CHAPTER 2

LITERATURE REVIEW

An ad hoc network is a system of wireless mobile nodes that dynamically self-organize in an arbitrary manner. It allows people and devices to work without any pre-existing communication infrastructure. In mobile ad hoc network, several routing protocols such as Ad hoc On-demand Distance Vector and Dynamic Source Routing can be used.

However, the unreliability of the wireless medium results in frequent communication failures. The high delays occur when the path reestablishment takes place. So a multi-path routing is a very promising alternative to single path routing as it provides higher resilience to path breaks and alleviates network congestion through load balancing and reduces end-to-end delay. Thus the multi-path routing can be highly suitable for multimedia streaming over wireless ad hoc networks. Nonetheless, as security remains an important factor that hinders the rapid deployment of multimedia applications over wireless ad hoc networks, the security issue must be addressed in multi-path multimedia streaming over wireless ad hoc networks.

A few research studies have been done to address the security for multimedia streaming and multipath routing issues in ad hoc networks. Secured multimedia streaming transmission in MANET issues that have been addressed particularly for ad hoc networks include key management, secure routing protocols, handling node misbehavior, preventing traffic analysis and so on.

2.1 MOBILE AD HOC NETWORK COMMUNICATION

In MANETs, packet transmission is impaired by radio link fluctuations. Xiaoqin Chen et al. (2011) introduced an enhanced, channel-aware version of the
AOMDV routing protocol that accommodates channel fading. CA-AOMDV uses the channel average non-fading duration as a routing metric to select stable links for path detection. It uses a preemptive handoff strategy to maintain reliable connections by exploiting channel state information. Using similar information, paths will be reused when they become available again, rather than being not needed. This protocol offers a dual attack for avoiding unnecessary route discoveries. The path failures leading to handoff are forecast. Then it brings paths back into play when they are again accessible, rather than simply discarding them at the first sign of a fade. Additionally, similar information is required to determine ANFD, AFD and forecast path failure for improving efficiency.

### 2.1.1 Mobility Issues in MANET

In mobile ad hoc networks, there are numerous applications in which mobile users can share information, for example, collaborative rescue operations at a disaster site and trade of word-of-mouth information in a shopping mall. For such applications, enhancing data availability is a momentous issue and various studies have been conducted with this intention. Takahiro Hara (2010) quantified the influences of mobility patterns of data availability from different viewpoints. It does not work of single application of protocol but the work proposes and quantifies several metrics that influence data availability.

The Dynamic Source Routing protocol is a simple and well-organized routing protocol designed especially for utilization in multi-hop wireless ad hoc networks of mobile nodes. D. Johnson and D. Maltz (2007) specified the operation of the DSR protocol for routing unicast IPv4 packets. DSR permits the network to be entirely self-organizing and self-configuring, without the requirement for any existing network infrastructure or management. The protocol is self-possessed of the two main mechanisms such as Route detection and Route Maintenance, which work jointly to permit nodes to discover and
maintain routes to random destinations in the ad hoc network. All features of the protocol operate completely by permitting the packet overhead of DSR to scale routinely.

Lyudmila Mihaylova et al. (2011) considered self localization problem of mobile nodes in view of the temporal correlation in the measurement noise. In the considered formulation of the difficulty, node mobility is modelled as a linear system determined through a discrete-time command Markov process, while the measurement models are nonlinear and require a reliable nonlinear estimation method. Because of the fact that the control process of the mobile nodes is unidentified, node mobility is modelled with manifold acceleration modes (regimes). The nonlinear estimation techniques can integrate physical constraints and possibly communications among frequently maneuvering mobile nodes in the form of supplementary measurements.

Uncertainty model defined by Feng Li and Jie Wu (2010) reflects a node’s confidence in terms of sufficiency of its precedent experience, and learns how the compilation of trust information affects uncertainty in nodes’ views. After defining a method to make and compute the uncertainty in trust views, it exploits mobility. A significant characteristic of MANET is that professionally it reduces uncertainty and speeds up trust meeting.

Sungwon Kim et al. (2010) investigated GPS mobility traces of human mobile nodes and monitored super diffusive performance in all GPS traces. It is typified by a faster-than-linear growth rate of the mean square displacement of a mobile node. Using random walk formalism, it examines a large amount of access point-based traces and builds up a theoretical framework. The degree of diffusive behavior of mobile nodes under probably heavy-tailed pause time distribution is measured. It recommended that the diffusive
performance of mobile nodes must be correctly captured and considered for the
design and comparison study of network protocols.

2.1.2 Data transmission in MANET

Data transmission over error-prone mobile ad hoc networks isecoming increasingly important as these networks become more widely
deployed. Yiting Liao and Jerry D. Gibson (2011) introduced a routing-aware
multiple description coding approach to support data transmission over MANETs
with multiple path transport. A statistical model is constructed to estimate the
packet loss probability of each packet transmitted over the network based on the
standard ad-hoc routing messages and network parameters. The frame loss
probability is estimated and dynamically it selects reference frames to alleviate
error propagation caused by the packet losses.

Behnam A. Rezaei et al. (2010) proposed a theoretical framework for
incorporation of random long range routes into wireless ad hoc networking
protocols. Wireless ad hoc routing methods based on this framework and they
deliver the packet successfully. The proposed result is a randomized network
structuring and packet routing framework while distributing the power necessity
almost equally over all nodes. Interestingly, all network formation and routing
algorithms are totally decentralized. The packets arriving at a node are routed
arbitrarily and separately, based only on the source and the destination positions.

The dispersed nature of the algorithm permits it to be implemented
within standard wireless ad hoc communication protocols. It creates the
framework for harnessing collective network resources in really large-scale
wireless ad hoc networking surroundings. Shuhui Yang and Jie Wu (2010)
handled the issues of efficient broadcasting in MANETs using network coding
and directional antennas. By using network coding, the whole number of
transmissions could be reduced compared to broadcasting using similar
forwarding nodes without coding. They developed the usage of directional antennas to network coding-based broadcasting to further decrease energy consumption.

Mobile Ad hoc Networks have been extremely vulnerable to attacks owing to the dynamic nature of the network communications. Among these attacks, routing attacks have acknowledged significant attention since they could cause the most devastating injury to MANET. Ziming Zhao et al. (2012) introduced a risk-aware response method that systematically handles the identified routing attacks. This method is based on an extended Dempster-Shafer mathematical theory of proof by introducing an idea of important metrics (dynamic nature) to identify the different types of attacks.

### 2.1.3 Attacks in MANET

Ad hoc networks use mobile nodes to enable communication outside wireless transmission range. Attacks on ad hoc network routing protocols disrupt network performance and reliability. Y.C. Hu and A. Perrig (2004) reviewed attacks on ad hoc networks and discussed current approaches for establishing cryptographic keys in ad hoc networks. They described the state of research in secure ad hoc routing protocols and also focused on the research challenges.

Communication is attained by relaying data along appropriate routes that are dynamically discovered and maintained via collaboration between the nodes. Detection of such routes is a main task, both from efficiency and security points of view. Burmester M. and De Medeiros B. (2009) demonstrated that the security evidence for the route discovery algorithm endairA is flawed and furthermore, this algorithm is vulnerable to a concealed channel attack.
In 802.11-based Wireless LAN, there is an enhanced risk of security attacks. To overcome concealed attacks, there is a requirement to authenticate both access points and wireless stations. Moorthy M. et al. (2012) proposed a defensive technique for Distributed Denial of Service attack in WLAN. This authentication method includes an Authentication Server (AS) in addition to the Wireless Station (WS) and Access Point (AP). The authentication server comprises both normal and attacker databases. The attacker database can be built from the outcome of fuzzy decision making.

**Routing attacks**

Mobile Ad hoc Networks have been extremely vulnerable to attacks because of the dynamic nature of its network infrastructure. With these attacks, routing attacks have received significant attention since they could cause the most devastating damage to MANET. Although there exist several intrusions response methods to mitigate such critical attacks, existing solutions classically attempt to isolate malicious nodes based on binary or naive fuzzy response decisions. In fact, binary responses might result in the unexpected network separation, causing further damage to the network communications. Fuzzy responses could guide to uncertainty in countering routing attacks in MANET.

Mobile ad hoc networks are dynamic mobile networks that might be built in the non attendance of any pre-existing communication infrastructure. MANETs are susceptible to jamming attack because of their salient characteristics. The purpose of a jammer is to hinder with legitimate wireless communications, and to humiliate on the whole, QoS of the network. Ben Othman J. and Hamieh A. (2009) proposed a new technique to respond to jamming attacks. The armed forces have long dealt with jamming with the help of frequency-hopping spread spectrum communication.
Chen, Siguang and Wu Meng (2011) proposed an anonymous multipath routing protocol based on secret sharing. The protocol offers location anonymity, identity anonymity, data and traffic anonymity by using cryptograph technology and secret sharing in MANET communication procedure. In the meantime, a hash function is introduced to notice active attacks in the data transmission process. The protocol can efficiently thwart various passive attacks and reduce the victorious probability of active attacks such as interception and physical destroy attacks.

2.1.4 Secure Wireless Ad Hoc Routing

Routing is one of the most essential networking functions in mobile ad hoc networks. Therefore, an adversary can simply paralyze the process of the network by attacking the routing protocol. This has been understood by many researchers and numerous secure routing protocols have been planned for ad hoc networks though the security of those protocols has been mostly analyzed by unofficial means only. G. Acs et al. (2006) disputed that the flaws in ad hoc routing protocols can be very tedious. The author suggested a mathematical framework to define the security and provided security mechanism using routing protocols for mobile ad hoc networks.

Stephen Dabideen J. J. and Garcia Luna Aceves (2012) presented an approach, namely Secure Time-Ordered routing Protocol for secure routing in mobile ad hoc networks, based solely on the relative transmission times of overhead packets. Contrasting most previous works aimed at securing route computation, STOP eliminates a key vulnerability (explicitly stated routing metrics) on the whole. It uses time-based orderings to ensure the establishment of multiple loop-free paths between a source and a destination. STOP is the primary routing protocol that employs performance-based path choice without source routing, path vectors, or total topology information. Adversaries cannot obtain
any action to manipulate the time-based ordering so as to unfairly gain control of the forwarding topology through design and avoid dropping data packets by the nodes.

Buttya L. and Vajda I. (2004) suggested a formal framework for the security analysis of on-demand source routing protocols for wireless ad hoc networks. The method is based on the well-known simulation model that has been proposed to confirm the security of cryptographic protocols. The major role is the application of the simulation-based approach in the situation of ad hoc routing. This engages a specific definition of a real-world model, which explains the actual operation of the protocol and an ideal-world model. It captures what the protocol needs to achieve in terms of security. Together, the models keep in view the peculiarities of wireless communications and ad hoc routing. They exhibit the usefulness of the approach by analyzing two secure ad hoc routing protocols such as SRP and Ariadne.

Mobile ad hoc networks pose new kinds of security troubles, caused by their nature of collaborative, open systems and by limited availability of resources. Cerri D. and Ghioni A. (2008) considered a Wi-Fi connectivity data link layer as a basis and focused on routing protection. The performance of the secure AODV protocol extension includes tuning strategies aimed at improving its performance. Authors suggested an adaptive mechanism that tunes SAODV behavior.

The nature of static infrastructure causes several concerns in mobile ad hoc network, such as power utilization, node authentication and secure routing. Himadri Nath Saha et al. (2012) designed a scheme for power efficient secure routing of data packets in MANET. This technique reduced the computational overhead to make it more energy efficient. As there is no stationary infrastructure, every node in MANET acts as a router that forwards
data packets to other nodes. Consequently, the selection of effective, appropriate, robust and adaptive routing scheme is of utmost significance. Such a selection has reduced the amount of network activity for each node required to route a data packet.

In contrast to earlier studies that sought only the shortest route, a trusted route is needed that considers communication reliability, path length for a reliable and possible packet delivery in a MANET. In the majority MANET routing systems, security is an additional layer above the routing layer. Jian Wang et al. (2011) mooted the concept of attribute similarity in finding potentially friendly nodes among strangers. Consequently, security is inherently integrated into the routing protocol where nodes evaluate the trust levels of others based on a set of attributes. The fixed probability of dropping packets adopted in other routing methods is designed based on the attribute similarity. It gives a recommended method in calculating the degree of similarity between attributes.

Several routing protocols have been proposed in recent years for the probable deployment of MANETs in armed forces, government and commercial applications. Abusalah L. et al. (2008) estimated routing protocols with a particular focus on security features. The protocols vary in terms of routing methodologies and the information used to create routing decisions. Four delegate routing protocols have been selected for analysis and evaluation together with Ad hoc On-demand Distance Vector routing, Dynamic Source Routing, Optimized Link State Routing and Temporally Ordered Routing Algorithm.

2.2 MULTIMEDIA STREAMING TRANSMISSION IN MANET

At present, most embedded systems support dissimilar kinds of multimedia applications and real-time tasks. The computational necessities of multimedia applications are typically very demanding and embedded systems may not be powerful and sufficient to support multiple multimedia applications.
Consequently, real-time tasks will overlook their deadlines and thus get rejected. Kai Jung Shih et al. (2009) developed a Dynamic Workload Shaping technique by extending a Dynamic Buffering Technique for multiple multimedia tasks and endorsed two optimization techniques (Dynamic Workload Shaping and Dynamic Buffering technique). DBT scheduling method guarantees that the playout devices are forever able to read out data items from the playout buffers. Hence, two algorithms DWS and DBT are proposed to optimize the quality of multimedia applications and to guarantee the QoS.

### 2.2.1 Protocols for Multimedia Streaming

Jinsuk Baek et al. (2010) worked out a video multicast protocol for multi-homed mobile terminals as a substitute Stream Control Transmission Protocol for moderately reliable multicast services. It performs with overlay peer-to-peer video multicast facility in the application layer. In support of a multi-homed mobile terminal, an error burst might occur when a handover is in process in the main path switching process. The key problem concerned in this protocol is the ability to forecast packet drop. If the packet is misplaced, it retransmits the misplaced packets as soon as a mobile terminal performs switching process.

Yuanguo Bi et al. (2009) suggested a multi-channel token ring Media Access Control protocol for Inter-Vehicle Communications. During adaptive ring coordination and channel scheduling, vehicles are separately organized into multiple rings operating on dissimilar service channels. Based on the multi-channel ring arrangement, emergency messages will be disseminated with a low delay. By the token based data exchange protocol, the network throughput is further enhanced for non-safety multimedia applications. The methodical model is developed to assess the performance of MCTR in terms of the average full ring delay, emergency message delay, and ring throughput.
Efficiently deal with arbitrary malicious disruption of data transmissions, Papadimitratos P. and Haas Z. J (2006) posited a Secure Message Transmission Protocol and its alternative Secure Single Path protocol. SMT and SSP robustly notice transmission failures and continuously configure their operation to evade, endure data loss, and make sure the availability of communication. This is attained at the expense of moderate transmission and routing overhead, which will be traded off for delay. In general, the capability of the protocols to mitigate both malicious and benign faults permits fast and reliable data transport even in highly adverse network environments.

T. Bheemarjuna Reddy et al. (2006) presented MuSeQoR: a new multi-path routing protocol that undertakes the look-alike issues of reliability (protection against failures of multiple paths) and security, while ensuring smallest amount of data redundancy. Authors also specified the security of the protocol in terms of the number of eavesdropping nodes. The reliability and security requirements are specified by a user and are connected to the parameters of the protocol adaptively.

A success likelihood function is related to every link, which could be controlled by power and rate allocation. The appearance for the network's stability region is primarily derived where the success function plays a serious role. Giovanidis A. and Stanczak S. (2011) considered functions with exact properties which are shown to be satisfied for different expressions of the success probability, related to dissimilar modulation and coding schemes as well as outage measures. A Network Utility Maximization problem with stability constraints is additionally formulated which decays into the input rate control and scheduling the power allocation. Beneath the convinced assumptions, the latter is relaxed to a simpler form. This allows the application of super modular game theory and the algorithmic approach is adapted to include the family of success functions of interest.
2.2.2 Multimedia Streaming Transmission in MANET

Cluster-based routes assist data transmission by acting as backbone paths in wireless ad hoc networks. A number of mobile users form a cluster to attain common multimedia services and node mobility does not assure multimedia transmission in a network with an active topology. Yueh Min Huang et al. (2007) first attempted a novel measure of cluster-based route’s stability, consistent with a prediction of connection probability at a particular time in future. It helped to broadcast multimedia streams across many clusters in a network. The chosen route is sufficiently stable to facilitate cluster-based mobile users to receive time-consuming multimedia streaming in prospect. Secondly, inter-cluster connectivity preservation schemes, together with forward and backward connectivity methods to defend non-stop multimedia streams, are established to maintain inter-cluster links.

Current advances in forward error correction and scalable video coding enable novel methods for robust, distributed streaming in Mobile Ad Hoc Networks. T. Schierla et al. (2008) offered an approach for distribution of real time video through uncoordinated peer-to-peer relay or source nodes in an overlay network on top of a MANET. This approach permits for dispersed, rate-distortion optimized transmission-rate allowance for competing scalable video streams at relay nodes in the overlay network. The method has the desirable feature of path/source diversity that will be used for enhancing reliability in connectivity to help nodes and/or attain an advanced throughput.

Skype is past any doubt the VoIP application in the present Internet application spectrum. Its wonderful success has drawn the attention of telecom operators and the investigation community, both interested in knowing its internal methods, characterizing its traffic and understanding its users' behavior. Bonfiglio D. et al. (2009) examined the characteristics of traffic streams
produced by voice, video interactions, and signal traffic produced by Skype. The method is twofold; utilizing both active and passive measurement techniques to collect a deep understanding of the traffic Skype creates extensive passive parameters collected from different dataset. They developed a source model which takes into the account of: (i) the service type (specifically, Skype Out calls or calls between two Skype clients) (ii) the chosen source node (iii) the accepted transport layer protocol, and (iv) network situation. Leveraging on the exploitation of an accurate Skype classification engine, Skype traffic is characterized based on extensive and passive measurements composed from campus LAN.

2.2.3 Multimedia Streaming

Venkatarama M. and Chatterjee M. (2012) undertook a trace-driven study to understand Quality-of-Experience capabilities of present-day Internet links using 51 diverse ISPs with a major presence in the US, Europe, and Asia-Pacific. They examined the links from 38 vantage points in the Internet using both passive tracing and active probing for six days. The links provided the first measurements of link-level degradations and case studies of intra-ISP and inter-ISP peering links from a multimedia standpoint. The proposed study offers surprising insights into intra-domain traffic engineering, peering link loading, BGP, and the inefficiencies of using autonomous system path lengths as a routing metric.

Hsien Po Shiang and Van der Schaar M. (2012) pioneered a quality-centric congestion control for multimedia streaming over wired IP networks, which are referred to as Media-TCP-friendly Congestion Control. The proposed solution adapts the sending rate to both the network condition and the application characteristics by explicitly considering the distortion impact, delay deadlines. The media-aware solution is able to provide differential services for
transmitting various packet classes and thereby, further improves the multimedia streaming quality compared to the conventional network-aware congestion control.

The dynamic characteristics of wireless networks and stringent QoS requirements of multimedia applications have identified significant challenges for providing QoS guarantees for real-time multimedia streaming in such wireless environment. QoS routing protocols can decisively contribute to the QoS provision of network systems. Jinjing Tao et al. (2011) deployed an Efficient Cluster-Based Routing Protocol for real-time multimedia streaming in mobile ad hoc networks. This mechanism contributes to reduce route overhead, and to increase the decodable ratio of video frame at the application layer as well.

2.3 MULTI-PATH STREAMING OF MULTIMEDIA TRANSMISSION OVER MANET

Mobile ad hoc networks without central infrastructure transform their topology rapidly because of node speed, making multimedia applications intricate to run across wireless networks. Furthermore, video transmission over ad hoc networks initiates frequent transmission loss of video packets owing to end-to-end transmission with a number of wireless links. It needs necessary bandwidth and restricted delay to offer quality-guaranteed display. Meng Yen Hsieh et al. (2007) hit upon an architecture supporting transmission of numerous video streams in ad hoc networks by establishing multiple routing paths to offer extra video coding and transport schemes. This analysis also proposed an on-demand multicast routing protocol to transfer layered video streams. Multicast routing protocol broadcasts layered video streaming based on a weight measure, which is derived consistent with the number of receivers, delay and termination time of a route.
The number of moveable electronic devices competent enough for maintaining wireless interactions increases little by little. Such mobile nodes might easily self-configure to structure a mobile ad hoc network without using any established infrastructure. Because the number of mobile devices grows, the requirement of multimedia services such as video-streaming from these networks is foreseen to augment too. M. Aguilar Igartua et al. (2012) came up with a proposal which seeks to progress the experience of the end users in such surroundings. A cross-layer multipath routing protocol includes techniques to attain a dynamic assignment of the Contention Window of the IEEE 802.11e MAC level.

2.3.1 Path selection in mobile ad hoc networks

Bouk S.H et al. (2012) suggested a gateway selection scheme that considered multiple QoS path parameters for instance path availability period, available capacity and latency, to choose a potential gateway node. It progresses the path accessibility computation accuracy and introduces a feedback system to updated path dynamics to the traffic source node. Then an efficient method to propagate QoS parameters is suggested in the proposed scheme. Gateway selection scheme improves throughput and packet delivery ratio with less per node power utilization. It also develops the end-to-end delay compared to single QoS path parameter gateway selection schemes. Additionally, by considering weighting factors to gateway selection parameters, the weighting factors develop the throughput and end-to-end delay compared to the conventional schemes.

In mobile ad hoc networks, hierarchical architecture and distributed approaches are more realistic than flat architecture and central approaches. El Hajj W. et al. (2009) proposed a group of protocols that achieved a distributed planning and routing scheme for MANETs. The planned suite, which is composed of three protocols, presents scalability and extends network lifetime.
The primary protocol, specifically, the Fast Distributed linked Dominating Set, builds the virtual backbone by designing a quick distributed hierarchical algorithm that finds a linked dominating set in the network graph. The built virtual backbone takes into account the node's limited energy, mobility, and traffic pattern. The subsequent protocol FDDS-M, suggests a distributed maintenance protocol that conserves the integrity of the hierarchical structure constructed by FDDS.

**Reliable and Stable path selection**

MANET is a compilation of wireless mobile computers forming a temporary network without any fixed infrastructure or wired backbone. Topological alterations in MANET frequently render routing paths not viable. An appropriate technique for addressing this problem is to improve the diversity of paths between the source and destination. Nevertheless, multipath routing is a demanding task. Specifically, the correlation between the failures of the paths in a path set must be as small as possible. Common nodes and links between the paths are usually failure points. Rambling path sets need the multiple paths to be link-disjoint or node-disjoint though selecting an optimal path set is an NP-complete difficulty. Artificial neural networks have been proposed as computational tools to resolve constrained optimization troubles. The utilization of Hopfield neural network as a path set choice algorithm is explored. While this algorithm produces a set of backup paths with much privileged reliability, it is helpful for MANETs. Sheikhan M. and Hemmati E. (2011) used link expiration time between two nodes to estimate link reliability. In this method, node-disjoint and link-disjoint path sets will be found concurrently with route discovery algorithm. Consequently, if someone wants to discover both node-disjoint and link-disjoint path sets, there is no need to submit extra control messages, like overhead, to the MANET.
Cooperative communications can considerably improve transmission reliability and bandwidth effectiveness in wireless networks though many upper layer aspects of cooperative communications give value for further investigation. Quansheng Guan et al. (2011) investigated its impacts on network topology and network capability, which is determined by large aspects such as physical layer ability, interference and path extent. This is because cooperative communications improve physical layer capacity and relay selection impacts on network topology. Authors suggested a Capacity-Optimized Cooperative topology control scheme for mobile ad hoc networks with cooperative communications. COCO topology considered both upper layer network capacity and physical layer relay selections in the proposed scheme. Additionally, only the channel estimate, not the ideal channel status, is unspecified to be known in this system.

MANET offers a resource constrained dynamic environment and initiates new aspects to dependability thus affecting reliability of the services provided by the Mobile Agent based System organized in MANET. MAS on MANET can be more reliable if the agents are need to share information and learn (reinforcement learning) about the fundamental MANET conditions animatedly. Chowdhury C. and Neogy S. (2011) estimated reliability of learning based agents. The MAS consists of independent agent groups comprising of some application which are well organized.

A basic issue arising in mobile ad hoc networks is the collection of the optimal path between any two nodes. A technique that has been advocated to progress routing efficiency and to choose the most stable path so as to decrease the latency and the overhead because of route reconstruction. Carofiglio G. et al. (2009) studied both the availability and the duration likelihood of a routing path that is subject to link failures initiated by node mobility. Especially, they focused on the case where the network nodes move consistent with the random direction model and obtained both exact and approximate (but simple) expressions of these
probabilities. The work on random way walk model as proposed by Min Qin et al. (2006) assumes that all nodes speed and directions are uniformly distributed. At last, they proposed an approach to progress the efficiency of reactive routing protocols and examined the problem of selecting an optimal route in terms of path accessibility.

2.3.2 Multipath routing in wireless ad hoc networks

Multipath routing is effectual in wireless ad hoc networks, because connectivity along multiple paths is less likely to be broken. Wei W. and Zakhor A. (2004) suggested a multipath extension to dynamic source routing to hold multipath video communication over wireless ad hoc networks. The suggested scheme is compared with others for interactive video applications. MANETs comprise a collection of wireless mobile nodes which dynamically trade data among themselves without the reliance on an unchanging base station or a wired backbone system. MANET nodes are classically distinguished by their restricted power, processing and memory resources with a high degree of node mobility. Therefore, routing is a critical issue to the design of a MANET.

Mueller S. et al. (2004) specifically examined the issues of multipath routing in MANETs. Multipath routing allows the organization of multiple paths between a single source and single destination node. It is classically proposed in order to enlarge the reliability of data transmission (i. e. fault tolerance) or to offer load balancing in which load balancing is of special significance in MANETs because of the limited bandwidth between the nodes. The application of multipath routing supports application constraints, for example, reliability, load-balancing, power-conservation and Quality-of-Service whereas security is difficult to be achieved. Roy et al. (2012) discussed the security vulnerabilities related to data aggregation systems, presenting a survey of complex and secure aggregation protocols that are compromised due to false data injection attacks.
A mobile ad hoc network is an active wireless network that can be created without the need for any pre-existing infrastructure in which each node can perform as a router. Since mobile nodes have limited battery power, it is consequently very important to use energy in a MANET professionally. Baolin Sun et al. (2010) provided energy Entropy Multipath Routing optimization algorithm in MANET based on GA. The key thought of the protocol is to discover the minimal node residual energy of each route in the procedure of selecting the path by descending node residual power. It will balance individual node’s battery power exploitation and therefore prolong the entire network’s lifetime and power variance.

Because of bandwidth constraint and dynamic topology of mobile ad hoc networks, multipath supported routing is a very significant research issue. Baolin Sun et al. (2012) marshaled a Network Coding-based on-demand Multipath Routing algorithm in MANET. NCMR is typically proposed in order to enhance the reliability of data transmission or to offer load balancing.

Obaidat M. et al. (2011) scheduled a novel multipath routing protocol for MANETs. The protocol is an alternative of the single path AODV routing protocol. The multipath routing protocol found node-disjoint paths that have the buck delays based on the interaction of many factors from dissimilar layers. Further delay aware MANETs routing protocols not consider the projected involvement of the source node that is requesting a path into the whole network load. The suggestion is that end-to-end delay acquired through the RREQ is not precise any more. In contrast to its predecessors, the proposed protocol keeps in focus the projected contribution of the source node into the calculation of end-to-end delay.

The rapid growth in mobile devices and wireless networking has provided the technical platform for video streaming over mobile ad hoc
networks. Though efforts to understand the concept related to video streaming over MANETs are complex, they have been addressed by different authors using different techniques. Examples comprise cross-layer optimization, packet scheduling, caching and replication. Cross-layer optimization classically leverages multiple description video coding and multipath routing to offer the receiver(s) enough video eminence. Caching and replication insert tolerance to disruptions and partitioning. Morten Lindeberg et al. (2011) recognized the challenges of video streaming over MANETs. As a result of 65% engage cross-layering model, the distribution of joint optimization and parameter exchanges are learned.

2.3.3 Multimedia applications over video transmission

Without needing multicast support from the fundamental networks, overlay multicast has the benefit of implementing inter-domain multimedia multicast communications. Typically, overlay multicast protocols use two different topologies: r-ary tree and m-D mesh(based on tree topology and mesh topology). Wanqing Tu et al. (2009) studied the influence of topology assortment on multimedia multicast performance. They presented a set of theoretical results on the worst presentation, the average presentation, the presentation difference along the link pressure, the number of overlie hops, and the number of shortest paths for r-ary tree-based and m-d mesh-based multicast, correspondingly. In addition, evaluations and insights into these two types of multicast used to transmit multimedia streams. The selection of overlay topology is application dependent.

In deepness image-based 3-D video transmission, the compressed video stream is extremely likely to be tarnished by channel errors. Because of the high compression ratio of H.264/AVC, it is frequently common to see that a whole coded picture is grouped into one packet. Therefore, the loss of a packet
may result in the loss of the entire video frame. At present, most of the frame suppression methods are mostly for 2-D video broadcast. Yan B. and Zhou J. (2012) have proposed a well-organized frame concealment algorithm for depth image-based 3-D video broadcast, which is able to offer accurate estimation for the motion vectors of the lost frame with the help of the depth information.

Scalable video transmission over a network is easily flexible to different types of mobile experiencing different network circumstances. Yet, the broadcast of differentiated video packets in an error-prone wireless environment remains difficult. Kyungtae Kang and Jeon W. J (2012) examined a cross-layer error control system that exploits Priority-aware Block Interleaving in the MAC layer for video broadcasting in CDMA2000 systems. The PBI system allocates a higher priority to shielding the data which are more dangerous to the decoding of a video stream and consequently it has more effect on picture quality in the application layer. The purpose of Reed-Solomon coding in conjunction with PBI in MAC layer is that it can handle error bursts if its implementation takes account of basic error distribution in physical layer. This is turn differentiates between different types of video packets in the application layer.

Wireless mesh networking is an efficient wireless technology for future broadband Internet retrieve. Ping Wang and Weihua Zhuang (2009) enumerated a collision-free medium access control scheme supporting multimedia applications for wireless mesh backbone. The proposed method is distributed, trouble-free, and scalable. Gaining from the permanent locations of wireless routers, the proposed MAC scheme reduces the control overhead greatly, compared with the usual contention-based MAC schemes (e.g IEEE 802.11). Moreover, the proposed scheme can offer guaranteed priority access to real-time traffic and simultaneously, can make sure fair channel access to the routers with data traffic. Nothing like most of the existing MAC schemes which concentrate on single-hop transmissions, the proposed MAC scheme gets the
intra-flow correlations between up-stream and downstream hops of a multi-hop flow into concern. To evade buffer overflow at bottleneck routers, a simple however effective congestion control mechanism is proposed.

Michele Nitti and Luigi Atzori (2012) considered the scenario of a Multi-Homed Hybrid Ad Hoc Network. It consists of self-organized and self-configured mobile nodes that utilize two or more fixed gateways attached to the Internet. Consequently, different network segments are created, each one connected with a different gateway. A node can keep its connectivity to the Internet when moving from a network to the other by performing handover procedures and altering its gateway to the Internet. This situation is somewhat interesting for its capacity of increasing the geographical addition of a single mobile network. Inside this scenario they concentrate on the modelling of the node connectivity. It is of practical interest for the model of rate control algorithms for multimedia streaming systems. Author considered a network structure with gateways placed in a honey cell structure. The nodes move consistent with the Random Direction Mobility Model. The possibility of a node changing the route from a network to another, leads to service interruptions which highly affects the quality, during multimedia streaming.

The quality of experience enhancement for a transmitted video sequence in MANETs is a demanding and significant issue in the networking research community. Inherent high levels of packet error probability in MANETs can cause high levels of distortion based on the location of packet loss in transmitted frames. Therefore, the exact modelling of the impact of packet loss on video quality and the resultant distortion are an important task. Many traditional distortion modelling techniques merely considered a linear relationship between the packet loss and deformation, which is imprecise. P. Goudarzi et al. (2012) developed an accurate model which could imprison the exact effect of network packet loss on video eminence performance (and hence
on the QoE) with group of picture-level granularity. Subsequently, based on this model, an optimal bandwidth allocation policy is developed in MANETs, with which, based on some network-specific restraints, the loss-induced distortion associated with a video source is minimized, using some cross-layer design methods.

Video recording in Internet Protocol TeleVision systems is a capable service that provides time-shifted services in relation to storing TV content closer to user devices(e. g. set-top boxes). The existing methods do not maintain collaboration between nodes which have connected contents, a fact that can affect the performance of the overall system. To create this service as more interactive and proactive, Seung Bum Lee et al. (2009) presented an architecture using the Smart Personal Information Network (Smart PIN) as a novel performance-based content allocation network for IPTV content. It uses a user-centric utility-based multimedia data replication scheme. The exchange of data is based on both network performance and user interests towards exchanged multimedia content to attain efficient content sharing.

2.3.4 Reliable Multi-path Multimedia Streaming

The growing accessibility of IP based heterogeneous wireless access technologies being joined with the increasing capabilities of mobile devices is creating opportunities for multimedia sharing. Through its multi-homing characteristic, the ability to maintain multiple network connections in a single end to end connection, the transport layer Stream Control Transmission Protocol can facilitate seamless and clear communication sessions over multiple heterogeneous networks. Changqiao Xu et al. (2011) analyzed the performance of multimedia distribution when utilizing two multi-homing SCTP-based approaches. They are Single path transfer and Concurrent multi-path transfer, in which a solitary or all paths within an association are used concurrently for data
broadcast. In this study, various retransmission policies and dissimilar parameter sets are used in turn and suggestions are made for achieving the best results during video delivery.

Providing VCR-like operations in peer-to-peer (P2P) environments is an important challenge. Changqiao Xu et al. (2009) proposed a distributed storage-assisted data-driven overlay network to hold P2P video-on-demand services. It put together two networks: a Data-driven Overlay Network (DONet) and a multi-way tree. DONet is improved and used for the routine video distribution based on the defense overlapping mechanism and gossip protocol. The algorithm uses a multi-way tree arrangement and extra pre-fetching buffers at the nodes are proposed to maintain efficient VoD process. Videos are separated into uniform sections, pre-fetched and stored in a distributed way along the tree topology. The assistance between DONet-based video delivery and the tree-located multimedia components enable multimedia streaming interactive commands to be performed efficiently. Changqiao Xu et al. (2009) presented and discussed the structure of SDNet and the distributed storage scheme, detailing the cooperation procedure.

The performance of wireless networks beneath video traffic is subjected to two main concerns: power minimization and other QoS requirements, for example, delay jitter. MANETs are more responsive to these issues where each mobile device acts like a router. Therefore, routing delay adds considerably to overall end-to-end delay. Tarek R. et al. (2011) examined the performance of the Warning Energy Aware Cluster head/Virtual Base Station-On demand protocol in terms of delay, multi-hop interaction and power minimization aspects that are the main issues in video transfer. In this connection, H.263 and H.264 standards are used to model the simulated system. HCB model is also used to reduce the power utilization. Single hop and
multi-hop settings include the power consumption and the effect of sudden
demise of cluster heads in the Warning Energy Aware Cluster head protocol.

Current years have witnessed a rapid increase in video applications
over wireless networks including on-demand video streaming and video phonig.
This enlargement has also brought out need to find good cooperation in the
disagreement between resource limitations affecting mobile devices and the wish
for high-quality multimedia services. It is probable to face this problem adopting
a cross-layer approach that together tunes the parameters of every layer in the
network protocol load. In this optimization approach, complexity is one of the
most important issues owing to the limited computational resources and power
supply. Milan S. and Calvagno G. (2009) presented a low-complexity cross-layer
algorithm that is able to tune together the parameters of different protocol layers
by adopting simple, yet effectual models. The eminence of the reconstructed
video series, the formed bit rate, and the service class connected to each packet
are seen as functions of the proportion of null DCT coefficients. This model
allows finding a closed-form solution to the joint optimization problem that will
be computed with a restricted number of operations and grants. Simultaneously,
it leads to a good visual quality in the rebuilt sequence.

Greco C. et al. (2012) addressed, confront of delivering a video
stream, encoded with multiple descriptions, in a mobile ad-hoc environment with
low-latency constraints. This type of application is meant to offer an efficient and
reliable video communication tool in scenarios where the deployment of an
infrastructure is not possible, such as military and disaster relief applications.
Initially, presented a recently proposed protocol (cross-layer congestion control
protocol) that employs a reliable form of one-hop transmits to construct an
efficient overlay network. It is consistent with a multi-objective function that
minimizes the number of packets injected in the network and exploits the path
diversity among descriptions. Cross-layer congestion control strategy where the
MAC layer is aware of video-coding adjusts its transmission parameter (the RTS retry limit) using congestion/distortion optimization. The most important challenge in this approach is providing a reliable assessment of congestion and distortion. It specified the limited information available at every node.

Magnetto A. et al. (2010) presented TURINstream, a novel P2P video streaming architecture designed to mutually achieve low delay, robustness to peer churning, restricted protocol overhead, and quality-of-service differentiation based on peers collaboration. Split control and video overlays are maintained by peers organized in clusters that represent sets of collaborating peers. Clusters are formed by means of a distributed algorithm and allow the exploitation of the participant node’s upload capability. The video is conveyed with a push mechanism by exploiting the advantages of multiple description coding. TURINstream intend has been optimized through an event driven overlay simulator capable of scaling up to tens of thousands of peers. An entire prototype of TURINstream has been established, organized, and tested on PlanetLab. They tested prototype beneath changeable degree of peer churn, flash crowd arrivals, unexpected massive departures, and restricted upload bandwidth possessions. TURINstream fulfills primary design goals, showing low average association, startup, and playback delays, high permanence index, low control overhead, and effective quality-of-service differentiation in all the tested scenarios.

Mansour H. et al. (2009) addressed the problem of capably allocating network resources to hold multiple scalable video streams above a controlled wireless channel. The resource allocation framework jointly optimizes the operation of the link adaptation scheme in the physical layer, and that of a traffic control module in the network or medium access control layer in multirate wireless networks, while fulfilling bandwidth/capacity constraints. Multirate networks, such as IEEE 802.16 or IEEE 802.11, regulate the PHY coding and modulation schemes to preserve the reliability of transmission beneath varying
channel conditions. Privileged reliability is achieved at the cost of reduced PHY bit-rate which in turn necessitates a decrease in video stream bit-rates. The rate decrease for scalable video is implemented using a traffic control module. Traditional solutions function unaware of the importance and loss acceptance of data and drop the higher layers of scalable video in total. Medium grain scalable is expansion of H.264/AVC video and builds up new rate and distortion models that characterize the coded bit stream.

2.3.5 Adaptive cross-layer schemes for multimedia delivery

A holistic approach must be made for a wider adoption of a cross-layer method. A cross-layer design on a wireless network assumed with a convinced network condition, for example, can have limited usage in heterogeneous situations with diverse access network technologies and time varying network performance. The primary step toward a cross-layer approach is routine detection of the underlying access network type, so that appropriate schemes can be applied without manual configurations. To tackle the issue, Baek Young Choi et al. (2009) examined the characteristics of round-trip time on wireless and wired networks. RTT variability on a wireless network exhibits really larger mean, standard deviation, and min-to-high percentiles as a minimum 10 ms, bigger than those of wired networks due to the MAC layer retransmissions. The crash of packet size on wireless channel is particularly important. Therefore, through a simple set of testing, one can precisely categorize whether or not there has been a wireless network concerned. An adaptive cross-layer scheme for multimedia delivery over error-prone links is planned.

Byung Joon Oh and Chang Wen Chen (2009) presented a cross-layer design for a reliable video broadcast over wireless ad hoc networks based on multichannel MAC protocol with TDMA. Initially, a study was conducted with multichannel MAC protocol using Markov chain model. Based on this analysis,
two novel cross-layer modules are adopted for the design of multichannel MAC protocol. Foremost, it adopts maximum latency rate as the channel quality metric. Contrasting the traditional MAC design based on network allocation vector, MLR is implemented to offer differentiated traffic. Consequently, that the channel with lesser MLR time is initiated for higher priority traffic. Subsequently, two congestion-aware metrics, namely MAC utilization and queue length of MAC layer, was adopted to progress the congestion-aware routing protocols with AODV and DSR.

GyeongCheol Lee and Hwangjun Son (2010) suggested an efficient cross layer optimized video streaming algorithm above multi-hop mobile ad hoc networks. The proposed method chooses the most efficient physical mode and retransmission limit of WLAN multi-rate service at each node in a distributed method. The control parameters of the proposed algorithm (i.e. PHY mode and retransmission limit) are decided based on the available information during application MAC, and physical layers in order to convince the end-to-end delay constraint and maintain packet loss rate in the acceptable range at the receiver.

2.3.6 Security Mechanism in Mobile ad hoc Network

Friend based ad hoc routing using challenges to establish security is an algorithm that offers secure routing in ad hoc mobile networks. Dhurandher S.K et al. (2011) proposed this scheme that has been drawn from a network of friends in real life situations. The algorithm works by sending challenges and sharing friend lists to offer a list of trusted nodes to the source node through which data broadcast lastly takes place. The nodes in the friend list are esteemed on the basis of the amount of data broadcast they accomplish and their friendship with other nodes in the network. The report of friendship of a node with other nodes in the network is obtained through the Share Your Friends process which is a periodic event in the network. As a consequence of this
scheme of operation, the network is able to efficiently isolate the malicious nodes which are left with no role to play in the ad hoc network.

Continuous user authentication is a significant prevention-based approach to protect high security mobile ad-hoc networks. In contrast, intrusion detection systems are also significant in MANETs to effectively identify malicious behavior. To acquire the optimal scheme of combining continuous user authentication and IDSs in a distributed way, Shengrong Bu et al. (2011) formulated the problem as a partially observable Markov decision process multi-armed bandit difficulty. Structural results technique solves the problem for a large network with a range of nodes.

**Link-state based routing security**

In most of the general mobile ad hoc networking scenarios, nodes begin communication based on long-lasting public identities. In some hostile and suspicious settings, node identities should not be exposed and node movements must be untraceable. As a substitute, nodes need to communicate on the basis of their current position. While such MANET settings are not very common, they do happen in military and law enforcement domains and need high security and privacy guarantees. El Defrawy K. and Tsudik G. (2011) addressed a number of concerns arising in suspicious location-based MANET settings by designing and examining a privacy-preserving and secure link-state based routing protocol. ALARM employs nodes' present locations to securely distribute and construct topology snapshots and forward data.
2.4 RESEARCH GAP

Mobile ad hoc networks have established their efficiency in the deployment for number of fields, but they are highly vulnerable to security attacks. The co-operative nature of ad hoc protocols makes it more vulnerable to impersonation, data tampering, and denial of services.

The lack of a fixed infrastructure restricts the applicability of some conventional security solutions, for example, a Public Key Infrastructure. It relies on a centralized trusted authority, and the intrusion detection system, which requires a concentration point to gather audit data.

The limited resources of mobile devices, such as the battery power, also limit the practical deployment of more comprehensive security schemes in an ad hoc network. Continuous and unpredictable ad hoc mobility clouds the distinction between normalcy and anomaly and makes the detection of the malicious behavior difficult.

Unreliability of the wireless medium and the dynamic topology due to node’s mobility or failure result in frequent communication failures, and high delays for path reestablishments. The shared wireless channel has a significant impact on the performance of multi-path routing.

The method to thwart misbehavior activity using data forwarding security was carried out by the mobile nodes that concentrated on the routing efficiency alone. However, malicious event or security threats may be posted on the data forwarding stage as well.

The data forwarding security utilizes straightforward cryptographic techniques which need a lot of round trip time and require efficient key generation mechanism. In mobile ad hoc network the cryptographic techniques
were ineffective on deployment, as most of the mobile nodes are dynamic in nature and the topology varies in tandem to the node transition.

2.5 RESEARCH CONTRIBUTION

The issues that follow in security handling of mobile ad hoc network motivate the researcher to present a new framework.

- Data security architecture is presented to improve the data transmission confidentiality in ad hoc networks based on multi-path routing.
- DSA utilizes the multiple paths between nodes in an ad hoc network to increase the confidentiality robustness of transmitted data.
- The original message to be secured is split into parts that are transmitted in multiple paths.
- The parted messages are encrypted on their course of transmission which improves the security to the next level.
- Reliable data security architecture is implemented for multimedia streaming to provide better bandwidth allocation and reduce transmission delay.
- RDSA for multi-path multimedia streaming over wireless network improves the multiple path routing efficiency in frequent communication failures due to channel interferences.
- Reliable multiple paths between nodes in the ad hoc network increase the security level of transmitted data.
- The proposed framework provides better bandwidth allocation and reduces transmission delay.