IJNRD.ORG ISSN : 2456-4184
INTERNATIONAL JOURNAL OF NOVEL RESEARCH AND DEVELOPMENT (IJNRD) | IJNRD.ORG
An International Open Access, Peer-reviewed, Refereed Journal

MMF Clustering: A On-demand One-hop Cluster Management in MANET Services Executing Perspective

Bhupathi Jeevana Sree Harshita,

UG Student,

Department of Computer Science and Engineering,
Karunya Institute of Technology and Sciences,
Coimbatore, India
bhupathijeevana@karunya.edu.in

Dr. A. Kathirvel, Professor
Department of Computer Science and Engineering,
Karunya Institute of Technology and Sciences,
Coimbatore, India
kathirvel@karunya.edu

Abstract - **Mobile Ad hoc Network (MANET) is an alternate wireless network architecture which is finding increasing use in defence, law enforcement, disaster management and commercial applications. MANETs are peer-to- peer networks in which mobile devices communicate with one another by routing the messages which are beyond their communication range without the support of any external infrastructure. The nodes thus act as routers in addition to being the end devices. The mobility of the nodes and the open architecture in which the nodes are free to join or leave the network keep changing the topology of the network. The routing in such scenarios becomes a challenging task since it has to take into account the constraints of resources of mobile devices. The routing protocols developed for MANETs can be grouped into three classes namely, proactive or table driven protocols, reactive or on-demand routing protocols and a combination of these two protocols which are clubbed into hybrid routing protocol category. Ad hoc On-demand Distance Vector (AODV) protocol and Destination Sequence Routing (DSR) protocol are widely used reactive routing protocols. The experimental results for performance comparison of these two routing protocols have confirmed that, though the performance of AODV and DSR is comparable for small and medium size networks, AODV performs better than DSR in large, dense networks with high load and mobility. Two approaches mainly have been adopted to secure the routing protocols; in the first approach the trust evaluation of nodes is done by monitoring the behaviour of the nodes. If the trust value of a node is less than the threshold then it is declared a malicious node and is not permitted to participate in routing process. This approach though is light on resources but it is time consuming, has difficulty in setting the threshold value and is less reliable. The second approach to secure the routing protocol is by use of cryptographic techniques involving symmetric and asymmetric cryptography. The cryptographic techniques though provide better security but are computationally very resource intensive.**

Keywords—**Mobile Ad-hoc network (MANET), Ad hoc on-demand distance vector (AODV), Distance sequence routing (DSR), hybrid routing, cryptographic techniques, Weighted clustering algorithm(WCA).**

I. INTRODUCTION

In Wireless Networks, the wireless nodes can change their location and configure themselves. The network can use a standard Wi-Fi connection or a cellular or satellite transmission. Some networks are restricted to a local area of wireless devices (such as a group of laptop computers), while others may be connected to the Internet. An example of such a network is a MANET (Mobile Ad Hoc Network) that allows vehicles to communicate with roadside equipment. The challenge faced by Ad Hoc Networks (AD HOC NETWORK) used in this Report is the transmission of real time multimedia data like the Audio and Packet, while considering their QoS and low latency demands. Mobile Ad hoc Networks (MANET) are utilized to set up wireless communication in improvised environments without a predefined infrastructure or centralized administration. Therefore, MANET has been normally deployed in adverse and hostile environments where central authority point is not necessary. Another unique characteristic of MANET is the dynamic nature of its network topology which would be frequently changed due to the unpredictable mobility of nodes. Furthermore, each mobile node in MANET plays a router role while transmitting data over the network. Hence, any compromised nodes under an adversary's control could cause significant damage to the functionality and security of its network since the impact would propagate in performing routing tasks. Several work addressed the intrusion response actions in MANET by isolating uncooperative nodes based on the node reputation derived from their behaviors. Such a simple response again malicious nodes often neglects possible negative side effects involved with the response actions. In MANET scenario, improper countermeasures may cause the unexpected network partition, bringing additional damages to the network infrastructure. To address the above-mentioned critical issues, more flexible and adaptive response should be investigated. The notion of risk

can be adopted to support more adaptive responses to routing attacks in MANET. However, risk assessment is still a nontrivial, challenging problem due to its involvements of subjective knowledge, objective evidence, and logical reasoning. Subjective knowledge could be retrieved from previous experience and objective evidence could be obtained from observation while logical reasoning requires a formal foundation. Wang et al. proposed a naïve fuzzy cost-sensitive intrusion response solution for MANET. Their cost model took subjectiveknowledge and objective evidence into account but omitted a seamless combination of two properties with logical reasoning.

first checks the value of sequence number in its routing table. The RREP is accepted if its sequence is higher than that in the routing table.

In this paper, we seek a way to bridge this gap by evidence (D-S theory), which offers an alternative to traditional probability theory for representing uncertainty. D-S theory has been adopted as a valuable tool for evaluating reliability and security in information systems and by other engineering fields, where precise measurement is impossible to obtain or expert elicitation is required. D-S theory has several characteristics. On the other hand, in a multihop network, nodes rely on other intermediate nodes to transmit if the destination node is out of their radio range. In contrary to the traditional wireless network, MANET has a decentralized network infrastructure. MANET does not require a fixed infrastructure; thus, all nodes are free to move randomly. MANET is capable of creating a self-configuring and self-maintaining network without the help of a centralized infrastructure, which is often infeasible in critical mission applications like military conflict or emergency recovery.

II. RELATED WORKS

The following are the inferences from the literature reviews used to build this paper.

In [1] the author proposed a distributed and cooperated "black hole" node detection mechanism which composes four sub-steps: (1) local data collection (2) Local detection (3) Cooperative detection (4) Global reaction. In local data collection, each node collects information through overhearing packets to evaluate if there is any suspicious node in its neighborhood. If finding one, the detecting node would initiate the local detection procedure to analyze whether the suspicious one is a malicious black hole node.

In [2] the author proposed a REAct scheme. This scheme provides publicly confirmable evidence of node misbehavior. REAct constitutes of three phases: (i) Audit phase, (ii) Search phase and (iii) Identification phase. The audit phase verifies the packet forwarding from audited node to the destination node. The audit phase constitutes three steps: (a) sending of an audit request. (b) Building up behavioral proof and (c) then processing of this build up behavioral proof.

In [3] the author proposed dynamic trust model to enhance the security of message routing in Mobile Ad hoc networks. Initially each node in the system is authenticated by an authentication mechanism if possible and is assigned a trust value according to its identity which would include a historical record of its trust level. A logical trust assignment hierarchy, similar to the hierarchies for distributed systems and Pretty Good Privacy is described.

In [4] the author proposed an anomaly detection scheme using dynamic training method in which the training data is updated at regular time intervals. To express state of the network at each node, multidimensional feature vector is found. Each dimension is counted up on every time slot. To detect the attack, the destination sequence number is taken into account. In normal state, each node's sequence number changes depending on its traffic conditions.

In [5] the author proposed DPRAODV (detection, prevention and reactive AODV) to prevent security of black hole by informing other nodes in the network. It uses normal AODV in which a node receives the Route reply (RREP) packet which

III. EXISTING SYSTEMS

Mobile Ad hoc Networks (MANET) are utilized to set up wireless communication in improvised environments without a predefined infrastructure or centralized administration. Therefore, MANET has been normally deployed in adverse and hostile environments where central authority point is not necessary. Another unique characteristic of MANET is the dynamic nature of its network topology which would be frequently changed due to the unpredictable mobility of nodes. Furthermore, each mobile node in MANET plays a router role while transmitting data over the network.

Hence, any compromised nodes under an adversary's control could cause significant damage to the functionality and security of its network since the impact would propagate in performing routing tasks. Routing protocol is a protocol used by a router to determine the appropriate path over which data is transmitted. The routing protocol also specifies how routers in a network share information with each other and report changes. The routing protocol enables a network to make dynamic adjustments to its conditions, so routing decisions do not have to be predetermined and static.

Ad-hoc On-Demand Distance Vector routing (AODV) also called as pure on-demand route acquisition system works both on wired and wireless media. A node does not have to discover any routing information nor participate in any periodic routing table exchanges. The nodes broadcast route discovery packets only when necessary. They have to distinguish between local connectivity management and general topology maintenance. The changes in routing information are only transmitted to neighboring nodes that are likely to need the information.

Path discovery is initiated whenever a node needs to communicate with another nodeFIGURE. It is started by initializing two separate counters node sequence number and broadcast_id. The source (node A in the figure) initiates route discovery by broadcasting Route request packets (RREQ). RREQ contains the following:

< Source address; source sequence number; broadcast id; destination address; destination sequence number; hop count >

Source sequence number is used to maintain freshness information about the reverse route to the source. Destination Sequence number is used to specify how fresh a route to destination must be. An Intermediate node, if it has a route to the source may reply to the source with a Route Reply packet (RREP) or forward the RREQ packet to the next available node after increasing the hop count. The Reverse path is set up through the RREQ packets. As the RREQ packet traverse from the source to the destination, it keeps a track of the path it follows. As a result, the reverse path is stored in the RREQ. When an RREQ packets arrive at a node which has a route to the destination. It checks for following conditions.

IV. PROPOSED SYSTEM

During congestion, Trust management plays an important role in improving the efficiency of a network in terms of throughput, latency and goodput. Based on the network conditions, Trust management helps in serving the packets better. Here, we focus on the Trust management techniques proposed to achieve QoS for Packet data over AD HOC NETWORK. In our scheme, we emphasize on serving the prioritized Packet packets over wireless networks.

Seong-ryong et al., proposed a Packet streaming framework that allows applications to mark packets with different priority and use multi-queue congestion control inside routers to effectively drop the less-important packets during Trust overflow. In [1] author proposed a Trust management scheme called Frame-Level Packet Discard with Dynamic Thresholds (FDDT), in which the packets are sorted/dropped based on the following conditions:

The first packet of B or P-frame is discarded when the Trust size reaches certain threshold levels.

An I-frame packet is only discarded when Trust is completely full.

If early packet of a frame is dropped, all the subsequent packets are dropped.

When two packets are competing, lower priority packets are dropped.

All incoming packets are dropped when the Trust is full. FDDT scheme showed results with great advantage for Packet quality, while having a small increase in computational complexity.

A Drop Dependency Based (DDB) scheme was proposed, where basic information of the packet priorities was provided in the packet header and a Trust management was done based on this information. An optimized strategy operates on the Head of line (HOL: The packet which resides longest in the Trust) group of packets. By dropping the HOL packet with the lowest priority, a significant improvement in the Packet quality was achieved. This was extended to achieve an optimal combination of scheduler and drop strategy. There have been some smart router based solutions such as Active networking. In which routers play very important role of smartly discarding the packets based on a priori knowledge of the transmission in progress. But, having functionality and computational complexity in the routers can go against the general norm of just forwarding the packets to the next node. But, this feature can be of great advantage in AD HOC NETWORKs where the mission/Packet information of the current communication can be transmitted in the header during session establishment. It means that more resources are allocated for higher QoS requirement streams. The lower QoS requirement stream packets are dropped while giving more access to important streams. This can lead to starvation of resources for the later. A joint APP and MAC adaptation scheme was proposed with the use of MPEG-4 and its Fine Granularity Scalability (FGS) extension. In this work, packets containing multimedia data are classified into different classes and in the light of poor network conditions only packets with high class value are transmitted. The network conditions are jointly measured by combining the information obtained by the retransmission number of lost MAC frames (ARQ) and the information provided by the RTCP protocol.

The idea is to retransmit only the important information in a Packet in order to achieve high quality of Packet streaming. Retransmission of important packets is a good idea, but since prevention is better than cure and we need to protect the high priority information and reduce the packet loss rate (PLR). In our scheme, the priority to the slices in the Packet is assigned based on the Cumulative Mean Square Error (CMSE) contributed by their loss.

We use the network simulator NS-2 for implementing our scheme. NS-2 has provision for Constant bit rate Data packets. Since, we use Packet traffic in our simulations; we use Evalvid to generate Packet packets. At the application layer, the Packet packets that are generated from the H.264 trace files using the CSME based prioritization is attached to the NS-2 agent using the Evalvid.

The CMSE contributed by the loss of the slice is computed in Equation below as the sum of mean squared error (MSE) over the current and all the other frames in the GOP,

$$CMSE = \sum_{i=current\ frame\ with\ slice\ loss-t}^{last\ frame\ of\ GOP} \left\{ \frac{1}{H \times W} \sum_{j=1}^{H} \sum_{k=1}^{W} \left(\widetilde{Pel}_{i,j,k} - \widetilde{Pel}_{i,j,k} \right)^2 \right\}$$

However, the computation of slice CMSE introduces high computational overhead as it requires decoding the entire GOP for every slice loss. The slice contributing the highest distortion is the most important slice (i.e., highest priority). This process defines the relative importance order for the slices in the GOP. The basic Queue structure in ns-2. The Interface Queue (IFQ) is the Trust between the Link layer and the MAC that holds the packets when they do not get channel access during congestion in the network. The Link layer is responsible for addressing. It makes use of the Address Resolution Protocol (ARP) to decide the source and destination address of a packet. MAC layer is responsible for the channel access and scheduling. It continuously monitors the channel and then schedules the packet transfer based on the availability of the channel.

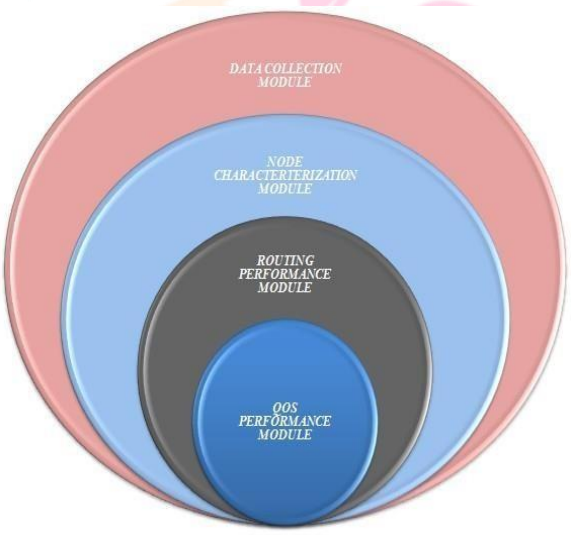


Figure1.1. Proposed Architecture

PROPSED ADVANTAGES

1. Redundancy can be avoided
2. Inconsistency can be eliminated
3. Data can be Shared
4. Standards can be enforced
5. Security restrictions ca be applied
6. Integrity can be maintained
7. Conflicting requirements can be balanced
8. Data independence can be achieved.

V. MODULES DESCRIPTION

AODV Protocol:

AODV, nodes obtain routes by periodic exchange oftopology information with other nodes and maintainroute information all the time. AODV protocol is a variation of the pure Link-state Routing (LSR) protocol and is designed specifically for MANET. AODV protocol achieves optimization over LSR through the use of multipoint relay (MPR) to providean efficient flooding mechanism by reducing the number of transmissions required.

TRUST MODELMECHANISM:

In this section, we articulate an adaptive TRUST MODEL mechanism based on quantitative risk estimation and risk tolerance. Instead of applying simple binary isolation of malicious nodes, our approach adopts an isolation mechanism in atemporal manner based on the risk value. We perform risk assessment with the extended D-S evidence theory introduced in Section 3 for both attacks and corresponding countermeasures to make more accurate response decisions illustrated Evidence collection. In this step, Intrusion DetectionSystem (IDS) gives an attack alert with a confidence value, and then Routing Table Change Detector (RTCD) runs to figure out how many changes on routing table are caused by the attack.

Response to Routing Attacks:

In our approach, we use two different responses to deal with different attack methods: routing table recovery and node isolation. Routing table recovery includes local routing table recovery and global routing recovery. Routing table recovery is an indispensable response and should serve asthe first response method after successful detection of attacks. In proactive routing protocols like AODV, routingtable recovery does not bring any additional overhead since it periodically goes with routing control messages. Also, as long as the detection of attack is positive, this response causes no negative impacts onexisting routing operations. Node isolation may be the most intuitive way to prevent further attacks from being launched by malicious nodes in MANET.

Risk Assessment:

Since the attack response actions may cause more damages than attacks, the risks of both attack and responseshould be estimated. We classify the security states of MANET into two categories: {Secure, Insecure}. In other words, the frame of discernment would be

{_, {Secure}, {Insecure}, {Secure, Insecure}}. Note that

{Secure, Insecure} means the security state of MANET could be either secure or insecure, which describes the uncertainty of the security state. BelfInsecureg is used to represent the risk of MANET.

Routing:

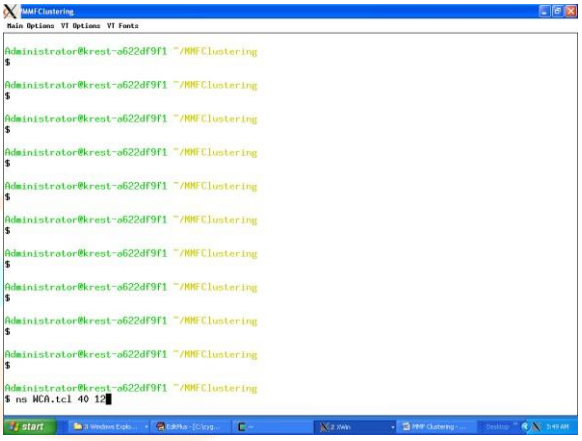
When the packets are sending from the source, they are transferred to the destination through the routers. Routers check for the IP address given by the source with their own IP address for the destination confirmation.

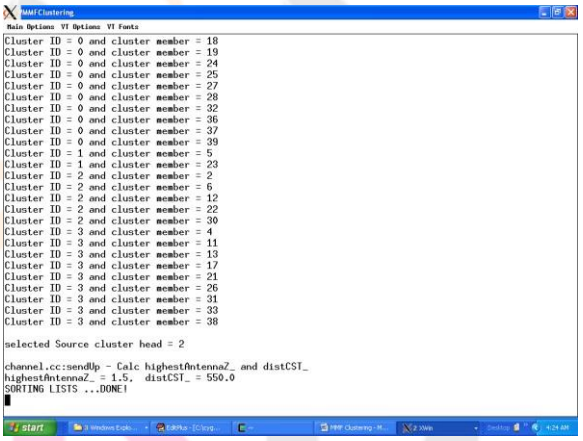
Table 5.1 Comparision of different attacks in MANETs

Attacks	Type of Attack	Techniques used for Prevention
Wormhole Attack	Active	SAW DAW, HMTI, Packet Leases, DELPHI
Sybil Attack	Active	Robust and light weight detection technique
Black Hole Attack	Active	SADOV
Denial of Service (DoS)	Active	LMAC and Evasion
Misrouting Attack	Active	Watchdog Mechanism
Eavesdropping	Passive	SSL
Traffic Analysis	Passive	Transmission Schedules

VI. RESULTS

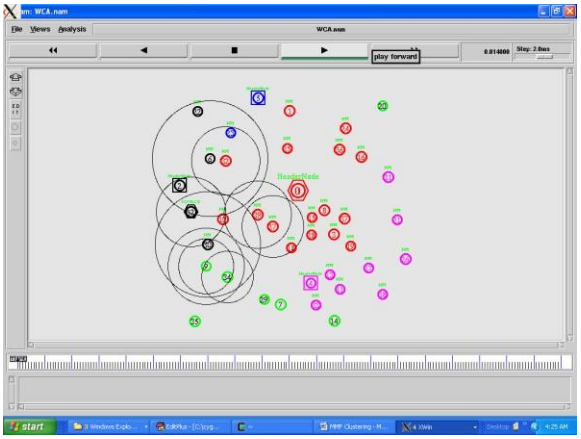
In this paper we have designed WCA existing and propose MMF clustering using NS2 where WCA will select cluster head based on available energy and MMF will select cluster head based on energy and available resources.

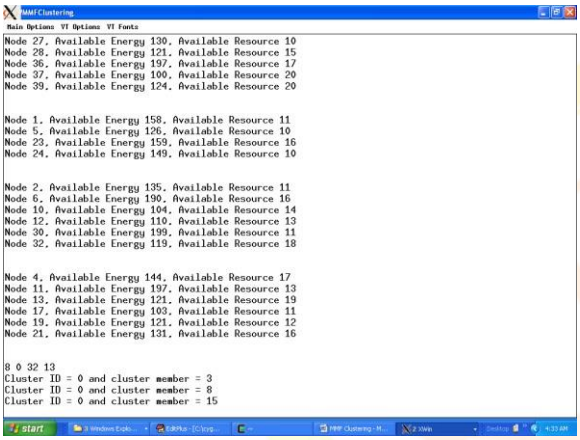




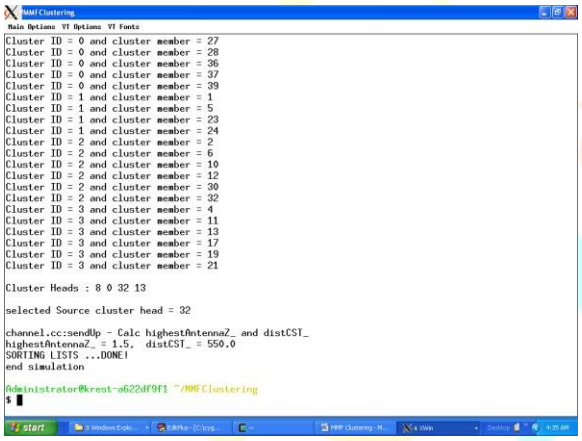
In above screen running WCA technique by using WCA.tcl simulation where 40 is total number of nodes and 12 is the source node.

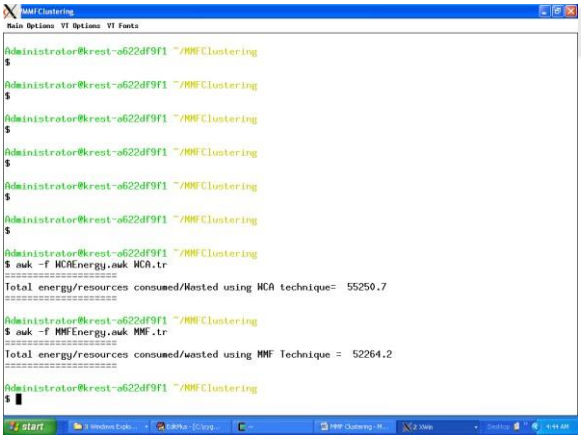
In above screen we can see all 40 nodes are placed at different location and now click on play button to get below page



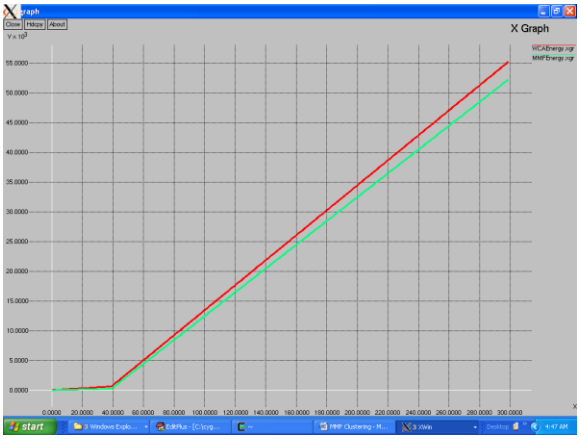


In above screen calculating available energy and resources and based on that MMF will select clusterhead and will get below output





In above screen with propose MMF technique total 52264 joules of energy consumed and now plot energy consumption or resource wastage graph.



In the above graph x-axis represents number of packets send's and y-axis represents energy consumption where red line represents WCA energyconsumption and green line represents MMF energy consumption and we can see in both techniques MMF took less energy consumption andnow close above graph and execute below command to calculate QOS throughput.

VII. CONCLUSION

In this paper we have implemented WCA and MMF clustering algorithms; where WCA performs based on the available energy and MMF performs based onboth energy and resources available. The comparision among both of the techniques stated thatMMF clustering will give us the high throughput i.e.,WCA gave us 1462 KBPS and MMF gave 1653 KBPS throughput. The energy consumption of WCA is high when compared to MMF clustering.

VIII. REFERENCES

[1] M. Van der Schaar *et al.*, "Adaptive Cross- Layer Protection Strategies for Robust Scalable Packet Transmission Over 802.11 WLANs," Dec. 2003.

[2] G. Liebl *et al.*, "Joint Trust management and scheduling for wireless Packet streaming," 2005.

[3] K. Seong-ryong *et al.*, "Multi-layer active queue management and congestion control for scalable Packet streaming," 2004.

[4] J. Novatnack *et al.*, "Evaluating ad hoc routing protocols with respect to quality of service,"2004.

[5] K. Seong-ryong *et al.*, "Multi-layer active queue management and congestion control for scalable Packet streaming," 2004.

[6] M. Ito and Y. Bai, "A packet discard scheme for loss control in ip networks with mpeg Packet traffic," in *Communication Systems-ICCS 2002*, Singapore, 2002, pp. 25-28.

[7] K. K. R. Kambhatla *et al.*, "Prioritized packet fragmentation for H.264 Packet," in *IEEE Int. Conf. on Image Processing*, Orlando, Florida, 2011, pp. 3233-3236.

[8] C. Mbarushimana and A. Shahrabi, "Comparative study of reactive and proactive routing protocol performance in adhoc networks," 21st Int. Conf. Adv. Inform. Networking and Applications Workshops, Ontario, Canada, 2007, pp. 679-684.

[10] J. Novatnack *et al*., "Evaluating ad hoc routing protocols with respect to quality of service," Dept. Compu. Sci., Drexel Univ., Philadelphia, PA. Tech. Rep. DU-CS-04-05. Oct. 2004.

[11] S. Reidt *et al.*, "Resource-constrained signal propagation modeling for tactical ad hoc networks,"in *IEEE Network Science Workshop (NSW)*, West Point, NY, 2011, pp. 22-24.

[12] K. Seong-ryong *et al.*, "Multi-layer active queue management and congestion control for scalable Packet streaming," in *IEEE Proceedings of the 24th International Conference on Distributed Computing Systems*, Tokyo, Japan, 2004, pp. 768- 777.

[13] G. Liebl, H. Jenkac, T. Stockhammer and C. Buchne, "Radio link Trust management and scheduling for wireless Packet streaming," in *Telecommun. Syst.*, vol. 30, no. 1/2/3, pp. 255-258, Nov.2005.

[14] G. Liebl *et al*., "Joint Trust management and scheduling for wireless Packet streaming," in *Proc. 4th International Conf. on Networking*, La Reunion, France, 2005, pp. 882- 891.

[15] D. Tmnenhouse *et al*., "A survey of active networkresearch," *IEEE Communicaotions Magazine*, vol. 35, no.1. pp. 80-86, Jan. 1997.

[16] M. Ito and Y. Bai, "User-Oriented Fair Trust Management for MPEG Packet streams," in *17th Int. Conf. Advanced Networking and Applications*, Xi'an, China, 2003, pp. 241- 247.

[17] M. Van der Schaar *et al*., "Adaptive Cross-LayerProtection Strategies for Robust Scalable Packet Transmission Over 802.11 WLANs," *IEEE Journal on Selected Areas in Communications*, vol. 21, no. 10, pp. 1752-1763, Dec. 2003.

[18] B. Zheng and M. Atiquzzaman, "A Novel Scheme for Streaming Multimedia to Personal Wireless Handheld Devices," in *IEEE Trans. Consum. Electron.*, vol. 49, no. 1, pp. 32-40, Feb. 2003.

[19] T. Wiegand, "Overview of the H.264/AVC Packet coding standard," *IEEE Trans.Circuits Syst. Packet Technol.*, vol. 13, no. 7, pp. 560-576,July.2002.