CHAPTER 2

LITERATURE REVIEW

2.1 INTRODUCTION

An ad hoc network is referred as wireless network and provides a wireless network communication without using infrastructure mechanism. Ad hoc is a Latin word and has the meaning “for this purpose”. A mobile ad hoc network is a part of ad hoc network defined as a self-configuring infrastructure-less network, each communicated by wireless links with the help of mobile devices. The nodes in the ad hoc network are independent of each other and free to move. Since nodes are independent, packet losses are found to occur while transferring the packets from source to destination. Due to the dynamic nature of network and node mobility, the unsecure ad hoc network loses packets. Each node or device in a MANET can move freely in any direction. Always some changes occur in the communication links.

2.2 A SECURE KEY MODEL FOR EFFICIENT NODE CLUSTERING BASED ON REPUTATION AND RANKING

Privacy plays a major role in forwarding a packet. Privacy-preserve routing is vital for ad hoc networks that entail stronger privacy protection. Data packets and control packets are still linkable and distinguishable in the old schemes but they do not tender inclusive unlinkability or unobservability property. Hence, Wan et al (2012) presented capable privacy requirements concerning privacy-preserving routing in mobile ad hoc networks. An
Unobservable Routing Protocol (USOR) was designed and it provided unlinkability and content unobservability to almost all forms of packets. USOR is capable, because it formed a new merging of cluster signature and ID-based encryption for route discovery. The security examination exhibits that USOR offers strong privacy protection as well as it provided security against attacks which are caused because of node compromise. But wormhole attacks were not prevented using USOR.

Thus, to provide protection against wormhole attacks a security protocol is to be proposed which is basically a difficult task. For communication anonymity, (Sankara & Bhagyaveni 2008) used Secure On demand position based private routing protocol (SO2P). It provided security in mobile ad hoc networks, by means of developing a cryptography algorithm to prevent message hacking. Global Positioning System (GPS) provided the position information of nodes for which privacy was more important. GPS obtained the position information of nodes in the network by a terminal node which behaved like a server. All the information about the terminal nodes present in ad hoc network was recorded by the server with the process of GPS system. The position information was prohibited from internal and external hackers by SO2P. It was performed using a secure routing algorithm in MANET to identify optimal path to reach the destination. Because of security mechanisms, SO2P faced some trouble in routing performance such as high packet loss ratio, less throughput, more time in end to end connection delay. Since SO2P was used under on demand basis, the secure communication might not be an efficient one.

MANET is to be secure from attacks and must be dynamic in providing security (Pankaj & Rajender 2009). Advancement in algorithms and protocols were mandatory for a secure ad hoc network because of heavy rise in security threats. Attackers or malicious nodes affect communication
process and it could be avoided using Encrypted Dynamic Source Routing (EDSR). EDSR was also used to prevent numerous types of Denial-of-Service attacks. If malicious agents were found on the pathway of forwarding a packet, EDSR could drop the data packet or acknowledgment, thus preventing malicious node not to get the right information. Data packets were delivered to their destinations by EDSR but when different malicious agents were presented, it drops the packet which was to be forwarded.

Nodes might also cause problems while packets were to be received by a particular node. The nodes that were engaged in routing and forwarding must have cooperation then only the MANET performs perfectly. Steps were to be taken to make a system work properly even during the existence of malicious nodes. The performances of MANET were greatly affected because of selfish or malicious nodes. Such misbehavior nodes were to be managed. Praveen Sam et al (2008) considered two factors, namely, direct factor and distributed factor, called DUAL factor for the management.

As a development to reactive source-routing protocol, the DUAL factor protocol was designed for MANET. DUAL factor holds the components namely, the observer, the trust analyzer, the reputation scheme and the route analyzer. These components were available in every node.

In DUAL factor each node traced the character of its next-hop neighbors. If any event was found to be suspicious, data to be forwarded was given to the reputation scheme. The node activity could be based on the topology created among the network.

In MANET topology control was a challenging problem. K-edge connected topology control algorithms were designed in order to build robust topologies for mobile networks but it seemed to be insufficient. Normally in networks, node moves at diverse speeds and hence, consistently applying k
values for localized topology control algorithms in any local graph was not useful. Hence, a dynamic method was presented by Nishiyama et al (2012) to use k-edge connected topology control algorithms in MANET. The proposed dynamic method automatically decided the appropriate k value for all local graphs based on local information. The trade-off among topology control and reliability was compromised by using scalable topology control algorithms. Network topology among MANET varied due to mobility and thus it could not manage the network connectivity. The above mentioned was a well known problem, but has yet to be solved. Topology problem arose mainly due to the attacks that affected the network.

The great increase in network based applications had resulted in numerous security leaks. The cryptographic protocols which provide secure communication were also affected by diverse attacks. The network traffic and host activities were monitored by Intrusion Detection Systems (IDSs) in order to avoid impacts caused by unauthorized accesses and attacks. But the traditional misuse-based and anomaly-based IDSs were vulnerable to attacks that affected the encrypted protocols because they were always concerned of payload contents inspection. An anomaly-based detection system with the help of strategically distributed Monitoring Stubs (MSs) was presented by Fadlullah et al (2010). The encrypted traffic was identified by MSs which remove features for detecting the attacks. MSs also trace back the originating network of the attack. The approach was called as DTRAB because it aimed on both Detection and TRAceBack in the monitoring stubs level. But the drawback was that attacks on encrypted protocols were not avoided.

MANET was a dynamic wireless network developed without any preceding infrastructure and so each node could behave like a router and MANET had no restriction (Khokar et al 2010). So it can be accessed by any legitimate network users and malicious attackers. The main challenge for
MANET even during the existence of malicious nodes was the development of robust security solution which must secure it from routing attacks. Solutions based on cryptography and key management to avoid attackers was promising, but based on resource constraints (limited bandwidth and battery power) they led to heavy traffic loads in exchanging and confirming the keys. Tradeoffs among effectiveness and efficiency were not good as well as quite solutions provide better results in the presence of one malicious node but were not suited when multiple attackers are present. The existing security solutions of wire networks could be enforced directly to MANET but they were more vulnerable to security attacks.

MANET should be provided with security because of the usage of wireless transmission medium that was more vulnerable to attacks. In MANET, analogously diverse forms of attacks were present and an efficient way was in need to identify them. Hence, a semantic security method was designed by Mamatha & Sharma (2010): It was highly secure because it focused on detecting misbehaving links, number of packets dropped and malicious nodes correspondingly. The performance of identification and avoidance of malicious nodes, launch packet dropping and message tampering attacks. The proposed security scheme was strong and highly secure. Reactive methods could be employed instead of proactive methods because in packet forwarding, attacks were tedious problem to be prevented. Using the above mentioned technique, by increasing the node density, the effect of attacks could be tested and analyzed. The attacks like blackhole, grayhole, wormhole, rushing attack etc., were still in existence because no algorithms had been launched earlier.

A MANET had large number of communicating hosts which form network topology with wireless communication media. In Quality of Service (QoS) based communication networks, the problem of stringent end-to-end
requirement was to be clarified and for that MANET communication produced a change in communication technology. Normally, complex distributed systems faced many challenges and the main one was the routing problem which depends on a predefined set of customer preferences. It is too critical to provide assurance for quality-of-service and so the author focused on the issue. Hence, Llewellyn et al (2011) made a modification in a cluster-based QoS routing algorithm for MANET which needed to provide fault tolerance. Providing fault tolerance was a hardest one in QoS which forms a link failure-prone environment. Using Fully Distributed Cluster-Based (FDCB) routing protocol, the scalability problems in centralized routing were avoided. The fully distributed cluster-based method was identical to hierarchical routing where every cluster node kept QoS information for other cluster members. Shared global states which were unmanageable and avoided because of FDCB’s distributed nature. For route discovery, initial latency was provided by FDCB’s distributed routing. Cluster heads were combined and could be used to avoid attacks but without providing key security it could not be solved.

Balancing of power consumption between Cluster Heads (CHs) was processed by increasing the coverage time of a clustered wireless sensor network. A model proposed by Shu & Krunz (2010) used both intra and inter cluster traffic because clustering minimized energy consumption but increased communication burdens on CH’s. The approach governed both the deterministic and stochastic models for maximizing the coverage time. In the deterministic approach, the location of the sensor and the CH was known. So a joint algorithm for connecting the sensor and CH-to-CH matrix was designed. In the stochastic model, this could not be done because the location was unknown and hence, a sensing region was assumed, where the sensors were uniformly distributed. Balancing power consumption was attained by
designing two ideas namely, the routing-aware optimal cluster planning and the clustering-aware optimal random relay. Usage of different types of Medium Access Controls (MACs) (e.g., Carrier Sense Multiple Access with Collision Avoidance (CSMA/CA), Time Division Multiple Access (TDMA), hybrid Time Division Multiple Access/Code Division Multiple Access (TDMA/CDMA)) in determined algorithm was an issue. The data transmission through the cluster nodes comparatively reduced the energy than the existing systems, but it had a disadvantage that the traffic at the cluster heads increased.

Dang & Wu (2010) inspected distributed clustering method and designed Delay-Tolerant Mobile Networks (DTMNs) which was a cluster based routing protocol. Grouping mobile nodes that were having identical mobility pattern into a cluster and then, sharing resources (such as buffer space) was the idea of DTMN for overhead reduction and load balancing which aimed to attain capable and scalable routing in DTMN. In mobile nodes, communication flow was not so efficient and in nodal contact estimation, possible errors might occur, so probability, convergence and stability were main issues in distributed clustering in DTMN. The DTMN functions were identified and particular node could make decision about joining or leaving a cluster depending on contact change among the cluster.

Once clusters were formed for inter cluster communications, gateway nodes were found. Key security could be provided along with clustering to avoid loss of packets or prevention from attacks.

A key management in cluster-based MANET was a needed one and it was hard to implement. Li & Liu (2010) designed a fully-distributed ID-based multiple secrets key management scheme for a secure communication using a protocol of group key management. By combining
ID-based multiple secrets and threshold cryptography the IMKM was established. Certificate-based authenticated public key distribution was not needed anymore for IMKM. For key update and key revocation methods, it provides capable mechanisms. Those mechanisms directed to be more suitable, economic, adaptable, scalable, and autonomous key management for MANET. Highly dynamic topologies and varying link qualities of ad hoc networks were addressed by generating a master secret key and it was distributed by all cluster heads. But the drawback in IMKM was that it consumes more bandwidth usage for a secure communication. The clustering with IMKM is also unreliable and it took several rounds to identify the secure channel. Yogita et al (2014), proposed improved Location aided Cluster based Routing Protocol with Key Management scheme with key distribution to generate a secure communication among nodes.

A pairwise key distribution was mandatory for wireless sensor networks because sensor nodes are susceptible to physical capture. Kwon et al (2009) proposed a location-based pairwise key pre-distribution scheme. The scheme obtained higher connectivity and flexible with less resources even during the presence of errors. Full and Random Pairwise key predistribution (FRP) used deployment knowledge and path key offering method. Key predistribution with deployment knowledge was processed first. Secondly, Shared Key Discovery (SKD) was employed. Once pairwise keys were not found by SKD, then extra key establishment was mandatory. After SKD, path key establishment with path key offering was employed. However, sensor node’s constrained capabilities were the problems, because public key cryptography was tough. Achieving higher connectivity was still a great problem because large resources were accompanied and deployment errors could disturb those connectivity severely. Kun & Li (2014) proposed pairwise key management with different security level to each node in the
wireless sensor networks and the compromised nodes cannot disclose the key information in the wireless networks which have higher security level.

In case of no network infrastructure self-healing key distribution schemes will be useful and the lost session keys can be recovered by group users, using self-healing mechanism. In case of unreliable network, specifically in infrastructure-less wireless network (messages may get lost) establishing group keys were also suitable. Hence, an efficient threshold self-healing key distribution method with good properties was proposed by Han et al (2009). With respect to network conditions, the lost data could be recovered by involving the distance between two broadcasts. A new user could be sponsored by the user having more threshold-value in order to combine in the group in consequences session without the knowledge of group manager. The storage overhead of the self healing key distribution at each group user was a polynomial over a finite field (no increase with the number of sessions). Forward and backward securities were not maintained by key distribution. Thus, self-healing key distribution method with original threshold was not secure.

Secure communication in ad hoc wireless networks was mandatory, because communication signals were normally available in a non secure form (openly) and so they were mostly affected by attacks. Moreover, due to the absence of central coordination and shared wireless medium they were greatly be affected by attacks compared to that of wired networks. Nodes behaved like both hosts and routers and with the help of multi-hop communication path they are interconnected. Interconnection happens mainly for forwarding and receiving packets to or from other nodes. So, Sumathy & Upendra (2010) designed a key exchange and encryption mechanism. In that, MAC address was used as an extra parameter denoted as message specific key for encryption and data was forwarded between nodes. In spanning tree fashion
nodes organization was done, because formation of cycles were avoided and exchanging occurs only with neighbors which are authenticated. If the particular node was not the expected recipient, re-encryption of message neighborhood key was made and transmission would take place with its authenticated neighboring nodes. The above said process was repeated until destination node was identified but it was a time consuming process. The drawback of the technique was consuming high bandwidth for a secure key exchange. The key storage and the message storage at the node level were not employed in the proposed technique.

### 2.3 A HYBRID APPROACH FOR NODE CO-OPERATION BASED CLUSTERING IN MANET

Routing misbehavior in MANET was a considerable one because of its open structure. Routing protocols for MANET depend on the assumption that completely cooperative nodes could only take part. Many routing misbehaviors were present and one among them is that, some nodes might be involved in route discovery and maintenance processes but they will fail to forward data packets. The route fails to forward packets, because it may be selfish, overloaded, broken, or malicious. So, to avoid routing misbehavior Liu et al (2007) implemented the two way ACKnowledgement (2ACK) method. The main idea behind 2ACK was to receive the acknowledgements from two different hops in order to identify the misbehaving node in routing. Hence, 2ACK avoided the routing problems by detecting misbehaving node which is also referred as network-layer technique. But, route with two hops received acknowledgements in opposite direction which caused data traffic collision.

In multihop networks like mobile ad hoc networks, a node could behave rudely by dropping other packets to save battery life, because of which the whole network performance was degraded. Reputation based
models have been introduced (Abbas et al 2010) to avoid node misbehavior and it was also used to avoid whitewashing attacks. Whitewashing means that if a node had poor reputation on its identity it would be changed to form a new one and would be escaped from the consequences because of its bad actions. It led the performance of reputation based models worst. Reputation based method behaves like an obstacle in whitewashing attacks. In the proposed method, every node must pay an entry fee to use network services. Selfish nodes could no longer whitewash as it needed to pay the entry fee whenever it entered the network. Watchdog mechanism was also adopted, in which reputations were performed at every node in the network. Reputation table was maintained in watchdog mechanism to note the reputation of one hop neighbors. The drawback of proposed method was that newcomers were not allowed. Blackhole attacks were also major problem creating attacks.

Mohmoud et al (2012) focused on the selfish nodes that distract proper node cooperation. A Fair, Efficient, and Secure Cooperation Incentive Mechanism termed FESCIM were developed to stimulate the node cooperation. The FESCIM mechanism performed a fair charging principle by modifying the source and destination nodes when both of them profit from the packet transmission. FESCIM employed hashing operations to make the node cooperation more effective. Hash operation in the ACK packets reduced the degree of digital-signature operations. However, FESCIM failed in the process of identifying misbehaving nodes. FESCIM dropped the packets due to mobility, bad channel, maliciously and frequently dropping packets resulting in malicious behavior causing less security.

A malicious node forms a blackhole attack on MANET, which found the route from a source to a destination and modified sequence number and hop count of the routing message. Su (2011) designed intrusion detection system nodes that were employed in MANET to detect and prevent blackhole attacks. The IDS nodes are put to sniff mode to perform Anti-Blackhole
Mechanism (ABM) function. ABM was used to find a suspicious value of a node regarding to the difference among the routing messages which were routed from the node. A block message denoting to isolate the malicious node was sent to every node on the network by IDS, only if the suspicious value was more than threshold. Even, Ad hoc On-demand Distance Routing (AODV) provides a network connection when the number of IDS could not able to cover most of the area, because of less processing loads and memory consumption. To identify whether routing message was new AODV uses sequence number. Malicious node executed Blackhole AODV (BAODV) routing algorithm to avoid blackhole attacks. Normal node implemented a mildly modified AODV, called Modified AODV (MAODV), to conduct normal routing. IDS node implemented ABM to identify blackhole nodes and block message was presented. Hence, privacy was to be provided for nodes but threats based on privacy also affected the nodes.

Privacy threat was the major issue in multihop wireless networks due to the open wireless medium, in which attacks such as traffic analysis and flow tracing were initiated effortlessly by a malicious attacker. Fan et al (2011) designed a network coding based on privacy-preserving method in regards to traffic analysis, flow tracing like size correlation, time correlation and message content correlation. By trimming each message to be of the similar length, size correlation could be blocked in network coding method. Using inherent buffering method of network coding, time correlation could be resisted. Using “mixing” feature of network coding, message content correlation could be avoided. Two efficient privacy-preserving techniques were designed along with homomorphic encryption on Global Encoding Vectors (GEVs). The methods were packet flow untraceability and message content confidentiality that were proposed for preventing the traffic analysis attacks. Calculation on incoming messages was achieved by intermediate
nodes which were allowed by network coding. Then, security was to be provided to avoid attacks.

During the existence of eavesdroppers, wireless networks connectivity would be diminished by information-theoretic security constraints. The security constraint motivates those networks for enhanced modeling and develops techniques which were robust to eavesdropping. Zhou et al (2011) considered the secure connections from a transmitter to the legitimate receiver(s) over fading channels, where the legitimate nodes and eavesdroppers were all randomly located. There were two forms of eavesdroppers, namely, non-colluding eavesdroppers and colluding eavesdroppers.

Multiple transmit antenna elements based nodes had a secure connectivity by the development of a directional antenna. With multi-antenna transmission techniques a large connectivity improvement was obtained. Even though security was provided, mobile users suffered a lot with authentication.

In wireless networks, roaming of mobile users, was ultimately high and authentication to be provided to mobile users was challenging. He et al (2011) designed a privacy-preserving universal authentication protocol (shortly termed as Priauth). It provided authentication against both eavesdroppers and foreign servers. Efficiency was obtained by the establishment of session key. Assumption was made as the attacker has full control against overall communication channels (among user, foreign server, home server), i.e., it might intercept, insert, delete, or modify any message running through the channel. Mainly, four forms of threats were there for user authentication namely, message en route threat, false mobile user threat, DoS attack and deposit-case attack. Here a roaming user, a foreign server and a home server were involved. In Priauth, foreign server established a session key with roaming user before it is authenticated. In Priauth, foreign servers
used the Revocation List (RL) to verify that the roaming user moved from the home server was revoked or not.

Security often dealt with cost regarding performance degradation, which should be evaluated and it was in the case of Wireless Ad hoc Networks (WANETs) because it provided communications over a shared wireless channel without previous infrastructure. Zhang et al (2011) proposed a network model in which the asymptotic behaviors of secure throughput and delay were noted and when the network size was huge the probability of neighboring nodes having a fundamental security association was evaluated. A secure communication method without Secure Link Augmentation (SLA) was used and its performance was analyzed. Achievable secure network performance was estimated when SLA was allowed. Upper bounds on the secure throughput are presented with or without SLA. Throughput maintenance was also a major thing and capacity of wireless networks should be decreased.

In order to increase the capacity of wireless networks, Multi-Input Multi-Output (MIMO) method was used. Capacity scaling laws, for MIMO ad hoc networks was examined. Jiang et al (2011) identified the achievable throughput of each node by increasing the number of nodes in the network. zero-forcing beamforming (ZFBF) scheme was mainly used to exploit the profits of antenna arrays at a node. ZFBF held the two main attributes of MIMO namely; spatial multiplexing and interference cancellation. In spatial multiplexing, a transmitter could send numerous autonomous data streams to its expected receiver concurrently on a link. In interference cancellation, the transmission and reception vectors could be designed properly, so that the interference among numerous conflicting links could be removed. The development of upper bound was the key idea of ZFBF, for which joint consideration of spatial multiplexing and interference cancellation was
needed. Both lower bound and upper bound had the same order and hence, asymptotic capacity for MIMO ad hoc network was tight. Delay might get increased because of the nodes and as a result, special care should be taken to avoid delay.

A TDMA based simple transmission method (Bhatnagar et al. 2010) which reduced the delay problem occurred by the poor synchronization of the relaying nodes against Ricean channels. A Pair-wise Error Probability (PEP) was also proposed based on precoder for unsynchronized cooperative networks against Ricean (fading) channels which were uncorrelated. If transmissions were scheduled correctly, then significant coding of optimized precoder could be gained. Full diversity could also be obtained based on approximate delay profile. The drawback of the above mentioned method was that higher SNR among the relays due to wrong relaying.

Rossi et al. (2011) took into account the wireless cooperative multihop networks, in which the message decoded by a node at the previous hop to cooperate in the transmission towards the next hop (with distributed space-time coding). The aim of the author was to find optimal cooperator selection approach for arbitrary topologies with links troubled by path loss and multipath fading. Through an appropriate Markov chain, the network behavior was modeled and cooperator selection process was devised as a Stochastic Shortest Path problem (SSP). A new pruning technique was developed to diminish the complexity of SSP. The technique started from the original problem and a diminished Markov chain was retrieved which was at last installed into a solver with the help of Focused Real Time Dynamic Programming (FRTDP).

The ability of mobile infostation network could be increased through short-range communications among mobile nodes and fixed infostations. Cooperation among mobile nodes was not fundamentally casual
for commercial applications. Yuen et al (2009) decided to present a means to generate cooperation in the contention distribution context among the selfish mobile infostation networks. Every node had an interest in all files, was the first assumption. A bilateral file exchange occurs only when the nodes obtained something which was wanted from the exchange. Capacity depends on mobility, the number of files to be declared, and node density. Downloading time of each node would decrease when nodes had implicit cooperation. Energy cost for transmitting one file was balanced. Analysis had proven that the networking performance of the file exchange method was based on node mobility and density. As number of files in the network increases, the fairness and throughput of the network also got improved. If nodes had overlapping interest, then network performance was highly corrupted. Cooperation enforcement should be addressable and should not increase to an extent.

Every user had its own rights in autonomous MANET but the cooperation enforcement performance problems were the major concern. The problems had to be resolved to perform network functioning, like packet forwarding which causes trouble under noise and imperfect monitoring. So, Ji et al (2006) focused on cooperation enforcement in autonomous MANET which causes noise and imperfect observation. The fundamental packet-forwarding function was considered by means of game models with information which were not correct. Belief-based packet forwarding framework was used to enforce cooperation to reduce noise and imperfect observation. Nodes were needed to figure out the future actions of other nodes which depend on their own imperfect observations. The inference process held noise and imperfect observations and to compute them traffic monitoring approaches were considered. It was carried out by each node which keeps track of its neighbors’ actions. Encryption techniques could be taken into account to provide security in routing.
An encryption technique designed by Sumathy & Upendra (2010) was used as a safe key alternate over the nodes in the network. The positive side of the security scheme was that encryption was done twice using two diverse encryption schemes (neighborhood key and message specific key). Hence more security was provided. Two forms of secrecy were also employed and they were backward and forward secrecy. In the backward secrecy, a network’s novel member was not able to access the data that was transferred before the member joined the group. In the forward secrecy, a member was not able to access the data that was transferred after the member goes away from the group. Normally, the topology changes by adding or removing a member, at that time a novel neighborhood key was generated and given to all authenticated neighbors. The neighborhood key for each authenticated neighbor was applicable when group communication was to be carried out in a secure manner. The neighbor detection method was to identity-free and was preceded with handshake procedure among several pair of neighbors. For key exchanges, handshaking procedure was followed among the given node and its newly identified neighbors. Key management based protection could be employed for secure communication.

Li & Liu (2010) proposed a system for a secure communication using group key management protocol. It used ID supported confirmation key over ad hoc network for safe forwarding. Key management was used in cluster-based MANET, because of the dynamic nature of the network and offering a secure communication is challenging. The master secret key was developed for addressing the dynamic topologies and link qualities. The key was distributed by all cluster-heads. As a result, not only attack and failure were avoided but it led to flexible key update methods. The number of rounds and bandwidth usage were also minimized by a significant one round ID-based Authenticated Group Key Agreement (ID-AGKA) protocol. All primary security concerns are also satisfied by ID-AGKA. Even though, the
ID-AGKA provided efficient packet delivery ratio through clustering operations, the time taken for transmission was bit high.

Most of the node cooperation was performed using the concepts of clustering. One such proposed method by Ashok Kumar et al (2011) was Energy Efficient Clustering and Cluster Head Rotation Scheme (ERP-SCDS) for WSN. ERP-SCDS supported clustering formation but it was time consuming and clustering energy dissipation was low. In addition ERP-SCDS faced the difficulty of large overhead in external information forwarding for cluster maintenance. Also Dong et al (2011) developed ODMRP protocol using a High-Throughput metric. Although ODMRP-HT was capable of providing high throughput and the efficiency in improving security in terms of quality was still lower.

Node distribution was not uniform in wireless networks; hence energy consumption by nodes was more in cluster-based sensor networks. Yu et al (2012) designed a cluster-based routing protocol for WSN along with nonuniform node distribution. The protocol involved an Energy-Aware Clustering Algorithm (EACA) and a cluster-based routing algorithm. Clusters of even sizes were generated based on competition range which was used by EACA. In the covered area, the forwarding tasks of the nodes was improved by routing algorithms, which was done by choosing nodes with higher energy by cluster heads. Then, next hop of cluster heads were fewer member nodes and obtains load balance among cluster heads. Cluster heads with higher energy was chosen based on the ratio of average residual energy of neighbor nodes and the residual energy of the node itself.
2.4 EFFICIENT NODE COOPERATION AND SECURITY IN MANET USING CLOSENESS - A DEGREE OF SEPARATION

A Sensor network consists of many sensor nodes and those networks were normally found to be in mesh structure. Mostly, nodes in sensor networks were static and some sensor nodes behaved like a router which forward messages from one neighborhood to another. In node connectivity, changes result due to the disruptions like transmission power changes, or loss of synchronization within neighboring nodes in wireless communication. Node connectivity was more important in providing security because, attacks may also spoil network connectivity. Sensors were conscious about their immediate neighbors, but still it should constantly manage its view, so a mechanism called continuous neighbor discovery was proposed by Cohen & Kapchits (2011). Two nodes were denoted as neighboring nodes only when they have straight wireless connectivity and it must be always bidirectional. Sensors in networks with heavy traffic do not need to initiate any particular neighbor discovery protocol instead of which the node could identify its neighbor by listening to the channel and could reform the lost connectivity.

Technologies for connectivity maintenance and message exchange between decentralized nodes were to be designed, so wireless multi-hop network adopted wireless communication technologies. Wireless resource allocation needed centralized coordinator as it is in heavy lack and so the design of medium access control protocols was difficult for throughput enhancement in the wireless ad hoc networks. The receiver blocking problem, was the major one in MAC protocol design and resulted in reduced of throughput performance. Feng et al (2013) used Multiple Receiver Transmission (MRT) and Fast Network allocation vector Truncation (FNT) mechanisms to solve the receiver blocking problem (no involvement of extra
control channels). The throughput performance was still to be enhanced and so the Adaptive Receiver Transmission (ART) along with dynamic adjustment of pointed receiver was presented. Effectiveness of ART protocol was validated by deriving analytical model.

Bu et al (2011) combined continuous user authentication and intrusion detection in the design of Value Iteration Algorithm (VIA) to provide high security to MANET. However, the value iteration-based solution for measuring the Gittins Index process only operated for a MANET with a small number of nodes and a small number of states as well as observation states. For a large network with a variety of nodes, the value iteration based solution become computationally intractable and was inefficient in providing security to nodes.

Message delivery in MANET was difficult because there was no connectivity in the network. Hence, a better idea was to find a route which provides good data delivery and produces low delay in a disconnected network. Daly & Haahr (2009) proposed social network analysis metrics that was in use for significant message delivery (forwarding solution) in broken network. The metrics depended on social analysis of node’s past interactions and consisted of three locally calculated factors, namely, a node’s “betweenness” centrality (with the help of ego networks), a node’s social “similarity” to the destination node and a node’s secure energy association with the destination node.

Among the three metrics that were evaluated separately, average utility resulted in better overall delivery performance but congestion was caused due to highly central nodes. Congestion had to be avoided and it could be done only by transferring other node’s data.
In many applications of MANET, mobile nodes shared and used data of alternative mobile nodes. In such type of application, avoiding the degradation of data availability during network partitioning was really a challenging problem. Specifically, in MANET because of free mobility of nodes, connectivity problem happened frequently and makes data in different networks to be unreachable to each other. Hara (2010) target was to quantify the consequences of mobility on data availability from various points of view. Rather than considering particular applications or data replication or diffusion protocols, many common metrics could be assumed to quantify data availability. For data replication protocols, the factors affecting the performance were number of data items to be replicated on connected mobile nodes and time taken and quantity of changes for group of connected mobile nodes.

For data diffusion protocols, factors for performance were the capability (fast) of data items to be allocated to a large number of mobile nodes. Mobility of nodes caused performance degradation in MANET.

The mobile nodes, mobility and resource restrictions resulted in network partitioning or performance reduction in MANET. Network partition was resulted often due to the free movement of nodes and thus, leads to data inaccessibility for some nodes, which was a vital performance metric. Replication of data at nodes was development to enhance data accessibility to carry on with periodic network partitioning. Replication normally enhanced data accessibility and minimizes query delay. Maximization of data accessibility could be done by restricting a node not to hold same replica that was held by other nodes which increased own query delay. Choi et al (2012) and Shoba & Neha (2014) denoted the problem of selfishness regarding replica allocation in MANET, i.e., a selfish node never divided its own memory space to hold replica and the problem was termed as selfish replica
allocation. Selfish node identification and new replica allocation approaches were used to hold the selfish replica allocation. Some selfish nodes were there which includes false data while data was to be transmitted.

In wireless sensor networks, sensor nodes added false data at the time of data aggregation and data forwarding. Ozdemir & Çam (2010) designed a Data Aggregation and Authentication protocol (DAA), to incorporate false data detection with data aggregation and confidentiality. Data aggregation was formed in accordance with false data detection, the observing nodes of each data aggregator performed data aggregation and corresponding small amount message authentication codes were computed for verification of data at their pairmates. Confidential data transmission was carried out as data integrity was authenticated in the encrypted data by the sensor nodes of two continuous data aggregators. One of the candidate aggregators among the two dropped its application and ran the secure Data Aggregator Selection Protocol (DASP) again. The procedure got continued till minimum intermediate nodes among any two consecutive data aggregator were present. Each sensor node should be capable of both aggregating and forwarding of data to advance network security and efficiency. Data forwarding had one major problem i.e., there was a delay in the transmission of packets.

Mobility of relay nodes was improved by delay-tolerant ad hoc networks to make permanent connectivity. Thus facilitate communication among nodes, which were out of range of each other. Delivery delay was to be minimized, so that the data to be delivered was replicated in the network. Altman et al (2008) designed an analytical method that allowed quantifying tradeoffs within resources and performance measures (energy and delay). The coding effect on performance of the network while accessing parameters, which were governed by routing, was also studied. Tradeoff between energy
and probability, which gave a successful delivery during the presence of limited storage capacity at a node were examined. In order to overcome disconnections in Delay-Tolerant Networks (DTN), coding schemes was used in which existence of phase transitions were present. Particularly, message should be applicable for a finite amount of time (i.e., after certain deadline message is of no use). The file to be transferred was splitted into k smaller units. Splitting of file was done when the file was large enough in accordance with buffering capabilities of nodes. Those k smaller units are to be forwarded without the involvement of others. If all k frames were received at the destination, then only the message would be considered to be received in good way.

Due to propagation of packets, node mobility got decreased and power outages got increased because of disconnection in networks that occur in delay tolerant networks. Krifa et al (2008) designed store-carry and forward protocols for above mentioned problem, in which a node stored a message in its own buffer and carried it for a long duration. Capable buffer management methods were required to make decision on which messages was to be discarded. Basics of encounter-based message dissemination were also used in optimal buffer management policy which depended on global knowledge of network. Buffer management policy could be set either to decrease the average delivery delay or to increase the average delivery rate. Finally, distributed algorithm came in existence which tried to estimate the global knowledge that was needed by optimal algorithm.

Devices like Personal Digital Assistance (PDA), cell-phones with wireless interfaces form MANET and communication happened through intermediate nodes. A store and forward network architecture named as delay tolerant network had been created for challenging network environments like network connectivity damage. Chuah & Yang (2009) proposed DTN method,
so the popular nodes got the coded packets by which greater message delivery ratio was got. Mitigation method had been designed to overcome data dropping attacks. For producing more coded packets, mitigation method used dynamic redundancy factor. A selfish or malicious node provides false information in control or data planes of a network coding (wireless network). If selfish nodes were launched in the control plane, attack would affect the selection of routing and in case of data plane, coded packets were corrupted by the attacker hence reconstruction of message by receiver was not possible. Selective dropping attacks based on the delivery performance of network coding were determined by the usage of Community Based (CB) model and Random Waypoint Model (RWP).

Yang et al (2012) denoted the issue in delivering data packets in mobile ad hoc networks based on reliability and time. Position-based Opportunistic Routing (POR) protocol was designed, in which forwarding nodes cache the packet that were to be received based on MAC interception. Some neighbor nodes which identified the transmission of a data packet will pose as forwarding candidates. Those candidates tried to forward the packet only, when it was sent by a best forwarder within mentioned time period. The additional latency utilized by local route recovery was diminished to an extent and the duplicate relaying was also decreased. For communication hole, a Virtual Destination-based Void Handling (VDVH) method was processed. Using VDVH the profits of greedy forwarding (e.g., large progress per hop) and opportunistic routing could be obtained when handling communication voids. Delay-Tolerant was an everlasting problem in MANET and had no end.

In delay tolerant mobile ad hoc networks, direct connectivity was no more needed and messages were delivered to their destination because of mobility of node subset which carried copies of the message. Altman & De
(2011) designed a fluid approximations for class of monotone relay methods (delay tolerant ad hoc networks). The class used epidemic and two-hops routing protocols. The relay policies were upgraded with probabilistic forwarding feature in which a message was forwarded to a relay with some probability. An optimal control problem was composed where a tradeoff between delay and energy consumption was found and optimized.

In DTN, connectivity between mobile nodes was not assured even though many solutions were in existence. DTN’s constant assumption was that the nodes always forwarded messages but the main problem arose when they were affected by attacks. Dini & Duca (2012) designed a reputation-based protocol for conflicting blackhole attacks. In every node, table’s node forwarding reputation and for forwarding the next node, it chose the node which has highest reputation. Three basic methods were involved in the protocol namely; node lists, aging (for efficient communication) and supports changing operating conditions (of DTN) to avoid attacks. Reputation-based approach was applied to Context Aware Routing (CAR) protocol (probability-based routing protocol) to protect the messages from blackhole attack. Lower the reputation, higher the chance of node being blackhole. Dropping of packets was major problem in MANET in order to save energy.

In multihop networks like MANET, to save battery life a node dropped other packets, due to which whole network got collapsed. Reputation based models had been introduced (Abbas et al 2010) to avoid node misbehavior and whitewashing attacks. Preventing the consequences which would be caused by bad actions when a node has poor reputation and fresh one was to be started. It led the performance of reputation based models worst. Reputation based method behaved like a deterrent for whitewashing attacks. In reputation based method paying entry fee by every node was a compulsory one in order to use network services. But a selfish node could not
whitewash for a long time because it needed to pay entry fee whenever it entered the network. Watchdog mechanism was also adopted, in which reputations were performed at every node in the network. Reputation table was used to note the reputation of one hop neighbors. The drawback of the method was that newcomers were not allowed. Hence, every user should had own authority than having it commonly.

In self-organized MANET, every user had their own rights which behave cooperatively like unconditionally forwarding packets for each other was not acceptable. Ji et al (2006) aimed in cooperation enforcement of self-organized mobile ad hoc networks which were with noise and imperfect observation. The basic packet-forwarding function with the help of repeated game models with no clear information was also studied. A belief-based packet forwarding framework was designed to gain cooperation-enforcement strategies which relayed on each node’s past actions. Applying repeated game model was to evaluate the nodes interactions. The drawback was that two nodes were needed for carrying a packet and forwarding a packet which led to delay in delivery. Simple solution was to provide key based security in delivering a packet with node clustering concept.

A key management in cluster-based MANET was important thing. Li & Liu (2010) designed a fully-distributed IMKM for a secure communication using a protocol of group key management. Combining ID-based multiple secrets and threshold cryptography, IMKM was established. Sharing secret key among cluster heads was done using the protocol and it was distributed to its master secret key. As a result, not only attack and failure were avoided by the protocol but it also led to flexible key update methods. Number of rounds and bandwidth usage were also minimized by a significant one round ID-based authenticated group key agreement protocol. All primary security concerns are also satisfied by ID-
AGKA. But the drawbacks in IMKM were that it consumes more bandwidth usage for a secure communication. The clustering with IMKM was also unreliable and it took several rounds to identify the secure channel and the communication between the nodes and clustering processes both were effectively reliable ones to communicate.

Security was the bottleneck for wireless applications because they were vulnerable to attacks. Guan et al (2012) was interested on authentication and topology control issues and developed a Joint Authentication and Topology Control (JATC) method in order to improve the throughput. JATC was an optimization problem, which needed the channel estimation rather than prior perfect channel status. With study to an authentication protocol, JATC method was designed. It improved the parameters of up-layer authentication protocol and PHY-layer transmission settings to raise resource utilization and throughput capacity of the network. JATC handled the imperfect channel knowledge and the changing topology, for that a discrete stochastic approximation approach was involved by JATC. Thus, more efficient security was to be provided with key model along with clustering concept in an advanced manner.

2.5 RESEARCH GAP

In wireless communications especially in MANET, security was the main challenge that needed to be concentrated. The security examination exhibits that USOR provided strong privacy protection between the nodes but wormhole attacks were not able to be prevented. A Secure on demand position based private routing protocol is an another security providing protocol, used for providing a shared secured key on demand for data packet but did not provide a secure communication between nodes. So it was difficult to provide security to the transmission of data without providing a secure communication between nodes.
In MANET, providing a secure communication was difficult due to the topology crisis and the attacks that affect MANET. A dynamic method was designed to employ topology control algorithms in MANET to avoid topology problems but the topology among the MANET varied due to the mobility of nodes, thus maintaining the network connectivity and node cooperation was difficult task.

There were many cryptographic protocols proposed to provide secure communication in MANET but were also affected by diverse attacks. Hence, DTRAB was established for Detection and TRAceBack in the monitoring stubs level. But it failed to avoid attacks like blackhole, grayhole, wormhole, rushing attack over an encrypted protocols. These attacks could be avoided by clustering nodes in MANET with the help of cluster heads. The Cluster heads were combined to avoid attacks but without providing key security they could not be solved. The data transmission through the cluster nodes was efficient regarding energy but the traffic at the cluster heads increased. A key security management could be provided along with clustering to avoid loss of packets or prevention from attacks.

A fully-distributed ID-based multiple secrets key management for group key management was proposed for a secure communication. But the drawbacks in IMKM were bandwidth usage for a secure communication, clustering and took several rounds to identify the secure channel. Due to this, the communication between the nodes and the clustering processes were main problem in group key management.

In a secure communication, the misbehavior of nodes might also cause problems in MANET. The routing misbehavior was avoided by implementing the 2ACK method but when misbehaving nodes participate in the route discovery, it degraded the performance in terms of dropping the packets and consumes more power.
The packet dropping problem was avoided by using reputation based method which mainly avoid whitewashing attacks. But if any new node participates in the route discovery process then there would be a delay, because they are not part of the clustered nodes. Then delay might get increased because the new node also taken into account i.e., due to delay, packets were not delivered to destination node in given period of time.

2.6 OBJECTIVES OF THE RESEARCH

The main objectives of this research work are as follows,

- To design a secure key model by clustering the nodes with group key management to provide security to the participating nodes in terms of packet transmission and routing, that helps the nodes to communicate without any loss of data and to evaluate the authentication of neighboring nodes with the help of cluster heads.

- To provide secure communication between the nodes in the MANET without any loss of data, the secure key model need the cooperation based clustering for monitoring the activity and behavior of nodes.

- To avoid the misbehavior of nodes in the clustered MANET, it is necessary to design enhanced mechanism that monitors the neighboring nodes who are participate in the communication in the cluster.

- To minimize the delay in the route discovery due to misbehavior of node, need to focus an end to end route awareness and end to end route quality in terms of path lifetimes.
2.7 CONTRIBUTIONS OF THESIS

The first work describes, a secure communication between nodes in MANET without data loss, using secure key model (SKM) for efficient node clustering based on reputation and ranking system. By using this model, nodes are clustered and each node maintains its own reputation table. The details are illustrated in the chapter 3.

Second research work, proposed is Hybrid Approach for Node Cooperation based Clustering (HANCC). The proposed method avoids security issues like illogical node participation to balance the cooperation among the nodes. The details are illustrated in the chapter 4.

Third work describes an Efficient Node Cooperation and Security (ENCS) mechanism. It reduces the packet loss due to security attacks using closeness technique. The mechanism for closeness technique based on reputation is illustrated in the chapter 5.

The final work, manages resource allocation with Routing Aware Packet Reserving (RAPR) framework for end-to-end throughput maintenance. It describes the approach to resolve the effective resource allocation based on node clustering, node cooperation and higher security level.