Analysis of Security threats and Vulnerability Issues in QoS Frameworks of MANET

Santosh Sahu[1], Sanjeev Sharma[2]
[1,2]*School of Information Technology, RGPV, Bhopal, India*
[1]santoshsahu@rgtu.net
[2]sanjeev@rgtu.net

Abstract: A QoS framework is a complete system that provides required QoS services to each node. All components within it cooperate together for providing the required services. As Quality of service (QoS) and security mechanism are in contradiction of each other. If we secure a QoS framework then it can't provide QoS Services. As QoS framework tend to be vulnerable to a number of threats and attacks like, over/under-reporting of available bandwidth, over-reservation, state table starvation, QoS degradation, information disclosure, theft of services timing attack, flooding attack, replay attack, and denial of service (DoS) attack, attacks on information in transit, black hole attack, wormhole attack and attacks against routing. In this paper we first describe a layer-wise classification of the existing QoS frameworks, and then analyses each of these Security breaches for threats and attacks. After analysis we determine that existing QoS Framework has critical issues of security. Must provide security mechanism for existing QoS framework. So it is required when designing protocols for QoS framework, the harmony between security and QoS must be present. Finally proposed a new QoS framework for ad hoc wireless network.

Key words: *QoS, Cross Layer Design, QoS Frameworks, QoS Signalling, QoS Routing, Resource Reservation, Admission Control, Scheduling.*

I. INTRODUCTION

Ad hoc Wireless Network (AWN) consists of a set of mobile nodes connected by wireless links which might be created on-the-fly while not victimization any infrastructure or body support [1]. These networks are characterized by self-organization and autonomy. Figure 1 shows the standard example of wireless mobile Ad Hoc Networks.

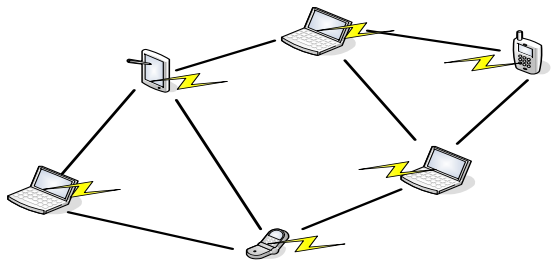

Fig.1 an example of Ad Hoc Wireless networks

These networks are often shaped on the fly, while not requiring any fastened infrastructure. As these infrastructure less networks, every node ought to act conjointly as a router. The distinctive characteristic of wireless ad hoc Networks like dynamic topology and resource constraint distinguishes it from wired networks and necessitates the necessity of special solutions in these networks [2].

Due to the characteristics of the MANETs, like fast topology amendment and restricted communication and computation capability, the standard security measures cannot be directly applied and new security techniques area unit necessary. While not protection of security mechanisms, a QoS framework is at risk of several threats and attacks that inhibit the guarantee of network resource availableness. While not protection of a security mechanism, attacks on QoS signalling system could finish in QoS routing malfunction, interference of resource reservation, or even failure of QoS provision. Security is thus an important issue for a signalling system. Therefore, security mechanisms unit necessary to prevent QoS systems from being maliciously attacked.

II. QUALITY OF SERVICE

Quality of service (QoS) is that the [2] performance level of a service offered by the network to the user. The goal of QoS provisioning is to realize an additional settled network behaviour, in order that data carried by the network are often higher delivered and network resources are often better used. A network or a service supplier offers completely different sorts of services to the users. After receiving a service request from the user, the network has got to make sure that service necessities of the users flow are met, as per the agreement, throughout the period of the flow (a packet stream from the source to the destination).

In alternative words, the network has got to offer a set of service guarantees whereas transporting a flow. When receiving a service request from the user, the first task is to look out associate acceptable loop-free path from the supply to the destination which can have the specified resources to satisfy the QoS demand of the required service. This method is thought as QoS routing. QoS routing has to decide on associate acceptable path that meets the QoS constraints per the service request created by the user. When finding an

appropriate path, a resource reservation protocol is used to reserve necessary resources on that path. QoS guarantees are often provided solely with acceptable resource reservation techniques. Technically there are two ways in which QoS can be achieved: Over-provisioning, Traffic engineering: QoS provisioning usually needs negotiation between host and network, call admission control, resource reservation, and priority scheduling of packets. QoS are often rendered in AWNs through many ways in which, viz., per flow, per link, or per node. In AWNs, the boundary between the service supplier (network) and the user (host) isn't outlined clearly, so creating it essential to possess higher coordination among the hosts to realize QoS. Characteristics of AWNs like lack of central coordination, mobility of hosts, and restricted availableness of resources create QoS provisioning terribly difficult.

III. BASIC MODEL OF QOS FRAMEWORKS

The key component of any QoS framework [3] is the QoS model which defines the way user requirements are met. The key design issue here is whether to serve users on a per session basis or on a per class basis. Each class represents an aggregation of users based on certain criteria.

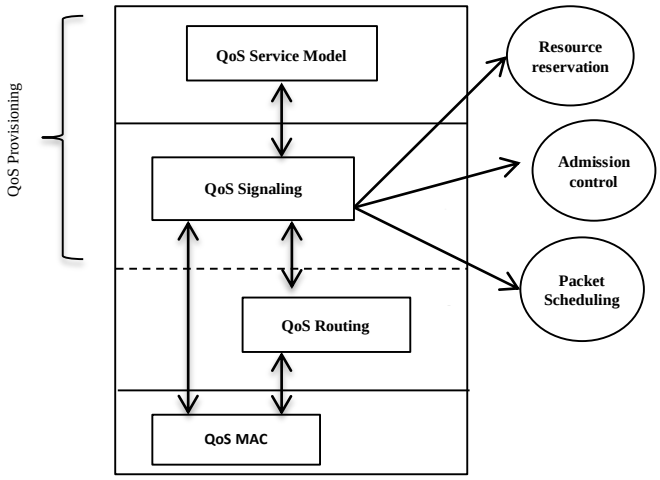

Fig.2 Basic QoS Framework Model

The other key components of the framework are, QoS routing [4] which is used to find all or some of the feasible paths in the network that can satisfy user requirements, QoS signaling for resource reservation, QoS medium access control, call admission control, and packet scheduling schemes as shown in figure 2 above. The combination of QoS service model and QoS signaling is called QoS provisioning. QoS Provisioning is the extra activity done by simple ad hoc network model to achieve quality of service. The QoS modules should react promptly to changes in the network state (topology changes) and flow state (change in the end-to-end view of the service delivered). In what follows, each components functionality and its role in providing QoS in AWNs will be described:

IV. SECURITY ISSUES IN QOS

Supporting quality of service [11] during a mobile ad hoc network (MANET) may be a difficult task, significantly within the presence of malicious users. Security may be a vital facet of QoS provisioning in MANET environment. We tend to give a depth description of all possible types of attacks and threats on QoS frameworks which will disrupt QoS framework in MANETs.

a) Over-Reservation

A greedy node will exploit the signalling protocol and reserve a lot of bandwidth for one in every of its Real time flows than what it truly must use. In an extreme case, the greedy node may reserve bandwidth for non-existing flows so as to perform a DoS attack or to make sure that its own Real time applications may be supported within the close to future.

b) State Table Starvation

The state table starvation attack is another attack specific to reservation-based signalling protocols, an attack is feasible once the protocol needs flow reservations, e.g., in INSIGNIA. It implies the reservation of state for illegitimate flows and this ends up in a state table exhaustion once the storage capability of a node is exceeded.

c) Over/Under-Reporting of accessible bandwidth

In this attack, a malicious node on the path from the source to the destination node incorrectly represents the available bandwidth on an outgoing link. For instance, in SWAN, a malicious node on a path may launch this attack by modifying the bottleneck bandwidth (BB) field of the BPReq message thus on incorrectly report the available bandwidth on its outgoing link.

d) QoS Degradation

QoS degradation represents a new class of attacks in QoS signalling. It involves increase within the delay or interference of the Real time packets to unacceptable levels.

e) Black hole Attack

In this attack [12] a malicious node informed that it has efficient path to destination. These fake replies area unit typically fictional to divert network traffic through the malicious node for eavesdropping, or simply to attract all traffic thereto thus on perform a denial of service attack by dropping the received packets.

f) Wormhole Attack

The wormhole attack [13] is one altogether the foremost powerful bestowed here since it involves the cooperation between a pair of malicious nodes that participate inside the network and create tunnel through all traffic is divert.

g) Timing Attack

The temporal order attack exploits the sequence during which signalling messages area unit sent or the timers outlined by the

protocol, with the target of perturbing the operation of the protocol. Each reservation-based or reservation-less signalling protocols is prone to this sort of attack. However, INSIGNIA above all, doesn't have simply exploitable temporal order dependencies so isn't prone to the temporal order attack.

h) Dropping Attacks

Malicious or inconsiderate nodes [15] deliberately drop all packets that don't seem to be destined for them. Whereas malicious nodes aim to disrupt the network association, inconsiderate nodes aim to preserve their resources. Dropping attacks will forestall end-to-end communications between nodes, if the dropping node is at a crisis. It'd together prune the network performance by inflicting information packets to be retransmitted, new routes to the destination to be discovered, and to boot type.

i) Flooding Attack

Flooding [14] may be a Denial of Service (DoS) attack that's designed to bring a network or service down by flooding it with giant amounts of traffic. Flood attacks occur once a network or service becomes thus weighed down with packets initiating incomplete connection requests that it will now not method real connection requests. By flooding a server or host with connections that can't be completed, the flood attack eventually fills the host's memory buffer. Once this buffer is full no additional connections is created, and also the result's a Denial of Service. Neither reservation-based nor reservation-less signalling protocols area unit immune to flooding DoS attacks.

j) Replay Attack

Replay attacks unit "Man inside the middle" attacks that involve intercepting information packets and replaying them, that is, resending them as is (with no decryption) to the receiving server. Any protocol that allows the exchange of unauthenticated information is in danger of modification and replay.

k) Theft of Services

Theft of services is that the legal term for a criminal offense that's committed once somebody obtains valuable services as against merchandise by deception, force, threat or completely different unlawful implies that, i.e., whereas not lawfully compensating the provider for these services.

l) Denial Of Services Attacks

A denial-of-service attack (DoS attack) may be a trial to make a machine or network resource or services unobtainable to its supposed users.

V. Literature survey

A framework for QoS could be a complete system that tries to provide required/promised services to every user or application. All components among this technique get together in providing the specified services. There are only four QoS framework are available in literature. The detail description of those frameworks is given below:

S.B. Lee et' al [6] was developed insignia QOS framework for providing adjustive services in AWNs. adjustive services support applications that need solely a minimum quantitative QoS guarantee (such as minimum bandwidth) known as base QoS. The service level is extended later to increased QoS once decent resources become obtainable. Here user sessions adapt to the obtainable level of service while not express communication between the source–destination pairs.

The insignia QOS framework permits packet audio, video and time period information applications to specify their most and minimum information measure desires and plays a central role in resource allocation, restoration management, and session adaptation between human activity mobile hosts. Supported the supply of end-to-end information measure, QOS mechanisms plan to offer assurances in support of adjustive services. To support adjustive service, the insignia QOS framework establishes and maintains reservations for continuous media flows and small flows. To support these communication services the badge QOS framework includes the subsequent beaux arts parts as illustrated in Fig. 3.

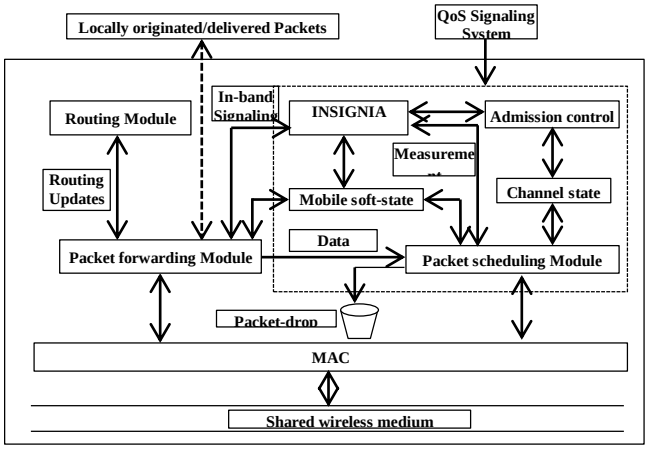

Fig.3 INSIGNIA QoS Framework.

This framework will scale down, drop, or proportion user sessions adaptively supported network dynamics and user-supplied adaptation policies. A key part of this framework is that the badge in-band communication system, that supports quick reservation, restoration, and adaptation schemes to deliver the adjustive services. The communication system is light-weight and responds quickly to changes within the configuration and end-to-end QoS conditions. The badge framework is delineated in Fig.7. The routing module is freelance of different parts and thus any existing routing protocol is used. Insignia assumes that the routing protocol provides new routes just in case of topology changes.

During the restoration method, the badge framework doesn't favor rerouted flows over existing flows (e.g., by forcing existing flows to scale right down to their minimum necessities

to permit rerouted or new flows to be admitted). During this sense, badge avoids the introduction of further service fluctuations to existing flows in support of the restoration of rerouted flows. As a results of this policy, admission management merely rejects scales down any rerouted flows once scarce resources are obtainable on a brand new path. 3 sorts of restoration are supported by the insignia QOS framework an instantaneous restoration, degraded restoration, permanent degradation. The insignia communication system supports 3 adaptation commands that ar sent from the destination host to the supply victimization QOS reports: scale-down command, drop command, scale-up command.

D. Dharmaraju et al. [7] has projected INORA QoS framework they create use of the badge in-band sign system with TORA [10] routing protocol within the INORA theme. It overcome the deficiency of badge that doesn't take any facilitate from the network with relation to redirecting the flow on routes that ar able to give the desired QoS guarantees. In INORA author build use of feedback on a per-hop basis to direct the flow on the route that's able to give the QoS necessities of the flow.

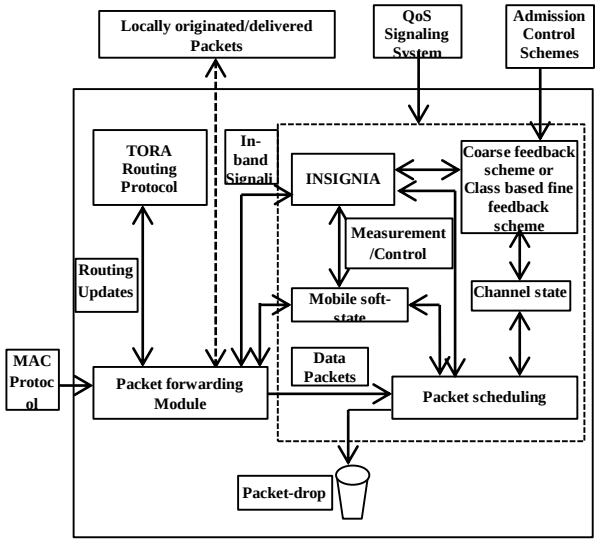

Fig.4 INORA QoS Framework.

TORA operates by making a Directed Acyclic Graph (DAG) frozen at the destination. The DAG is extraordinarily helpful in theme since it provides multiple routes from the supply to the destination. The INORA QoS framework is shown in Fig.4. The QoS resource reservation sign mechanism interacts with routing protocol to deliver QoS guarantees. The TORA routing protocol make available multiple routes between a given source–destination combine. The badge sign mechanism provides feedback to the TORA routing protocol relating to the route chosen and asks for alternate routes if the route provided doesn't satisfy the QoS necessities. For resource reservation, a soft state reservation mechanism is utilized. INORA may be classified into 2 themes: coarse feedback theme and class-based fine feedback scheme.

Ahn et al. [8] proposed a distributed network model known as stateless wireless ad hoc networks (SWAN) that assumes a best-effort macintosh protocol and uses feedback based mostly management mechanisms to support time period services and repair differentiation in AWNs illustrated in Fig. 5. SWAN uses a neighborhood rate management mechanism for regulation injection of best-effort traffic into the network, a source-based admission management whereas accepted new time period sessions, and a certain congestion notification (ECN) mechanism for dynamically regulation admitted time period sessions. During this model intermediate nodes area unit mitigated from the responsibility of maintaining per flow or mixture state info not like state full QoS models cherish badge and INORA. Changes in topology and network conditions, even node and link failures, don't have an effect on the operation of the SWAN system. SWAN uses Distributed management algorithms that is any classified in to a few categories: native rate management of best effort traffic, source-based admission of time period traffic, dynamic regulation of time period traffic. In SWAN author used two forms of regulation algorithms: Source-Based Regulation, Network-Based Regulation. This makes the system straightforward, robust, and scalable.

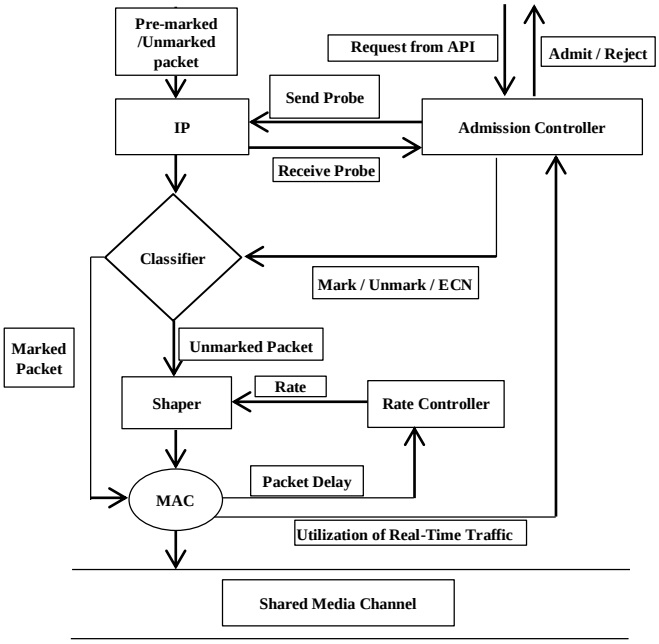

Fig.5 SWAN model.

Vivek et al. [9] has proposed Proactive RTMAC (PRTMAC) could be a cross layer QoS framework, with associate degree on-demand QoS extension of DSR routing protocol at the network layer and RTMAC (real-time MAC) [5] protocol at the MAC layer. PRTMAC could be a tightly coupled resolution, which needs the information measure reservation and information measure accessibility estimation services from the underlying mack protocol. It's designed to supply increased period traffic support and repair differentiation to

extremely mobile spontaneous wireless networks comparable to that fashioned by military combat vehicles. The performance of period sessions in spontaneous wireless networks is laid low with quality of nodes in many alternative ways that.

The two major ways that during which quality affects period session's ar breakaways and reservation clashes. If a node taking part in an exceedingly QoS session moves out of the transmission vary of either or each of its upstream and downstream nodes, we are saying the QoS session is broken because of breakaway. The PRTMAC framework is shown in Fig. 6. RTMAC [5] is employed because the mack protocol. The out-of-band communication channel gathers extra info concerning the continuing period sessions, specified proactive measures is taken to shield these sessions from breakaways and clashes.

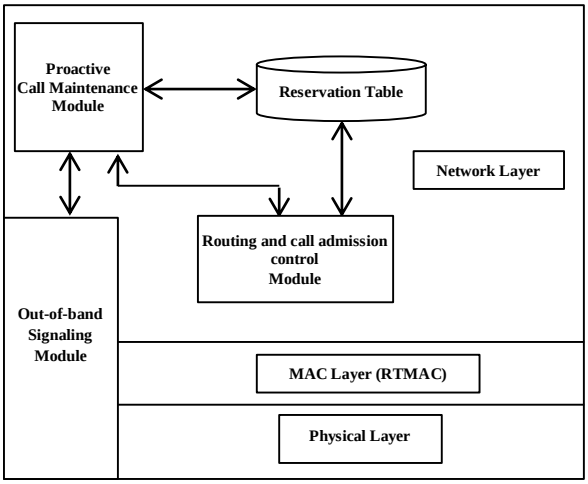

Fig.6 Modules in PRTMAC Framework.

PRTMAC uses Crossover-time prediction technique that predict time at which a node crosses another nodes data transmission range r. it also use breakaways handling techniques to handle link break in the network. It also resolve the problem of clashes in MAC layer.

VI. SECURITY ANALYSIS OF FRAMEWORKS

Here we analyses QoS frameworks for different security attack and threats

A. INSIGNIA,

As we examines that there is no security mechanism present in INSIGNIA QoS framework. So it is vulnerable to threats like over/under-reporting of available bandwidth, over-reservation, state table starvation, QoS degradation, information disclosure, theft of services. The possible attacks on INSIGNIA QoS framework are flooding attack, replay attack, black hole attack, wormhole attack and denial of service (DoS) attack, attacks on information in transit and attacks against routing.

B. INORA

As we inspects that INORA QoS framework is slight secure against few attacks like timing attack, replay attack. But it is vulnerable to threats like over-reservation, QoS degradation, information disclosure, theft of services. The possible attacks on INORA QoS framework are, flooding attack, black hole attack, wormhole attack and denial of service (DoS) attack, attacks on information in transit and attacks against routing.

C. SWAN

As we determine that SWAN QoS framework is little secure against some attacks like flooding attack, replay attack, wormhole attack. So it is vulnerable to threats like over/under-reporting of available bandwidth, over-reservation, state table starvation, QoS degradation, information disclosure, theft of services. The possible attacks on SWAN QoS framework are timing attack, black hole attack, and denial of service (DoS) attack, attacks on information in transit and attacks against routing.

D. PRTMAC

As we observes that PRTMAC is some secure against attacks and threats. But it also vulnerable to threats like QoS degradation, information disclosure, theft of services. The possible attacks on PRTMAC QoS framework are timing attack, black hole attack, and denial of service (DoS) attack, attacks on information in transit and attacks against routing.

VII. COMPARISON

Here we compare the existing QoS frameworks on different parameters

parameters	QoS Frameworks			
	INSIGNIA	INORA	SWAN	PRTMAC
Type of Service support	Adaptive services, audio, video, and real-time data applications	Real-time audio, video and data	Real time UDP traffic, and best effort UDP and TCP traffic	Enhanced real-time traffic support and service differentiation to highly mobile ad hoc wireless networks. such as military combat vehicles
QoS Model	IntServ model	IntServ model	DiffServ model	DiffServ model
Type of signaling used	In-band signaling	In-band signaling	ECN-based regulation	out-of-band
Routing Protocol used	TORA, DSR, ZRP, AODV	TORA	AODV	DSR
MAC Protocol Used	IEEE 802.11e MAC protocol	IEEE 802.11e MAC protocol	IEEE 802.11e MAC protocol	RTMAC
End-to-end delay	High	Very High	Low	Medium

Throughput (%)	Low	Medium	High	Very High
Vulnerable to threats	Over/under -reporting of available bandwidth, over-reservation, state table starvation, QoS degradation , information disclosure, theft of services.	Over-reservation, QoS degradation, information disclosure, theft of services.	Over/under -reporting of available bandwidth, over-reservation, state table starvation, QoS degradation , information disclosure, theft of services.	QoS degradation, information disclosure, theft of services.
Vulnerable to attacks	Flooding attack, replay attack, black hole attack, wormhole attack and denial of service (DoS) attack, over-reservation and state-table starvation attacks, QoS degradation etc.	Flooding attack, black hole attack, wormhole attack and denial of service (DoS) attack, QoS degradation etc.	Timing attack, black hole attack, and denial of service (DoS) attack, QoS degradation etc.	Timing attack, black hole attack, and denial of service (DoS) attack, state-table starvation attacks, QoS degradation etc.

VIII. CONCLUSION

INSIGNIA framework provides an integrated approach to QoS provisioning by combining in band signalling, call admission control, and packet programing along. The soft state reservation scheme employed in this framework ensures that resources area unit quickly discharged at the time of path reconfiguration. But, this framework supports solely adaptive applications, for instance, transmission applications. Conjointly as this framework assumes that routing protocol provides new routes within the case of topology changes. If enough resources aren't available as a result of the dynamical topology, the enhanced QoS application is also downgraded to base QoS or maybe to best-effort service. As this framework uses in-band signalling, resources aren't reserved before the particular information transmission begins. Therefore INSIGNIA isn't appropriate for Real time applications that have demanding QoS needs.

INORA is better than INSIGNIA in this it will search multiple methods with lesser QoS guarantees. It uses the INSIGNIA in-band signalling mechanism. Since no resources area unit reserved before the particular information transmission begins and since data packets got to be transmitted as best-effort packets just in case of admission control failure at the intermediate nodes, this model might not be appropriate for applications that need hard service guarantees.

SWAN provides a framework for supporting Real time applications by presumptuous a best-effort waterproof protocol and not creating any resource reservation. It uses feedback based mostly management mechanisms to control Real time traffic at the time of congestion in the network. As best-effort traffic is a buffer zone for Real time traffic, this model doesn't work well in situations wherever most of the traffic is Real time in nature. Even supposing this model is climbable (because the intermediate nodes don't maintain any per flow or combination state information), it cannot give arduous QoS guarantees attributable to lack of resource reservation at the intermediate nodes. AN admitted Real time flow might encounter periodic violations in its bandwidth needs.

PRTMAC is suitable in providing higher Real time traffic support and repair differentiation in high quality AWNs like military networks shaped by high rate combat vehicles, fleet of ships, fleet of air-crafts wherever the ability resource isn't a serious concern. In AWNs, shaped by low power and resource forced hand-held devices, having another channel might not be an efficiently viable answer.

IX. PROPOSED QOS FRAMEWORK

In the literature we've got study that in QoS provisioning techniques employed in existing QoS framework. Security wasn't provided for any QoS framework like INSIGNIA, INORA, SWAN and PRTMAC. Whereas these frameworks tend to be at risk of variety of threats and attacks. QoS frameworks are typically subjected to first level of attack; the adversary focuses on disrupting the basic mechanisms of the QoS provisioning, such as resource reservation, admission control, flow restoration, and adaptation, which are essential for appropriate QoS operation. During this work I have proposed a secure and proficient QoS framework which can be tries to realize best performance in secured manner. I have conjointly proposed a new signalling methodology which can be lightweight weight and low process overhead.

REFERENCES

[1]. Jie Wu, Ivan Stojmenovic, "Guest Editors' Introduction: Ad Hoc Networks," IEE *Computer*, vol. 37, no. 2, pp. 29-31, Feb. 2004.

[2]. Kui Wu and Janelle harms, QoS support in Mobile Ad hoc networks. Computing Science Department University of Alberta 2001.

[3]. Reddy, T. B., Karthigeyan, I., Manoj, B. S., & Murthy, C. S. R., "Quality of service provisioning in ad hoc wireless networks: a survey of issues and solutions" Ad Hoc Networks, 4(1), 83-124, 2006.

[4]. Hanji, Bhagyashri R., and Rajashree Shettar. "Survey on QoS Routing protocols challenges and recent advances in

MANETs." Journal of Computing Technologies 1, no. 2, 2012.

[5]. B.S. Manoj, C. Siva Ram Murthy, Real-time traffic support for ad hoc wireless networks, in: Proceedings of IEEE ICON 2002, August 2002, pp. 335–340.

[6]. S.B. Lee, A. Gahng-Seop, X. Zhang, A.T. Campbell, INSIGNIA: An IP-based quality of service framework for mobile ad hoc networks, Journal of Parallel and Distributed Computing 60 (4) (2000) 374–406.

[7]. D. Dharmaraju, A.R. Chowdhury, P. Hovareshti, J.S. Baras, INORA—A unified signalling and routing mechanism for QoSsupport in mobile ad hoc networks, in: Proceedings of ICPPW 2002, August 2002, pp. 86–93.

[8]. H. Ahn, A.T. Campbell, A. Veres, L. Sun, Supporting service differentiation for real-time and best-effort traffic in stateless wireless ad hoc networks, IEEE Transactions on Mobile Computing 1 (3) (2002) 192–207.

[9]. V. Vivek, T. Sandeep, B.S. Manoj, C. Siva Ram Murthy, A novel out-of-band signaling mechanism for enhanced real time support in tactical ad hoc wireless networks, in: Proceedings of IEEE RTAS2004, May 2004.

[10]. V. Park, S. Corson, "Temporally Ordered Routing Algorithm (TORA) version 1 functional specification", draft −IETF − MANET− TORA− spec− 04.txt, July 2001.

[11]. Zouridaki, Charikleia, Marek Hejmo, Brian L. Mark, Roshan K. Thomas, and Kris Gaj. "Analysis of Attacks and Defense Mechanisms for QoS Signaling Protocols in MANETs." In Wireless Information Systems, pp. 61-70. 2005.

[12]. Mohammad Al-Shurman and Seong-Moo Yoo, Seungjin Park, "Black Hole Attack in Mobile Ad Hoc Networks" ACMSE'04, April 2-3, 2004, Huntsville, AL, USA.

[13]. Yih-Chun Hu, Adrian Perrig, and David B. Johnson., "Packet Leashes A Defense against Wormhole Attacks in Wireless Ad Hoc Networks" In Proceedings of the Twenty-Second Annual Joint Conference of the IEEE Computer and Communications Societies (INFOCOM 2003), April 2003.

[14]. Kannhavong, Bounpadith, Hidehisa Nakayama, Yoshiaki Nemoto, Nei Kato, and Abbas Jamalipour. "A survey of routing attacks in mobile ad hoc networks." IEEE Wireless communications 14, no. 5 (2007).

[15]. Ukey, Aishwarya Sagar Anand, and Meenu Chawla. "Detection of packet dropping attack using improved acknowledgement based scheme in MANET." IJCSI International Journal of Computer Science Issues 7, no. 4 (2010): 12-17.