International Journal of Computing and Digital Systems
ISSN (2210-142X)
Int. J. Com. Dig. Sys. 6, No.1 (Jan-2017)

http://dx.doi.org/10.12785/ijcds/060102

Layer-wise Security Schemes with Secure Routing Protocol for Integrated UMTS and WLAN Ad Hoc Networks

Shashank Tripathi[1] and A K Jain[2]

[1,2] *Department of Instrumentation and Control Engineering, Dr B R Ambedkar National Institute of Technology Jalandhar, Jalandhar, India -144011*

Received 6 Jul. 2016, Revised 12 Nov. 2016, Accepted 5 Dec. 2016, Published 1 Jan. 2017

Abstract: It is well known that the Integrated Universal Mobile Telecommunications System (UMTS) and Wireless Local Area Network (WLAN) ad hoc network is not secure, due to the vulnerable routing infrastructure of ad hoc nodes to a variety of active attacks. In this paper, we introduce a secure, robust newly developed routing protocol, namely SNAuth_SPERIPv2, based on a Bellman Ford algorithm. It can be widely used in heterogeneous Next-Generation Networks (NGNs) on the inter-domain routing for un-trustworthy environment. A security framework is proposed for determining how the combination of the secure routing protocol and different layer security schemes (DSSS, CCMP-AES, IPSec and WTLS) should be working together against Wormhole Attack (WHA). WHA analysis and simulation results show the security scheme strength in terms of QoS metrics under CBR background traffic.

Keywords: Integrated UMTS and WLAN Ad Hoc network, QoS, Routing, Scalibility, Security, WHA

1. INTRODUCTION

The promise of Integrated UMTS and WLAN [1] multi-hop next generation network to solve challenging real-world problems sustains to attract various projects related to academic and industrial research. The routing and communication problems in multi-hop networks have been discussed by assuming a trusted environment in most of previous research work [2]. However, allots of applications that run in un-trusted environments wants secure communication and routing to protect network from unhealthy situations [3]. In online transactions, critical business operations, military networks, etc. are the application that may require secure communication.

The purpose of integration of UMTS network with the WLAN Ad Hoc network is used for real-time safety feedback to continue network services in emergency situations such as after a natural disaster like a tsunami, flood, or earthquake; infrastructures based UMTS network may be damaged. In this situation, integrated WLAN multi-hop ad hoc network might be used to provide network communication for emergency rescue teams because such license free network can be deployed rapidly. The rapid deployment cost of ad hoc nodes and wireless network hardware are very low (inexpensive) due to self-maintaining and configuring of network.

The Integrated UMTS and WLAN multi-hop networks support different class of services, namely: conversational, streaming, interactive, and background class service [4, 5, and 6]. First two classes are guaranteed QoS classes (highly delay sensitive) and next two are non-guaranteed best-effort QoS classes (loss sensitive) [7]. This paper selects only CBR background best-effort class that is used for delivery of e-mail, SMS, downloading files, etc. In this paper, inter-domain traffic model is based on non-real asymmetric file downloading background service under network scalability. Here, scalability is ability of particular network to extend their network size (by increasing both numbers of active user nodes for load scalability and network infrastructure for infrastructure scalability) without compromising its QoS.

Our contributions in this paper are presentation of the WHA (including eavesdrop), the development and analysis of new secure robust neighbor authenticated distance vector routing protocol that provide solid authentication against WHA, and design integration of this secure routing protocol with different security schemes for further improvement of confidentiality, integrity and availability of packets in Integrated UMTS and WLAN networks services against WHA.

E-mail: shashankt.ic.12@nitj.ac.in, jainak@nitj.ac.in

The rest of this paper is organized as follows: Section II discusses background: integrated UMTS and WLAN ad hoc network vulnerabilities and attacks, section III introduce related work, section IV discuses secure routing requirements and design of secure routing protocol for the integrated network and section V introduces performance evaluation. Finally, Section VI concludes this paper.

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

The integrated UMTS and WLAN Ad Hoc network, ad hoc nodes 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 [8]. The integrated network has unstable infrastructure vulnerability due to absence of wired network deployment in ad hoc network [9, 10]. A lot of network applications may run in this untested environment and therefore this network may require the use of a secure routing protocol most. In RIPv2, there is several known security vulnerabilities exist because its routing update message contains a vector of pairs (destination distance) [11, 12]. Some of attacks are discussed below.

A. 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 [13]. Keyed mechanism is better, but also vulnerable due to compromised router which may disclose keying materials of all routers [11, 12].

B. Prefix Impersonation

In prefix impersonation, an unauthorized or malicious node may claim a zero distance to those routers which are not directly connected to network subnet (prefix). The MD5 authentication scheme [13] is not enough for this attack. Prefix impersonation can easily launch Denial of Service (DoS) in inter-domain (e.g., BGPv4 [14]) as well as intra-domain routing protocol (e.g., RIPv2) [11, 12]. In the ARPANET [15], a similar incident has occurred known as a black hole attack.

C. 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 in the network. The RIPv2 with MD5 authentication scheme is not enough for this attack [11, 12].

D. Wormhole Attack (WHA)

This paper introduced a powerful active attack that may have severe consequences on distance vector routing protocols by showing shortest path for routing packets [16]. In this paper, the active WHA has been considered with passive eavesdropping threat [10, 17]. 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. An attacker intercepts packets at one location in the network and tunnels them to another location, and then replay (potentially altered) all tunneled packets into the network [10, 17, and 18]. 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 [19].

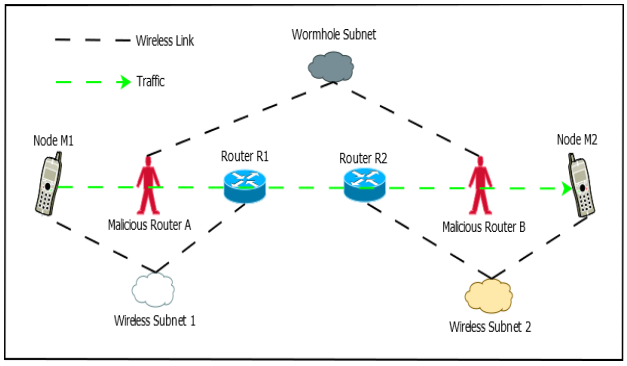

Figure 1. WHA adversary under transparent mode

In this paper, the WHAs have performed under transparent mode as an external adversary which can be shown in Figure1. In this Figure, ad hoc nodes M1 send packets to M2 under the presence of wormhole tunnel developed by external malicious nodes A and B. Suppose these two malicious nodes "A" and "B" has formed high bandwidth, low latency wormhole tunnel within the victim network and this low latency and high bandwidth tunnel intercept routing packets/frames by showing the shortest path for them. If node A and B intercept 70 and 30 frames from victim network nodes and tunneled 65 out of 70 frames and 25 out of 30 frames on wormhole tunnel and replayed 40 frames out of 65 frames from "A" to "B" and 20 frames out of 25 frames from "B" to "A". Then the total number of frames dropped and total number of frames replayed by the wormhole tunnel will be 30 and

60, respectively. In this replay attack IP header of some packets can be potentially altered due to high speed frame collisions. Finally, this attack disrupts the routing protocol and performs a denial-of-service (DoS) in victim network.

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 [20]) and inter-domain path vector routing protocol (e.g. BGPv4 [21]) using public-key digital signatures or Message Authentication Code (MAC) cryptographic approaches [11, 12, 22 and 23]. The works of several researchers have been reviewed below.

Hu et al. [10] 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. According to this paper, 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. The results discussed in this paper are also applicable to cellular networks.

Hu et al. [24] 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. [25] 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. [26] proposed a secure routing protocol for ad hoc network known as Authenticated Routing for Ad hoc Networks (ARAN) and successfully work against active tunneling 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. [27] 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. [28] 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. [12] 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. [11] 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

The integrated network is using RIPv2 distance vector routing protocol as a base intra-domain routing protocol. By configuring Gateway GPRS Support Node (GGSN) as an IP gateway for ad hoc nodes, this dynamic routing protocol will help to support for inter-domain routing from UMTS to WLAN. Whereby configuring static or default routes, this dynamic protocol is supported in inter-domain routing from WLAN to UMTS network. In integrated UMTS and WLAN network, the multi-hop WLAN ad hoc network is a wormhole prone region. This can make overall integrated network insecure. The protection of vulnerable domain is preserved by a securing routing protocol. To avoid the impact of WHAs on the QoS of integrated network, this paper introduced a Secure Neighborhood Authenticated Strict priority Equal-cost multipath RIPv2 (SNAuth_SPERIPv2) distance vector routing protocol and integrate the secure distance vector routing protocol with different security schemes.

A. The 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 routes.

1) The secure neighbor authentication (SNAuth) schemes: SNAuth schemes work with symmetric as well as asymmetric cryptography. The SNAuth [27] is applicable for both wired as well wireless IP routing scenarios. In the SNAuth with symmetric cryptography, the authentication variant is based on 16 byte pair-wise shared secrets key [29] variant between sender and receiver nodes which is hidden from remaining users. Where, in the SNAuth with asymmetric cryptography, the authentication variant is based on certification.

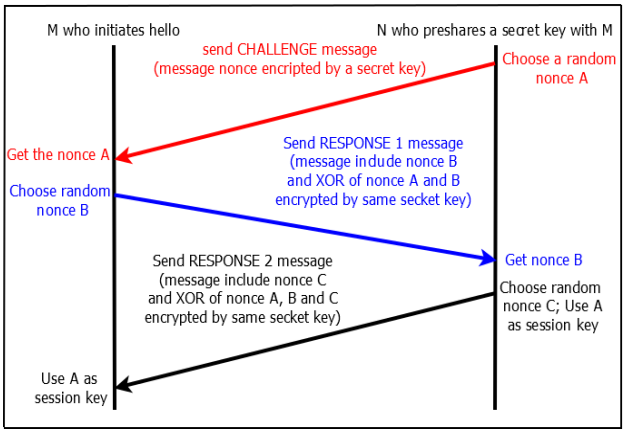

Figure 2. The pair-wise shared secret variant of SNAuth

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 [30]. 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 exclusively be practiced once with particular authentication message. The Figure2 illustrates three way handshakes based on pair-wise shared secret variant.

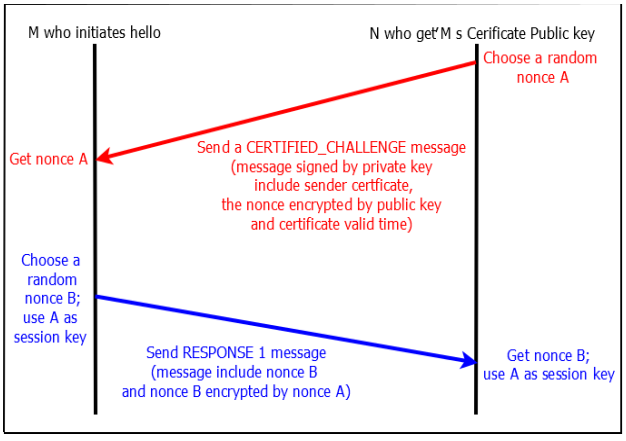

Figure 3. The SNAuth variant based on certification

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 [31]. The challenge certificate messages uses, its own certificate and a usual public key encrypted cipher-text signed by its own secret key. The public key cryptosystem uses an Elliptic Curve Cryptosystem (ECC) which has shorter certificate length and cipher-text length and offers less communication overhead [32]. The response messages use a secret session key to encrypt and decrypt their nonce. The Figure3 illustrates two way handshaks based on certificate variant.

2) Strict Priority Equal-cost multipath RIPv2 (SPERIPv2): In this paper, Routing Information Protocol version2 (RIPv2) has taken for intra-domain distance vector routing. RIPv2 is classless dynamic routing protocol works on bellman ford algorithms. It is used by medium and small organizations (IP networks of moderate size) because it's limited hop-count, which is 15 hops per packet and 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 4.

In Figure 4(a), command is 8bit 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 Figure4 (b). The unsigned 8 bit authentication data length present in this 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) [33]. 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.

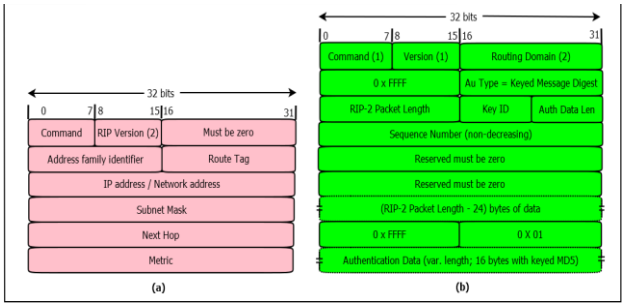

Figure 4. RIP v2 message format (a) with a plain text password (b) keyed MD5

In the present scenario most of internet application wants 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 use 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 [34]. The meaning of equal cost multipath is that more than one equal cost path between the source and 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 [20]. This thing helps to increase robustness of the routing protocol and provide load balancing by distributing traffic among all routers. The Figure5 illustrates the equal cost path in RIPv2 between source and destination based on a Bellman Ford algorithm.

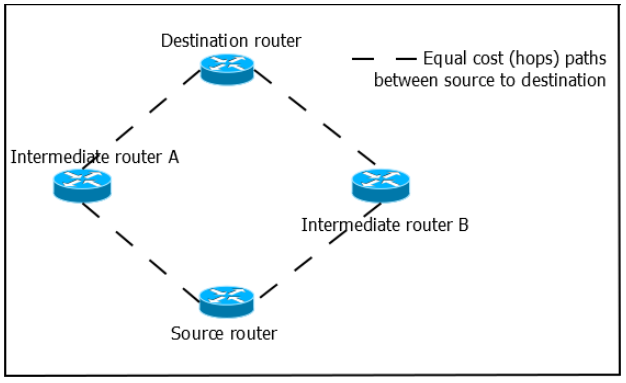

Figure 5. Equal cost path in RIPv2

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. In this paper, the time interval for which a node waits to do the next neighbor detection handshake (secure-neighborhood expiration timeout) has been specified as 5000 ms.

B. 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-section.

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 a pairwise 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. In this paper, a multi-layer wormhole adversary model with the network security models has been used. WHAs on routing protocol that produces dose directly on the network layer and indirectly on other layers of network that affect 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 [35]. In this paper, the transmission and reception turnaround latency for UMTS and WLAN radios have been specified as 25µs and 2µs, respectively. In Figure6, DSSS system model has been illustrated.

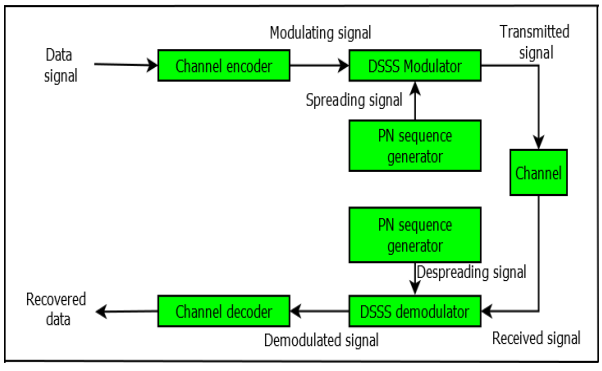

Figure 6. DSSS system model

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 [36, 37]. 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. The encryption and description schemes of MPDU are shown in Figure 7(a) and 7(b), respectivelly.

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 [38]. The proposed IPSec scheme uses a hybrid version of IPSec protocol that includes both Encapsulating Security Payload (ESP) and Authentication Header (AH) protocols [39, 40, and 41] as shown in Figure8.

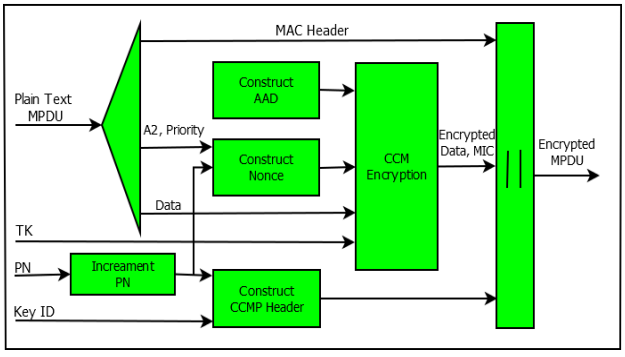

Figure 7. (a) The encryption scheme of MPDU

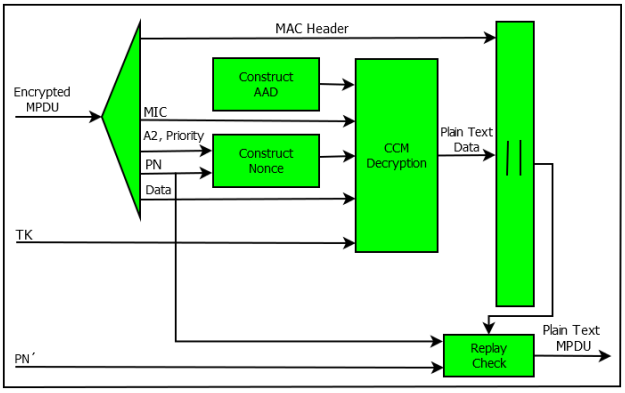

Figure 7. (b) The decryption scheme of MPDU

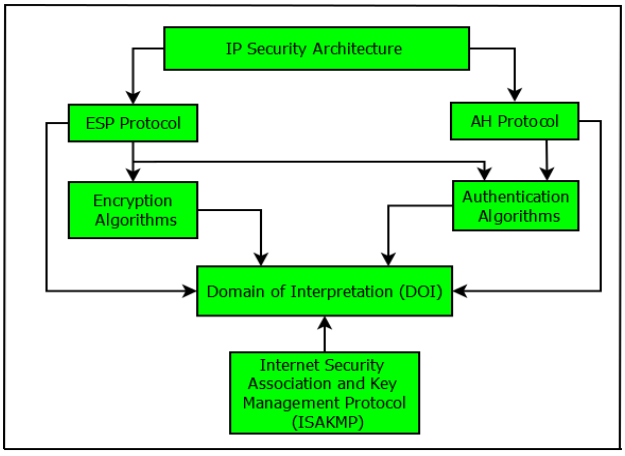

Figure 8. The IPSec protocol architecture

ESP provides confidentiality with integrity and optional 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. A 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 [42]. 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.

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 provides routing protocol message authentication, where, WTLS provide data privacy, authentication and integrity for Wireless Application Protocol (WAP) applications against man in the middle DoS attacks [26, 43, 44, 45].

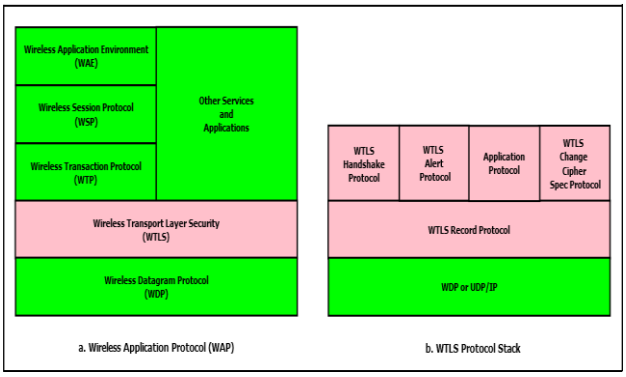

Figure 9. Wireless Application Protocol (WAP) architecture

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 [46]. As shown in Figure9, WTLS consists of record protocol that is used for basic security services for higher layer and further extended into four protocol clients the handshake protocol, the change cipher spec protocol, the alert protocol and the application data protocol [47]. In this scheme, WTLS certificate has been implemented on each IP interface with IPSec ESP in transport mode for transport and upper layer security. In this paper, WTLS uses modern cryptographic algorithms are MD5, SHA1, AES, 3DES, and Elliptic Curve Cryptography (ECC) [48].

5. PERFORMANCE EVALUATION

This section presents the simulation results which have conducted using QualNet to evaluate the performance of security schemes under WHA. QualNet simulator is a parallel discrete-event simulator that is the commercial version GloMoSim. QualNet provides the exact model in each layer including the physical and MAC layers of networks. The results of the simulation of wireless networks show that the accuracy of the models.

A. Configuration of the network, including wormhole adversary

The Integrated UMTS and WLAN Ad Hoc network parameters of the models have been configured according to WLAN wireless model library and UMTS model library of QualNet, respectively. Configuration of the integrated network parameters is given in Table I.

TABLE I. CONFIGURATION OF THE NETWORK PARAMETERS

Parameter	UMTS	WLAN
No. of channels (channel frequencies)	02 (1.95 GHz UL, 2.15 GHz DL)	01 (2.4 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	

The Integrated UMTS and WLAN Ad Hoc network provide ubiquitous mobility to User Equipments (UEs) under inter Node Bs handoff and connect these users with fixed Ad Hoc network users, which are extending the coverage area of the integrated network to those areas where UMTS PLMN infrastructure not available.

The integrated network can be divided into three parts for recognizing the IP routing domains. In this paper, packets routing in WLAN Ad Hoc network fully depend on policy based dynamic routing protocols. The ad hoc network domain connected to the GGSN of Core Network (CN) by Wireless Access Gateways (WAGs) using GPRS Tunneling Protocol (GTP) which is a group of IP-based communications protocols used to carry General Packet Radio Service (GPRS) within UMTS CN. In CN, packet routing depends on GTP influenced by dynamic routing protocols over an IP based backbone. Serving GPRS Support Node (SGSN) including Visitor Location Register (VLR), Home Location Register (HLR) is the part of the CN and connected to each other by GTP tunnel.

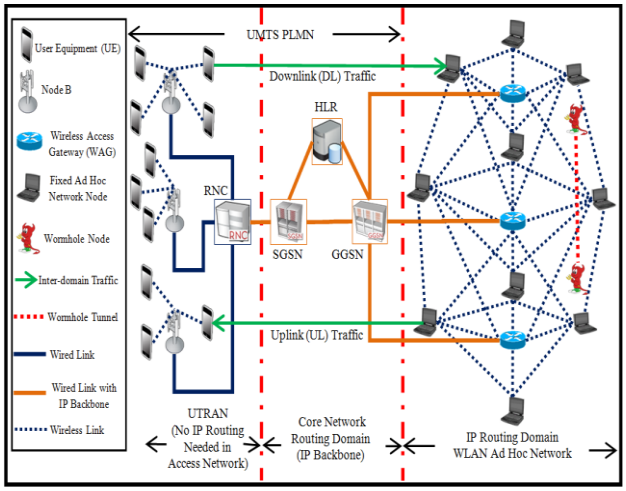

Figure 10. Integrated UMTS and WLAN Ad Hoc network with wormhole adversary

As shown in Figure10, Universal Terrestrial Radio Access Network (UTRAN) is a part of the integrated network uses WCDMA radios, where IP routing is not needed. The UTRAN, sometimes it may also be known as the Radio Network Subsystem (RNS) is included Node Bs (base stations) and Radio Network Controller (RNC). The RNC, which provides Radio Access Bearer (RAB) for packet data services through Service Access Points (SAPs) allows connectivity between the User Equipment (UE) via Node B and the SGSN of CN.

This paper implements a wormhole adversary in the vulnerable area of integrated network which can disrupt routing protocols by higher bandwidth and low latency wireless link tunnel as shown in Figure10. The wormhole is working in transparent mode as external adversary and performs a DoS attack.

B. Performance Metrics

QoS performances of integrated networks under wormhole adversary and different security schemes have been analyzed by seven 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 [49].

This paper employs CBR background traffic in the QoS performance evaluation of integrated network under WHA. This traffic use network end-to-end delay as a performance metric. The performance metric are defined as follows:

Number of Frames Dropped by Wormhole (WH)=Number of Frames Tunnelled - Number of Frames Replayed (1)

$$Routing\ Overhead = \frac{\sum_{n=1}^{N}\sum_{p=1}^{P_n^{cs}} b_{n,p}}{T_{sim} \times N} \quad \left(\frac{\text{bps}}{\text{node}}\right) \tag{2}$$

$$Average\ Packet\ Loss = \left(1 - \frac{\sum_{n=1}^{N} P_n^{dr}}{\sum_{n=1}^{N} P_n^{ds}}\right)\% \tag{3}$$

$$Throughput = \frac{\sum_{n=1}^{N}\sum_{p=1}^{P_n^{dr}} b_{n,p}}{T_{sim} - t_F} \quad \text{bps} \tag{4}$$

$$Average\ End-to-End\ Delay = \frac{\sum_{n=1}^{N}\sum_{p=1}^{P_n^{dr}} D_{n,p}}{\sum_{n=1}^{N} P_n^{dr}} \quad \text{ms} \tag{5}$$

$$Average\ Jitter = \frac{\sum_{n=1}^{N}\sum_{p=1}^{P_n^{dr}} (D_{n,p} - D_{n,p-1})}{\sum_{n=1}^{N} P_n^{dr} - 1} \quad \text{ms} \tag{6}$$

$$Average\ Hop-Count = \frac{\sum_{n=1}^{N}\sum_{p=1}^{P_n^{dr}} h_{n,p}}{\sum_{n=1}^{N} P_n^{dr}} \quad \left(\frac{\text{hops}}{\text{packet}}\right) \tag{7}$$

Where, N is the total number of network nodes,

T_{sim} is the total simulation time when statistics are collected,

P_n^{cs} is the total number of routing control packet sent by the n^{th}node,

$b_{n,p}$ is the total number of bit in the p^{th} packet received by the n^{th}node,

P_n^{dr} is the total number of packet sent by the n^{th}node,

P_n^{ds} is the total number of packet received by the n^{th}node,

t_F is the time first packet received by the n^{th}node,

$D_{n,p}$ is the packet transmission delay experienced by the current p^{th}packet received by the n^{th}node,

$D_{n,p-1}$ is the packet transmission delay experienced by the previous $(p-1)^{th}$ packet received by the n^{th} node,

$h_{n,p}$ is the number of hops roamed by the p^{th}packet of the n^{th} node.

C. 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 route stability. Simulations are run for one way background application with Constant Bit-Rate (CBR) traffic. Background traffic is non-real time non-guaranteed best effort service supported by the Radio Access Bearer (RAB) service of UMTS network and this traffic model is used to evaluate the performance of the routing protocol in a more realistic scenario. The simulations are performed 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 II.

TABLE II. SIMULATION SETUP

Parameter	Scenario-I	Scenario-II
Packet size	1024 Byte	1024 Byte
Traffic load	12.5 packets/s	12.5 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 km^2	6x6 km^2

The simulation scenario-I is performed to evaluate the influence of scalability with wormhole adversary by increasing network size using increasing number of fixed nodes from 8 to 40. The distribution of fixed nodes is uniform in 3x3 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 of 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-II is performed to evaluate the influence of large scalability with wormhole adversary 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 80 ms are considered as 100% inter-domain traffic ratio. The CBR background 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 [50], 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 background 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 all scenario statistics are collected after 1s.

In all experiments, 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 tunneled 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.

This paper is presented a robust, secure neighbor authenticated strict priority equal cost multipath routing information protocol version 2 (SNAuth_SPERIPv2) 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.

The comparative analysis of different security schemes under WHA based on mentioned QoS metrics for all scenarios are given in the following sections.

D. Simulation results and analysis for scenario - I

This scenario shows different security schemes with and without WHA under the extension of network diameter by increasing number of fixed network nodes from 8 to 40 while keeping network density constant. This simulation scenario is totally dedicated for low network size scalability issue under stable network nodes.

1) The performance of integrated network on a number of frames dropped by Wormhole Tunnel(WH) under different security scheme while the number of fixed network nodes are increased

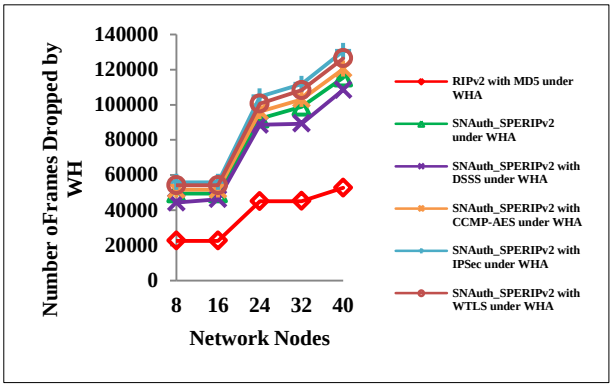

Figure 11(a). Number of frames dropped by WH versus number of network nodes

Figure 11 (a) shows the number of frames dropped by WH tunnel with and without different security scheme. Frame dropped by WH is increasing with network size. The security schemes which have maximum number of frames dropped produce minimum dose 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.

2) The performance of integrated network on routing overhead under different security scheme with and without WHA while the number of fixed network nodes are increased

Figure 11(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.

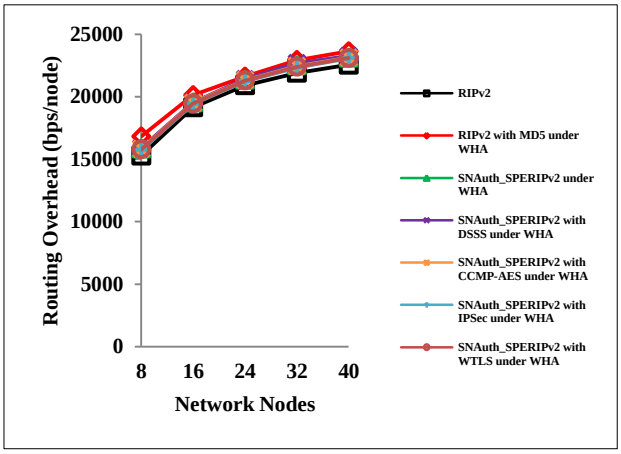

Figure 11(b). Average routing overhead versus number of network nodes

3) The performance of integrated network, on average packet loss under different security scheme with and without WHA while the number of fixed network nodes are increased

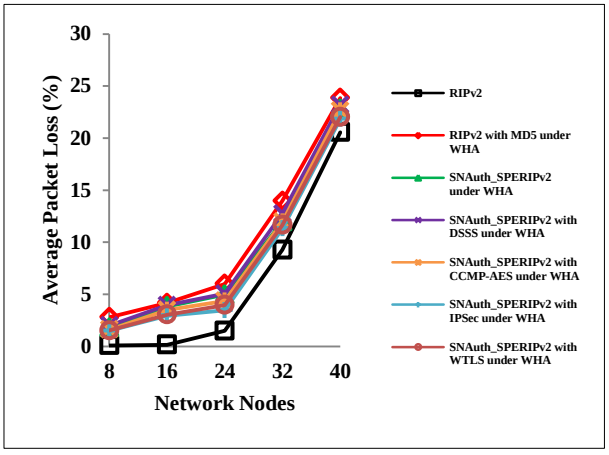

Figure 11(c). Average packet loss versus number of network nodes

Figure11(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.

4) The performance of integrated network, on average throughput under different security scheme with and without WHA while the number of fixed network nodes are increased

Figure11 (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 shows 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.

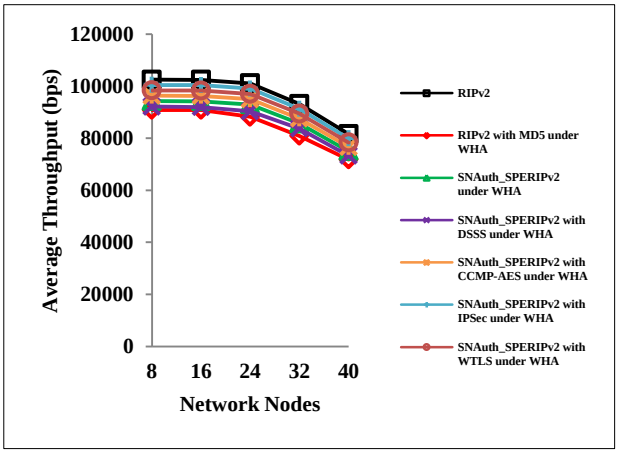

Figure 11(d). Average throughput versus number of network nodes

5) The performance of integrated network,on average end-to-end delay under different security scheme with and without WHA while the number of fixed network nodes are increased

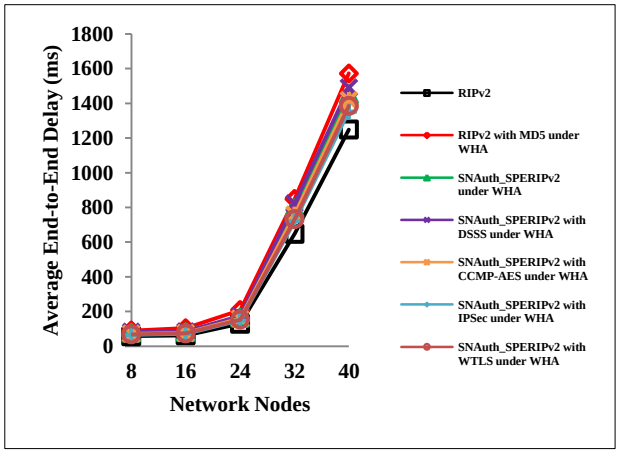

Figure 11(e). Average end-to-end delay versus number of network nodes

Figure11(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. It shows 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.

6) The performance of integrated network,on average jitter under different security scheme with and without WHA while the number of fixed network nodes are increased

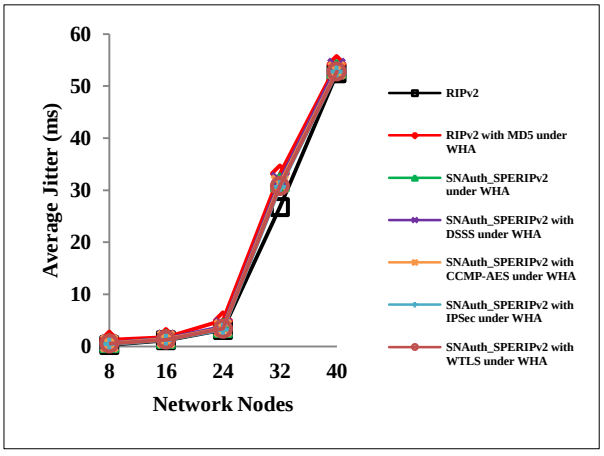

Figure 11(f). Average jitter versus number of network nodes

Figure11 (f) shows the average jitter is decreasing with the network size for the background service. The average jitter of different security schemes with WHA increases as average packet loss is increased. It shows RIPv2 with MD5 is having maximum average jitter where SNAuth_SPERIPv2 routing protocol with DSSS is having minimum average jitter among them.

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

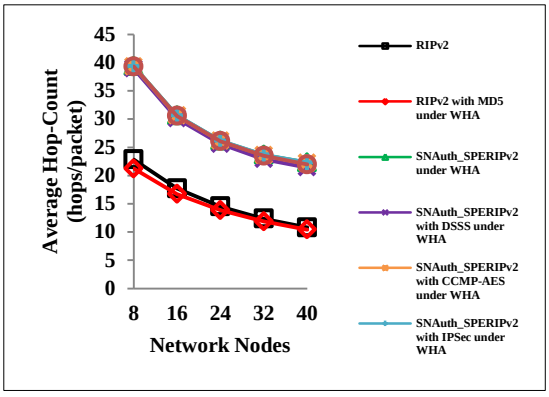

Figure 11(g). Average hop-count versus number of network nodes

Figure11(g) shows the average hop counts is decreasing with the network size at different security schemes with and without WHA because UEs offers zero hop-count. 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 [51]. The route selection algorithm favours 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 [52]. To protect the network from WHA, it is necessary to make routing protocols robust.

E. Simulation results and analysis for scenario - II

This scenario shows different security schemes with and without WHA under the extension of network diameter by increasing number of fixed network nodes from 40 to 200 while keeping network density constant. This simulation scenario is totally dedicated to high network size scalability issue under stable network nodes.

1) The performance of integrated network on a number of frames dropped by WH under different security scheme while the number of fixed network nodes are increased

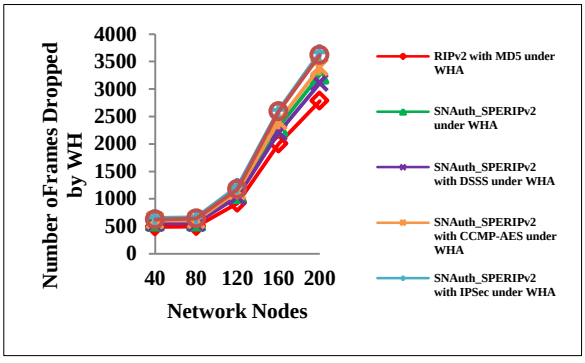

Figure 12(a). Number of frames dropped by WH versus number of network nodes

Figure12 (a) shows the number of frames dropped by WH tunnel with and without different security scheme. Frame dropped by WH is increasing with network size. The security schemes which have maximum number of frames dropped produce minimum DoS in 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.

2) The performance of integrated network on routing overhead under different security scheme with and without WHA while the number of fixed network nodes are increased

Figure12 (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.

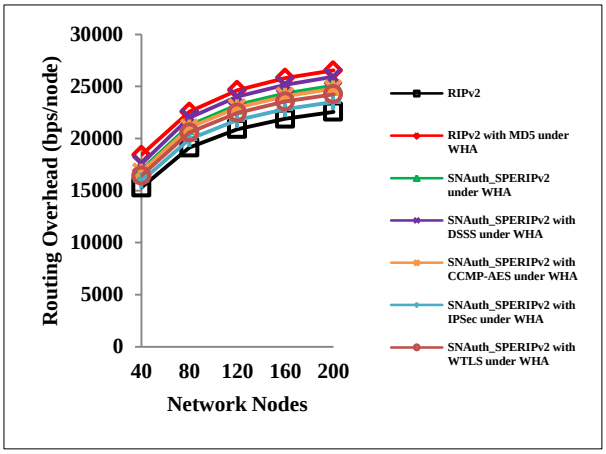

Figure 12(b). Average routing overhead versus number of network nodes

3) The performance of integrated network, on average packet loss under different security scheme with and without WHA while the number of fixed network nodes are increased

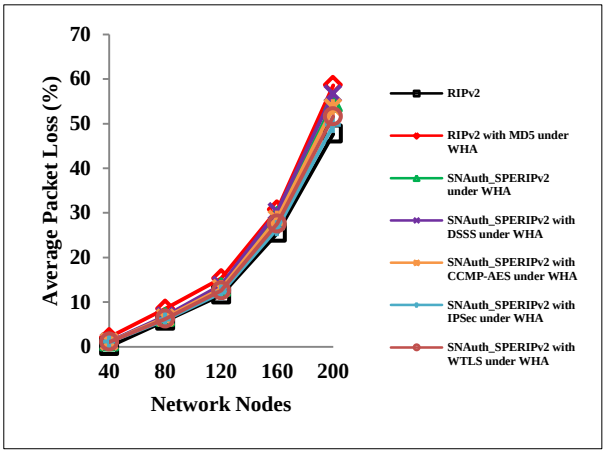

Figure 12(c). Average packet loss versus number of network nodes

Figure12(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.

4) The performance of integrated network, on average throughput under different security scheme with and without WHA while the number of fixed network nodes are increased

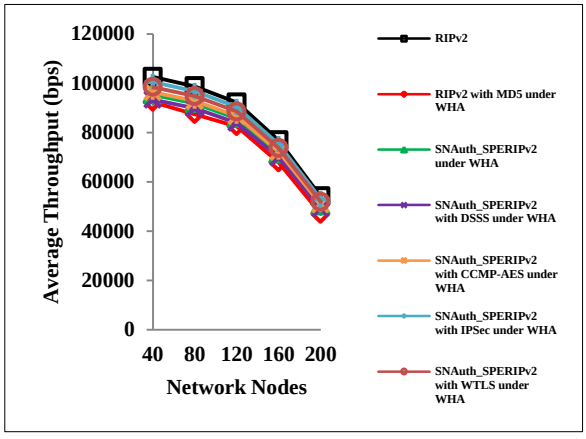

Figure 12(d). Average throughput versus number of network nodes

Figure12 (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 shows 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) The performance of integrated network, on average end-to-end delay under different security scheme with and without WHA while the number of fixed network nodes are increased

Figure12 (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. It shows 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.

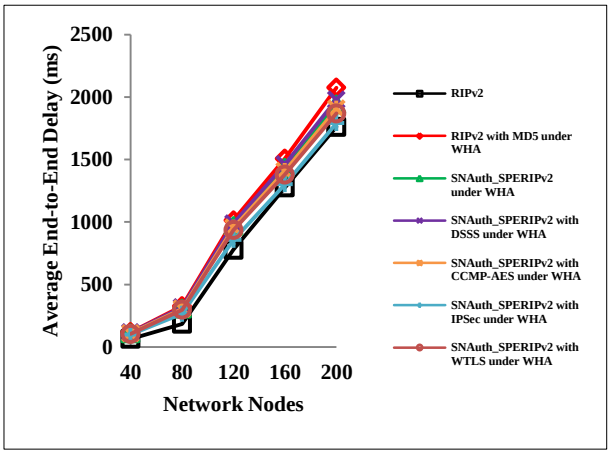

Figure 12(e). Average end-to-end delay versus number of network nodes

6) The performance of integrated network, on average jitter under different security scheme with and without WHA while the number of fixed network nodes are increased

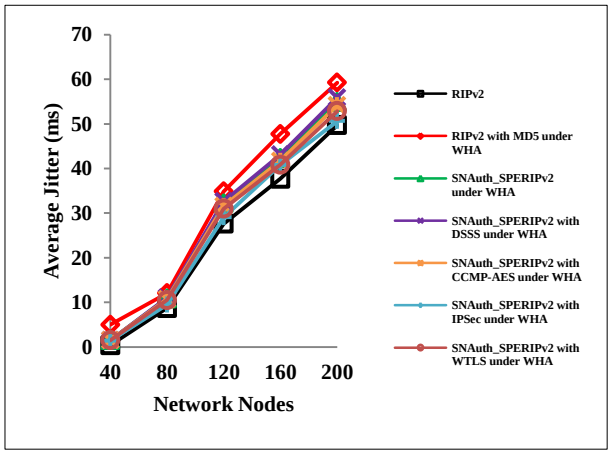

Figure 12(f). Average jitter versus number of network nodes

Figure12 (f) shows the average jitter is decreasing with the network size for the background service. The average jitter of different security schemes with WHA increases as average packet loss is increased. It shows RIPv2 with MD5 is having maximum average jitter where SNAuth_SPERIPv2 routing protocol with DSSS is having minimum average jitter among them.

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

Figure12(g) shows the average hop counts is decreasing with the network size at different security schemes with and without WHA because UEs offers zero hop-count. 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 favours 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.

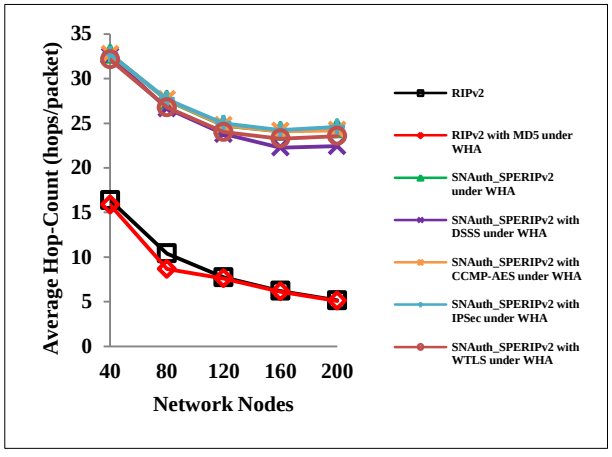

Figure 12(g). Average hop-count versus number of network nodes

6. CONCLUSION

The integrated UMTS and WLAN Ad Hoc networks are becoming increasingly popular as they have significant advantages within next generation networks. In this paper, we introduce a new secure, robust routing protocol SNAuth_SPERIPv2, specifically designed for next generation technologies. The design of the proposed secure routing protocol takes advantage to the integrated network, maintaining QoS under WHA. Simulation results show that, SNAuth_SPERIPv2 routing protocol with IPSec outperforms existing security schemes for the integrated UMTS and WLAN Ad Hoc networks under WHA, for high packet loss sensitive background traffic under network node scalability. The secure protocol performs best when used in most common cellular and ad hoc network scenarios. The impact of WHA on ad hoc nodes of integrated network under SNAuth_SPERIPv2 routing protocol is mitigating. All simulation result collected, are within limits as specified by guidelines [2, 3 and 4].

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] M. Saadeh, A. Sleit, M. Qatawneh, and W. Almobaideen, "Authentication Techniques for the Internet of Things: A Survey," IEEE Cybersecurity Cyberforensics Conf., pp. 28–34, 2016.

[3] V. S. Bhargavi and S. S.Viswanadha Raju, "Enhancing Security in MANETS through Trust-Aware Routing," IEEE Conf. WiSPNET, pp. 1940–1943, 2016.

[4] 3G TS22.105v3.9.0 Release 1999; "Univarsal Mobile Telecommunications System (UMTS), Service Aspects, Services and Service Capabilities," June 2000.

[5] L. Skorin-Kapov, D. Huljenic, E. N. Tesla, D. Mikic, and D. Vilendecic, "Analysis of End-to-End QoS Networked Virtual Reality Services in UMTS," Networked Virtual Environ. IEEE Commun. Mag., pp. 49–55, April 2004.

[6] N. Baghaei and R. Hunt, "Review of Quality of Service Performance in Wireless LANs and 3G Multimedia Application Services," Comput. Commun. Elsevier B. V., vol. 27, pp. 1684–1692, July 2004.

[7] F. C. de Gouveia and T. Magedanz, "Quality of Service in Telecommunication Networks," Telecommun. Syst. Technol. EOLSS, vol. 2, pp. 1–8.

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

[9] M. A. Mobarhan, M. A. Mobarhan, and A. Shahbahrami, "Evaluation of Security Attacks on UMTS Authentication Mechanism," Int. J. Netw. Secur. Its Appl., vol. 4, no. 4, pp. 37–52, 2012.

[10] Y. Hu, A. Perrig, and D. B. Johnson, "Wormhole Attacks in Wireless Networks," IEEE J. Sel. Areas Commun., vol. 24, no. 2, pp. 370–380, 2006.

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

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

[13] F. Baker and R. Atkinson, "RIP-II MD5 Authentication," RFC 2082, Jan.1997.

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

[15] J. M. McQuillan, G. Falk, and I. Richer, "A Review of the Development and Performance of the ARPANET Routing Algorithm," IEEE Trans. Comm., vol. 26, no. 12, pp. 1802–1811, Dec.1978.

[16] S. R. Deshmukh and P. N. Chatur, "Secure Routing to Avoid Black Hole Affected Routes in MANET," IEEE Symp. Colossal Data Anal. Netw., pp. 1–4, 2016.

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

[18] L. Qian, N. Song, and X. Li, "Detecting and Locating Wormhole Attacks in Wireless Ad Hoc Networks through Statistical Analysis of Multi-path," IEEE Commun. Soc. / WCNC, pp. 2106–2111, 2005.

[19] I. Hbabeh, I. Khalil, A. Khreishah, and S. Bataineh, "Performance Evaluation of Wormhole Security Approaches for Ad Hoc Networks," J. Comput. Sci., vol. 9, no. 12, pp. 1626–1637, 2013.

[20] G. Malkin, "RIP Version 2," RFC 2453, Nov.1998.

[21] Y. Rekhter, and T. Li, "A Border Gateway Protocol 4," RFC 1771, March.1995.

[22] S. Kent, C. Lynn, and K. Seo, "Secure Border Gateway Protocol (Secure-BGP)," IEEE J. Sel. Areas Commun., vol. 18, no. 4, pp. 582–592, April 2000.

[23] R. White, "Securing BGP Through Secure Origin BGP," Internet Protoc. J., vol. 6, no. 3, pp. 15–22, Sept. 2003.

[24] Y. Hu, D. B. Johnson, and A. Perrig, "SEAD: Secure Efficient Distance Vector Routing for Mobile Wireless Ad Hoc Networks," Ad Hoc Networks Elsevier B.V., vol. 1, pp. 175–192, 2003.

[25] Y. Hu, D. B. Johnson, and A. Perrig, "Efficient Security Mechanisms for Routing Protocols," Proc. NDSS'03, pp. 1–17, 2003.

[26] K. Sanzgiri, B. Dahill, B. Levine, C. Shields, and E. Royer"A Secure Routing Protocol for Ad Hoc Networks," 10th IEEE Int. Conf. Netw. Protoc., pp. 1–10, 2002.

[27] Y. Hu, D. B. Johnson, and A. Perrig, "Rushing Attacks and Defense in Wireless Ad Hoc Network Routing Protocols," ACM Wirel. Secur. conjunction with MobiCom, pp. 30–40, Sept. 2003.

[28] Y. Hu, D. B. Johnson, and A. Perrig, "Ariadne: A Secure On-Demand Routing Protocol for Ad Hoc Networks," Wirel. Networks Springer, vol. 11, pp. 21–38, 2005.

[29] S. Zhu, S. Xu, S. Setia, and S. Jajodia, "Establishing Pair-wise Keys For Secure Communication in Ad Hoc Networks: A Probabilistic Approach," Proceedings. 11th IEEE Int. Conf. Netw. Protoc., pp. 326 – 335, Nov. 2003.

[30] J. Arkko, J. Kempf, B. Zill, and P. Nikander, "SEcure Neighbor Discovery (SEND)," RFC 3971, March 2005.

[31] R. Gagliano, S. Krishnan, and A. Kukec, "Certificate Profile and Certificate Management for Secure Neighbor Discovery (SEND)," RFC 6494, Feb. 2012.

[32] S. Blake-Wilson, N. Bolyard, V. Gupta, C. Hawk, and B. Moeller, "Elliptic Curve Cryptography (ECC) Cipher Suites for Transport Layer Security (TLS)," RFC 4492, May 2006.

[33] V. Fuller and T. Li, "Classless Inter-domain Routing (CIDR): The Internet Address Assignment and Aggregation Plan," RFC 4632, 2006.

[34] "Configuring RIP," Cisco Nexus 7000 Ser. NX-OS Syst. Manag. Config. Guid. Release 5.x, Dec. 2011.

[35] T. Kang, X. Li, C. Yu, and J. Kim, "A Survey of Security Mechanisms with Direct Sequence Spread Spectrum Signals," J. Comput. Sci. Eng., vol. 7, no. 3, pp. 187–197, Sept. 2013.

[36] A. Samiah, A. Aziz, and N. Ikram, "An Efficient Software Implementation of AES-CCM for IEEE 802.11i Wireless St," 31st Annu. Int. Comput. Softw. Appl. Conf., pp. 689 – 694, July 2007.

[37] I. Saberi, B. Shojaie, M. Salleh, M. Niknafskermani, and S. M. Alavi, "Improving confidentiality of AES-CCMP in IEEE 802.11i," Int. Jt. Conf. Comput. Sci. Softw. Eng., pp. 82 – 86, 2012.

[38] I. Aouini, L. Ben Azzouz, and L. A. Saidane, "A Secure Neighborhood Area Network Using IPsec," IEEE Int. Wirel. Commun. Mob. Comput. Conf., pp. 102–107, 2016.

[39] S. Kent, "IP Encapsulating Security Payload (ESP)," RFC 4303, Dec. 2005.

[40] Y. Zhang and B. Singh, "A multi-layer IPsec protocol," SSYM'00 Proc. 9th Conf. USENIX Secur. Symp., vol. 9, pp. 1–16, Aug. 2000.

[41] V. Manral, "Cryptographic Algorithm Implementation Requirements for Encapsulating Security Payload (ESP) and Authentication Header (AH)," RFC 4305, April 2007.

[42] D. Piper, "The Internet IP Security Domain of Interpretation for ISAKMP," RFC 2407, Nov. 1998.

[43] "Wireless Transport Layer Security, Wireless Application Protocol, WAP-261-WTLS-20010406-a," (WTLS) WAP Forum, Apr. 2001.

[44] A. Levi and E. Savas, "Performance Evaluation of Public-Key Cryptosystem Operations in WTLS Protocol," Eighth IEEE Int. Symp. Comput. Commun. 2003. (ISCC 2003). Proceedings., vol. 2, pp. 1245 – 1250, July 2003.

[45] S. Jormalainen and J. Laine, "Security in the WTLS," pp. 1–18,1999. <http://www.tml.tkk.fi/Opinnot/Tik110.501/1999/papers/wtls/wtls.html>

[46] X. Li, J. Xu, Z. Zhang, D. Feng, and H. Hu, "Multiple Handshakes Security of TLS 1.3 Candidates," IEEE Symp. Secur. Priv., pp. 486–505, 2016.

[47] Y. Son, "Transport Layer Security Protocol in WAP version 2.0," Glob. Inf. Assur. Certif. Pap. Inst. 2000 - 2005, pp. 1–8, Aug. 2001.

[48] C. Khatwani and S. Roy, "Security Analysis of ECC Based Authentication Protocols," IEEE Int. Conf. Comput. Intell. Commun. Networks, pp. 1167–1172, 2015.

[49] J. Jun and M. L. Sichitiu, "MRP: Wireless mesh networks routing protocol," Comput. Commun. Elsevier B.V., vol. 31, no. 7, pp. 1413–1435, May 2008.

[50] S. Tripathi and A. K. Jain, "Background Service QoS in Integrated UMTS-HSDPA and WLAN Ad Hoc Networks with Various Inter-Domain Routing Protocols," J. Comput. Technol. Appl., vol. 6, no. 3, pp. 1–29, Jul. 2015.

[51] A. O. Alkhamisi, S. M. Buhari, and Jeddah, "Trusted Secure Adhoc On-Demand Multipath Distance Vector Routing in MANET," IEEE 30th Int. Conf. Adv. Inf. Netw. Appl., pp. 212–219, 2016.

[52] A. P. Rai, V. Srivastava, and Rinkoo Bhatia, "Wormhole Attack Detection in Mobile Ad Hoc Networks," Int. J. Eng. Innov. Technol., vol. 2, no. 2, pp. 174–179, Aug. 2012.

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 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. 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. 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 & ISTE India.