Research Scholar at Department of Instrumentation and Control Engineering, Dr. B. R. Ambedkar National Institute of Technology, Jalandhar, Punjab, India. He has published over thirteen research papers in national and international journals. His research area of interest is modelling and simulation of next generation wireless networks.

A.K.Jain received his B.E and M.E both from IIT, Roorkee, (erstwhile University of Roorkee, Roorkee) India in 1981 and 1987 respectively and received his Ph.D. degree on Quality of Service in High Speed Networks from the Dr. B. R. Ambedkar National Institute of Technology, Jalandhar, India in 2009.He has published over sixty research papers in national and international journals/conferences. He is presently working as Professor in the Department of Instrumentation and Control Engineering, Dr. B. R. Ambedkar National Institute of Technology, Jalandhar, India. He is guiding PhD and M.Tech students in the area of Wireless Networks. Before joining N.I.T, Jalandhar, he has served at TIET Patiala, IET Lucknow, and NIT Hamirpur (Erstwhile REC Hamirpur) in various capacities. His research interests include quality of service in wireless networks, medium access protocols for mobile computing, and mesh networks. Dr. Jain is member of IEEE and ISTE India.