Comparative Study of Energy Efficient Routing Protocols in Manet

[1]K. THAMIZHMARAN, [2]A. CHARLES
[1]Department of ECE, Annamalai University, Tamil Nadu, INDIA
[2]Department of ECE, GCE, Bargur, Tamil Nadu, INDIA

Abstract - Today in the world most of young researchers focused infrastructure less network is ad hoc network, especially one type of the best research temporary network is called Mobile Ad hoc Network (MANET). Mobile ad hoc network is collection of in-depended mobile nodes that able to communicate anytime anywhere in the emergency environment through wireless link with each other also every node acts as transmitter, receiver and router. This self configured infrastructure less network having some issues like traffic, delay, throughput, energy, security attacks, bandwidth and storage etc., [2] more are less energy and security attacks is very dangers issue due to dynamic nature, battery power, packet drop, misbehaviour attack, conjunction and mobility. In this research writing mainly we discussed energy issue because of when solve energy automatically network lifetime will be increased and also delivery ratio and throughput will be increased due to reduces of energy utilization, so here we discussed some of valuable research work they conclude the importance of energy efficient with help of one of leading simulation model called Network Simulator (NS2).

Index - MANET; Routing; Issues; Energy Models; NS2;

1. Introduction

Now fast growing global human population the emerging and unpredictable developed technologies is wireless network; this network is classified two types: one of fixed, centralized and wired gateways network called cellular network, when an each mobile unit goes out of range of one base station, it connects with another new base station. To solving natural issue demand implemented technology, that every node of these networks behave as routers and take part in discovery and maintenance of routes to other nodes called wireless ad hoc network show as fig. 1.

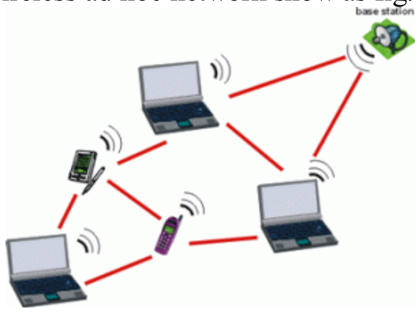

Figure 1 Wireless Ad hoc Network

The above figure shows base of infrastructure less networks called ad hoc network this is Latin word, ad hoc means "for this," further meaning "for this purpose only”. This development start from 1970’s PRNET (Packet Radio Network), 1980’s – SURAN (Survivable Adaptive Radio Network), 2000’s - Ad hoc network consortium in Japan and 2010’s - Not fixed Infrastructure. Moreover the unique characteristics of network that not guaranteed bandwidth due to designed shared radio channel more suitable for best-effort data traffic and dynamic frequency reuse based on carrier sense mechanism with distributed routing then infrastructure based network **[1, 5]**. Even though lack of security issue, energy management and frequent path breaks due to mobility but they provide more services of all the environments because of exclusive personality as shows in fig 2.

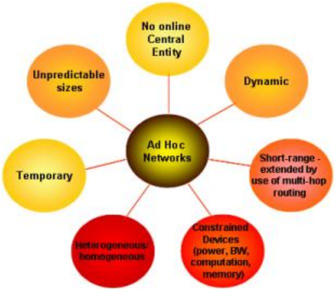
No online Central Entity
Unpredictable sizes
Dynamic
Ad Hoc Networks
Temporary
Short-range - extended by use of multi-hop routing
Heterogeneous/ homogeneous
Constrained Devices (power, BW, computation, memory)

Figure 2 characteristics

There is more Classification of wireless ad hoc network like Mobile Ad hoc Network (MANET) policy formed for consumer electronics, military and rescue via mobile devices connected by wireless, Wireless Mesh Network (WMN) design shaped for shared internet for community with static mesh routers using various of mesh client laptops, cell phones and routers etc., implemented over WLAN, Wireless Sensor Networks (WSN) that designed mainly surveillance by localization and environment monitoring, Vehicular Ad hoc Networks (VANET) that developed especially safety and traffic management etc.

1.1 Mobile Ad hoc Network

Mobile node no default router offered and can be connected dynamically in an arbitrary manner because of network service provide anytime and anywhere in the world due to all the individual node becomes a transmitter, receiver and also act as router: must be able to forward traffic on behalf of others. Sole rules network for Self organized due to update routing information when repeatedly change the topology, multi hop when a node contain more base station sources, MANET nodes travel 360' because of dynamic nature, mobile node limited battery power, very dangers quality is limited security reason for design to node can join anywhere, any place **[3]**. There is more research area available in mobile ad hoc network like quality, routing, path metrics, hop count, geographical, energy conservation, QoS, multicast, security etc., the following parameters now delivered valuable research outcome MANET as show in fig 3.

Figure 3 Mobile Ad hoc Network

Many of existing researcher form reputed institutions, research centers and industrials published more articles with analysis own idea outcome to some of leading parameters such as throughput, end-to-end delay, packet delivery ratio, quality of service, power control, energy efficient routing, multipath routing, congestion Control, bandwidth and loss detection and recovery and etc. **[4]** all the researchers focused and update routing for work above areas to solve the issues, MANET need for router to communicate and data transmission from source to destination, fig 4 shows some of ISO approved protocol.

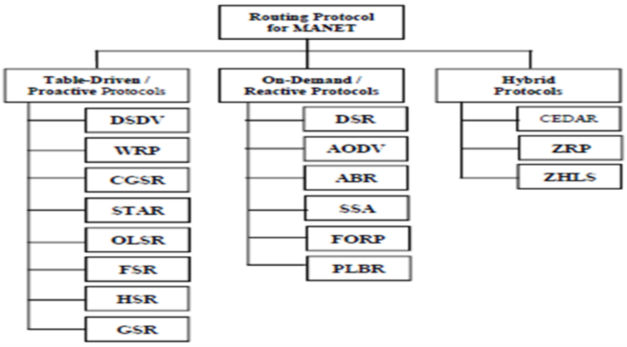
Routing Protocol for MANET
Table-Driven / Proactive Protocols
On-Demand / Reactive Protocols
Hybrid Protocols
DSDV
WRP
CGSR
STAR
OLSR
FSR
HSR
GSR
DSR
AODV
ABR
SSA
FORP
PLBR
CEDAR
ZRP
ZHLS

Figure 5 Routing Protocols

In this research paper need to surveyed one of most leading mobile ad hoc network issue is energy; we discussed existing suggested technology for Energy because of when reduced delay and retransmission also avoided misbehavior automatically throughput maximized so node lifetime and network life time will increased due to increasing remaining energy reason for limited power **[6]**. Very importance states to consume energy to transmit, receive and Sleep. Maximum energy affected in tow layers data link layer and network layer fig 6 shows energy management schemes in particular layers

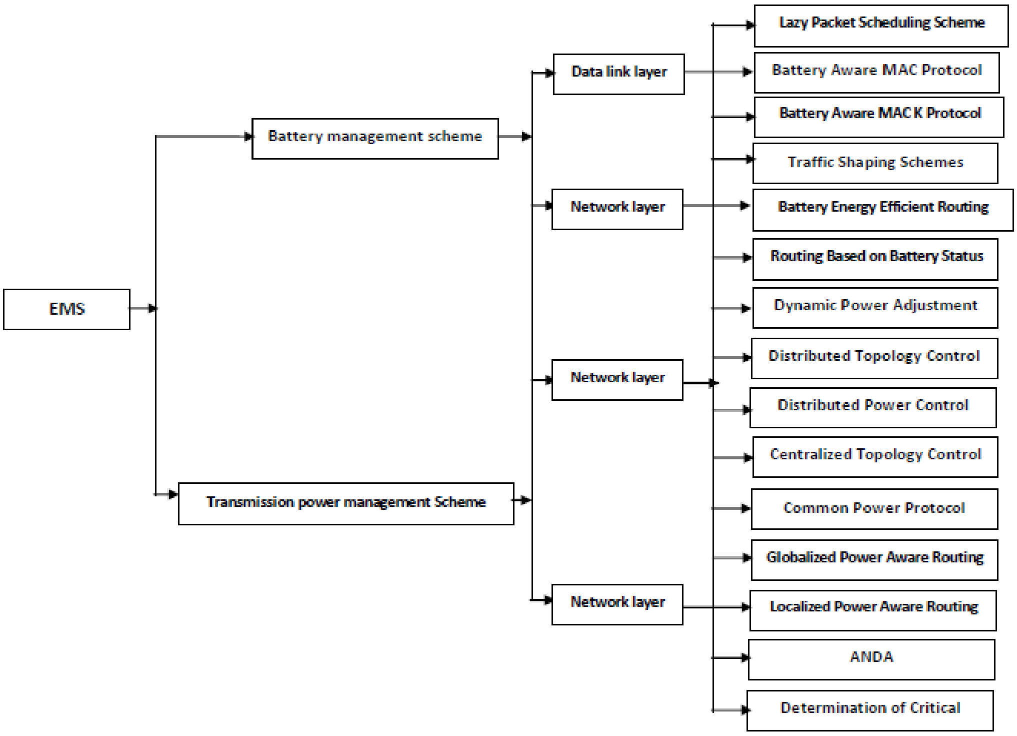
EMS
Battery management scheme
Transmission power management Scheme
Data link layer
Network layer
Network layer
Network layer
Lazy Packet Scheduling Scheme
Battery Aware MAC Protocol
Battery Aware MACK Protocol
Traffic Shaping Schemes
Battery Energy Efficient Routing
Routing Based on Battery Status
Dynamic Power Adjustment
Distributed Topology Control
Distributed Power Control
Centralized Topology Control
Common Power Protocol
Globalized Power Aware Routing
Localized Power Aware Routing
ANDA
Determination of Critical

Figure 5 Energy Management Scheme for N/W & DL Layers

Moreover the above discuses for ad hoc, MANET and routing, In section 2 brief discussion energy based developed researches, section 3 research outcomes, In section 4 conclude this paper.

2. Related Work

Energy is very dangers problem of mobile ad hoc network when retransmitting of packet, increasing time duration of path finding and link breakage to reducing remaining energy due to limited battery power below discussed last 15 years of some of effective reputed research articles **[7]**.

Chan-Ho Min and Sehun Kim, (2007) proposed novel on-demand energy aware routing protocol called Utility Based Power Control Routing (UBPCR), which reduced the trade-offs that arise in the other energy aware route selection mechanisms that had been proposed for MANETs. Evaluation of simulation result, performances of UBPCR with Constant blocked Rate (CBR) and Constant Dropped Rate (CDR). Proposed scheme significantly improves both CBR and CDR by estimating the transmit power for any link. Although some strategies produce relatively small degradations in both CBR and CDR, these capabilities greatly increase transmit power and decrease network lifetime due to approach is based on an economic framework **[8]**. ***Jyu-Yuan Lai and Chih-Tsun Huang, (2008)*** presented a design framework that consisted of a high throughput, parallel and scalable ECC processor. A two phase scheduling methodology was proposed to optimize the ECC such as coarse-grained and fine-grained scheduling. The comparison of speed and overhead among different ECC designs justified the cost effectiveness of the proposed design. Moreover, the biggest problem is packet drop and symmetric key encryption to get the key to the party with whom you are sharing data and also malicious detection has not been considered **[9]**. ***William Chelton and Mohammed Benaissa, (2008)*** have proposed a new high speed pipelined Application Specific Instruction set Processor (ASIP) for ECC using field programmable gate array technology. Three complex instructions were used to reduce the transmit and receive latency after path will create between source to destination by reducing the overall number of instructions and a new combined algorithm point-doubling operation (DBL) and point-adding operation (ADD) was developed to perform using the application specific instructions. Although, ECC scheme that it increases the size of the encrypted message significantly more than RSA encryption by the way delay also increased, increased the possibility of implementation errors and thereby reduced the security of the algorithm due to ECC design is very complex **[10]**. ***Sunho Lim et al, (2009)*** explained very clearly a new communication mechanism called random cast, which a sender could specify the desired level of overhearing, making a discreet balance between energy and routing performance. Simulation results demonstrated, performance comparison of 802.11, 802.11 power saving mechanism, on-demand power management and random cast. In addition, it reduced redundant rebroadcasts for a broadcast packet, and thus, saved remaining energy by 30% also increase delivery ratio of random cast than other scheme through simulation using NS-2 but not suitable to other routing protocols. Meanwhile, average delay and packet drop will be increases when presence of misbehaviour **[11]**. ***Peng Zhang et al, (2009)*** they proposed a mobile average network coding to reduce the energy consumed by data encryption in MANET. In their work, they used P-Coding lightweight encryption scheme to provide confidentiality for network coded MANETs, in an energy efficient way. Finally, they demonstrated that due to its lightweight nature, P-Coding achieved minimal energy consumption with less transmission compared to other encryption schemes. Moreover, problem was with access control over the remotely stored files, while enable resource limited mobile devices to easily access the protected data, especially if the storage server maintained by a third party was un-trusted so misbehaviour will attack the performance also P-coding reduce performance of other communication network with environment **[12]**.

Zhang Tao et al, (2009) have suggested effectively the newly emerging side channel attacks on elliptic curve cryptosystem, and an efficient Fractional Width-w NAF (FWNAF) algorithm was proposed to secure ECC scalar multiplication from these attacks. This algorithm adopted the fractional window method and probabilistic Shortest Path Algorithm (SPA) scheme to reconfigure the pre-computed table. Results compared proposed FWNAF with WBRIP and EBRIP schemes, the proposed analysis had the lowest total computation cost, reduced utilization energy and bandwidth. However, cryptosystem needs lower reconfiguration capability when changing topology or attacker will enter in network, average delay and packet drops increased with lower remaining energy **[13]**. ***Venkateswaran et al, (2009)*** proposed two instances of the relay deployment problem, to gather with the solutions, to achieve goal is Min-Total Min-Max, aimed to minimize the total energy consumed. The results indicated that even when the relay nodes constituted a small fraction of the total nodes in the network, the planned framework resulted in significant energy savings except at the time of retransmission. Simulation results shows, relay based schemes reduced total transmission energy than without relay also remaining energy of Min-max better than Min-Total scheme both scheme suitable for low mobility and minimum number of users. Furthermore, high mobility network is not support because when increase users attackers also increased also delay will be increased so automatically utilization energy will be increased **[14]**. ***Burmester and de Medeiros (2009)*** proposed a complete self-configured Secure Energy Efficient (SEC) protocol that was able to create the network and share secure services without any infrastructure. The network allowed sharing resources while offering new services among users in a secure environment. The protocol included all functions needed to operate without any external support. Their proposal was implemented in order to test the protocol procedure and performance also increased remaining energy. Although, multipath routing protocols for MANET ignore the topology exposure problem and routing overhead has not been considered in this work **[15]**. ***Jithra Adikari et al, (2010)*** who discussed single and double scalar multiplications as the most computational intensive operations in ECC based cryptosystems. Improving the performance of these operations is generally achieved by means of integer recoding techniques, which aim at minimizing the scalars' density of nonzero digits. Proposed scheme present three novel algorithms such as hybrid binary ternary form, hybrid binary-ternary joint form and reduced hybrid binary-ternary joint form for both single and double scalar multiplication. Finally, the experiment results showed that the algorithms were almost always faster than their widely used counterparts. Moreover, this algorithm increased energy consumption because hybrid binary-ternary number system increase the average running time of network, security attacks have been not considered also energy saving issue because average delay increased **[16]**. ***Morteza Nikooghadem et al, (2010)*** they have efficient key management and key derivation schemes based on ECC to solve dynamic access problems in a user hierarchy. Proposed method had less time complexity and Simulation results, achieve best performance and highest security level in transmission through all the nodes between source and destination than previous works using private and public key until attacker will be present. Furthermore, misbehave detection and routing overhead are still challenging issues due to when changing topology will take some time to configure the network **[17]**.

Manikandan and Sathyasheela, (2010) have proposed technique called ADCLI for MANETs. This algorithm can be used to detect malicious nodes in a set of nodes such that each pair of nodes in the set are within the radio range of each other used to message passing between the nodes. The simulation was done for four different set of values and achieve high performance of delivery ratio and low packet loss but time delay increases due to node are dynamic nature, when a new node is added in the network, then the topology of the network will change and it takes some time to converge during that time if they want to send data to destination through that new node immediately, which causes grasp in energy by way of network congestion and link breakage also increases **[18]**. ***Karim El Defrawy and Gene Tsudik (2011)*** analyzed secure MANETs which are particularly useful and well-suited for critical scenarios. They constructed an on-demand location based anonymous MANET routing protocol called Privacy-friendly Routing In Suspicious MANETs (PRISM) that achieved privacy and security against both outsider and insider adversaries. Results showed that PRISM was more efficient and offered better privacy than the prior work, lower used energy. However, these protocols are vulnerable to the attacks of misbehaviour packets broadcasting, even the node misbehaviour attacks increased and network life time also decreased **[19]**. ***Ming-Yang Su, (2011)*** Developed new intrusion detection technique to detect block-hole attacks called Anti-Black-Hole (ABM) mechanism. When a suspicious value exceeded a threshold, an IDS nearby would broadcast a block message, informing all nodes on the network, asking them to cooperatively isolate the malicious node. It fails to judge on route replies coming from the intermediate node based on a trusted third party which is the destination node. Performance comparison of proposed and existing AODV protocols, results shows AMB reduce total packet loss rate by 10.05% than existing scheme. Meanwhile, network delay and routing overhead will be increased due to network usage also increased big challenge issue in this protocol **[20]**. ***Nicola Costagliola et al, (2012)*** they designed a new optimized energy aware path selection called MChannel-opt, use to enabling uncast routing based on two alternative metrics, namely delay and overall network lifetime. Proposed module MChannel-opt, they proved better network lifetime and average delay compared MChannel protocol also increased network remaining energy due to link established all the nodes before the transmitting the packet in the network because suggested MChannel-opt based on proactive protocol. Moreover, misbehaviour attacks and packet dropping attack based solutions do not address in this work so they don't provide secure path **[21]. *May Zin Oo and Mazliza Othman, (2012)*** they have proposed and compared mobility models to measure single path and multipath (proactive and reactive) routing protocols across the mobility models by tuning into TCP and CBR traffic individually. They developed algorithm interaction between mobility models, single path and multipath routing protocols that varied depending on the usage of traffic (TCP and CBR) that significantly reduced the end-to-end delay and reducing remaining energy consumption at a same network lifetime also decreasing. Moreover, security aspects and packet loss and link breakage have not been considered in this work **[22]**.

Chun-Ta Li (2013) suggested an advanced smart card based password authentication with ECC, an updated scheme and extended the scheme to provide the privacy of the client. By comparing the criteria with other related schemes, this scheme not only solved several hard security threats but also satisfied more number of functionality features, and delivery ratio and throughput increased, Proposed ECC based scheme achieve mutual authentication and low computation cost. Although, all the strategies of proposed scheme are not analyzed from misbehave and collision of network and traffic security perspective to increased average delay when enter malicious attacker also network throughput significantly reduced **[23]**. ***Wang et al, (2013)*** have proposed Distributed energy Adaptive location based Cooperative Medium Access Control (DEL-CMAC) to improve the performance of the MANETs in terms of network lifetime and energy efficiency. Furthermore, they projected DEL-CMAC protocol under various conditions even for high circuitry energy consumption in comprehensive simulation study. Finally, the energy utilization of nodes is reduced with the possibility of link breakage within the network because DEL scheme all the node actives monitor in network in every time but for large network cannot support new protocol due low security and network throughput will be reduced **[24]**. ***Zijian Wang et al, (2013)*** they proposed a novel location service protocol called hierarchical hashing location server protocol that optimized the distance travelled by the location update and query packets, and reduced the overall energy cost. Simulation results demonstrated that the proposed protocols achieved around 30 to 35% energy efficiency while improving or maintaining the query success rate in comparison to the previously proposed algorithms. Even though, Energy models address only the hidden terminal issue, but result in network throughput and packet delivery ratio during the presence of misbehaver node **[25]**. ***Hafizul Islamand and Biswas (2014)*** suggested new password based mutual authentication using several dynamic energy ID-based remote user authentication schemes which were implemented using password, smartcard and ECC. Additionally, the proposed scheme was provably secure in the random oracle model under the hardness assumption of computational Diffie-Hellman problem. Data security, privacy and user authentication are enormously important for accessing important medical data over insecure communication. The proposed scheme is thus more efficient, secure and flexible than other existing schemes. Hence protocol cannot achieve complete security requirements. Congestion and link breakage are also not discussed **[26]**. ***Abdulsalam Basabaaa et al, (2014)*** discussed most of the proposed protocols assuming that all nodes in the network were cooperative, and did not address security issues. They projected new IDS named Adaptive 3 Acknowledgements (A3ACKs) that solved three of six significant problems of watchdog technique presence of malicious node. They implemented and tested the proposed system under various mobility speeds through NS2. Increases packet delivery ratio by 13.3% of high speed network and by 12% of low speed network when measured over 30% to 40% malicious nodes, the A3ACKs improved network performance with or without the presence of consecutive cooperative misbehaving nodes in a route path. Even though the network congestion has slightly increased, the network security is more robust and remaining energy will be increase **[27]**.

Gopinath and Nagarajan (2015) presented energy efficient routing protocol called Residual Energy-based Reliable Multicast Routing (RERMR) protocol to attain more network lifetime and increased packet delivery and forwarding rate. The proposed protocol is based on threshold value to maintain the reliable multicast routing which enhances the stability and connectivity of the network. Based on the simulation results, the proposed work achieved better performance than the previous protocols in terms of packet reliability rate, network stability rate, delay and routing overhead than old existing energy efficient based protocols. However, the problem of delivering / transferring data packets for dynamic network causes lowering of efficiency of the network due to misbehave attacks in this work not consider in security issues **[28]**. ***Baojun Huang et al, (2015)*** proposed Efficient Remote User Authentication with Key Agreement Scheme Using ECC, technology evolution identity authentication in the network that is becoming more and more significant. Simulation results shows performance comparison of three different phases such as Registration phase, Login and authentication phase and Password change phase through network simulation 2, proposed scheme was much more secure and practical as the secure universal access control mechanism also increased delivery ratio and remaining energy then other existing schemes. The scheme suffers from offline password guessing attack and impersonation attack. Moreover, new scheme could not achieve perfect user privacy and encryption decryption will take more time to increase latency of the network **[29]**. ***Sengathir and Manoharan, (2015)*** they effectively are suggested isolated the selfish nodes from the routing path based on the exponential reliability coefficient. From the simulation results, it was evident that the proposed exponential reliability coefficient based reputation mechanism approach outperformed the existing packet conservation monitoring algorithm, proposed method achieve higher packet delivery ratio and throughput than existing methods, and also isolate 28% of selfish nodes from the routing path. However, new method not been consider presence of malicious node when attacked malicious node, path increase packet drop, average delay and remaining energy **[30]. *Parth Patel et al, (2016)*** proposed approach; Hybrid EAACK (HEAACK) is designed to tackle three of six of six weaknesses of watchdog scheme presence of malicious attacks. HEAACK is capable of finding the malicious nodes as compared with the existing scheme with different scenario through simulation. HEAACK was the proposed system which added cryptography mechanism giving a secure network and thus the rate of data manipulation and network overhead decreases. Moreover, the malicious node increases the network remaining energy, average delay and also key exchange problem has not been solved **[31]**. On other hand ***Muthurajkumar et al, (2017)*** suggested new secured routing protocol called Cluster based Energy Efficient Secure Routing Algorithm (CEESRA) in this paper which is energy efficient and uses cluster based routing in which the trust scores on nodes are used to detect the intruders effectively. This routing algorithm reduces the Denial of Service attacks more efficiently by using intelligent agents for effective decision making in routing. Simulation results show reduces energy consumption and routing delay. Although, proposed new system reduces throughput due to increasing packet loss because of attacks **[32]**.

Gautam, M. and Mahajan, A.R. (2017) was proposed new secure ad hoc on-demand multi-path distance vector protocol is extended called Dolphin Echolocation Algorithm for efficient communication in MANET. The performance analysis and numerical results show that our proposed routing protocol produces better packet delivery ratio, reduced packet delay, reduced overheads and provide security against vulnerabilities and attacks and also remaining energy is reduced due to finding multipath between source and destination **[33]**. Topology based dynamic protocol implemented by ***Jiann Shen et al, (2017)*** proposed new protocol named Organized Topology Based Routing (OTBR) to adapt to the environments mentioned above. It can be divided into two different situations: one is called the static organized topology using anti-pheromone and the other is called the dynamic organized topology using greedy algorithm. Simulation results show that OTBR achieved higher remaining energy and packet delivery ratio reduced delay when network size changes. Moreover, packet loss is increased when network size changes due to malicious attackers **[34]**. One of my best researches is **K.Thamizhmaran et al, (2017)** is proposed enhanced acknowledgement based research work EA3EAK. This work mainly focused to reduced routing conjunction during to detect malicious attacker and find alternate route with secure path communication, help with one of most accuracy hybrid cryptograph called MARS4 which combine RSA & MAJE4 cryptograph. MARS4 act as secure routing also reducing tine delay, utilization energy, increased packet delivery ratio and throughput with help of enhance adaptive 3 acknowledgement not only this merits solved key exchange issue. Moreover this concept not suitable for all the environments whenever mobility high automatically performances will be decrees **[35]**. Recent published energy efficient research work proposed by ***Neha et al, (2018)*** they designed clinched using directional antenna are to find destination location, antenna focusing, signal power and distance calculations. Simulation result show improved energy savings using re-configurable directional antennas and an associated algorithm. However, developed system increased packet drop due to misbehaviours **[36]**. On other hand, secure nonlinear chaotic encrypted energy aware adaptive watermarking system for wireless image sensor networks is proposed by ***Hamzah et al, (2018)*** the watermarking scheme embedding locations and mechanism are to be decided based on the conditions of the channel in order to ensure watermark security and energy efficiency of the designed system. Simulation results show higher throughput and delivery ration. However, weakness of above scheme delay and energy due to time of encryption and decryption **[37]**.

K. Anish Pon Yamini et al, (2019) proposed new energy efficient system called transition state MAC protocol compared with existing models static power consumption MAC protocol and dynamic power consumption MAC protocol that coordination to mobile devices that communicate among themselves with no information from administration. Mobile node and network lifetime will be increased due to energy efficient lifetime maximizing methods based on channel awareness in MANETs result in better performance of the networks until the node's energy is capable of handling control messages than old method. Performance of cooperative MAC protocol for both conserving node energy and to utilize available node and also reduces the total energy consumption minimum 14% than DPCMP and minimum 24% than SPCMP with traffic falls almost 45 than SPCMP and 27% than DPCMP. Although an isolate misbehaviour attack is still not overcome, slight increase in network overhead and also reduces remaining energy of mobile nodes **[38]**. On other hand ***K. Anish Pon Yamini et al, (2019)*** they proposed the cooperative physical layer network coding scheme, the requirement of energy transmission can be reduced. They implemented using two routing algorithms namely CCSPR and COSPNCR with efficient power aware routing method is proposed which distinguishes the capability of nodes by its residual battery power, and through the expected energy that spent in reliably data packets forwarding on a specific link. Thus energy consumption can be decreased and hence lifetime of a node can be improved. The conventional shortest path routing method on regular line and the grid line networks attains the gain of energy savings up to energy consumption rate can be decreased to 80% with help of efficient power aware routing. However, the authors have not considered the delay and packet droppers presence of malicious activities in MANETs **[39]**.

N.S. Saba Farheen and Anuj Jain, (2020) is discussed Predicting the mobile node position and routing based on predicted positions helps to establish routing path with much longevity. Most predictions approaches are based on the past locations of the node. In this work a node location prediction based on the temporal and spatial characteristics with respect to its neighbourhood is applied to estimate the probable locations using a hybrid model. Result analysis above routing protocol improved routing performance in lower packet conjunction. The multi path routing is fine tuned based on the spatial temporal results to improve the effectiveness and reliability of routing through network simulation 2, the packet delivery ratio was found to be higher in the proposed solution compared existing design, moreover remaining energy and malicious node detection and correction not considered **[40]**. On other hand ***Nobuyoshi Komuroa and Hiromasa Habuchi, (2021)*** developed effective nonorthogonal Code Shift Keying Spread Spectrum (CSK/SS) ALOHA design one of the normal random design that access routing protocol investigated for mobile ad hoc network without carrier sensing function techniques. Result of above system to improve throughput and delay under MANET environment with one of the multilevel modulation systems for the spread spectrum technique with increasing the number of bits per frame. Proposed method numerical results show than Mos=8 and Mcon=3 achieved the highest throughput, combination Mos=8, Mcon=4 and Mos=32, Mcon=1 than existing spread ALOHA method. Although conclude from the numerical results that the new nonorthogonal system energy conception and security attack not considered above model **[41]**. ***V. Nivedita and N. Nandhagopal, (2021)*** most recently published research article focused trust calculation solving problem is going to proposed efficient multi-hop relay dependent better data transmission model is called Random Repeat Trust Computational (RRTC) that suggested technology provide better quality of mobile nodes and their services buffered the primary route and alternate to route for efficient data transmission. Research outcomes of this developed model to improve quality of network with help of random repeat trust computational method also increasing the security level because different stage of trust evaluation due to avoid the false trust issue so possible to detect attacker more than 30%. Even through malicious node detection and energy issues is did not considered **[42]**.

3. Research Outcomes

Wireless communication technologies have dramatically affected our data society due to dynamic movable device of mobile ad hoc network, among all users who wish to communicate between each other through mobile nodes.Limitation is a major motivation for many research initiatives whose goal is to establish a efficient architecture of group communications. Node mobility faces many of the challenges that an ad hoc network, mobility may result in frequent link breaks and utilize more energy; it can even lead to loss of packets. While it is very difficult to guarantee that the connectivity is maintained at all time in a dynamic and mobile environment below table 1 discussed merit and demerits many of existing research works.

Table 1 Merit and Demerits of above researchers

Author	**Protocols**	**Merits**	**Demerits**
Chan-Ho Min and Sehun Kim [8]	UBPCR	improves both CBR and CDR by estimating the transmit power	decrease network lifetime due to economic framework
Jyu-Yuan Lai and Chih-Tsun Huang [9]	ECC	speed and overhead & ECC cost effectiveness	packet drop and symmetric key encryption and malicious detection are not considered
William Chelton and Mohammed Benaissa [10]	ASIP	delivery ratio and throughput	Increased delay and reduced the security due to ECC design is very complex
Sunho Lim *et al* [11]	random cast	reduced broadcast packet, and saved remaining energy by 30% also increase delivery ratio	not suitable to other routing protocols average delay and packet drop will be increases when presence of misbehaviour
Peng Zhang *et al* [12]	P-Coding	minimal energy	misbehaviour will attack the

	LWE	consumption with less transmission	performance also P-coding reduce performance
Zhang Tao *et al* [13]	ECC&EFW-w NAF	FWNAF had the lowest total computation cost, reduced utilization energy and bandwidth	attacker will enter in network, average delay and packet drops increased with lower remaining energy
Venkateswaran *et al* [14]	Min-Total Min-Max	minimize the total energy consumed	suitable for low mobility, delay and used energy will be increased
Burmester and de Medeiros [15]	SEEP	increased remaining energy	ignore the topology exposure problem and routing overhead has not been considered
Jithra Adikari *et al* [16]	SDSM	faster than their widely used counterparts	energy consumption, security and delay have been not considered.
Morteza Nikooghadem *et al* [17]	KM&KD schemes	highest security level in transmission through all nodes	misbehave detection and routing overhead are still challenging issues
Manikandan and Sathyasheela [18]	ADCLI	achieve high performance of delivery ratio and low packet loss	delay increases, energy by way of network congestion increases
Karim El Defrawy and Gene Tsudik [19]	PFRSM	better privacy than the prior work, lower used energy	misbehaviour attacks increased and network life time also decreased
Ming-Yang Su [20]	ABHM	AMB reduce total packet loss by 10.05% than existing scheme	network delay and routing overhead will be increased
Nicola Costagliola *et al* [21]	MChannel-opt	better lifetime and delay also increased remaining energy	misbehaviour attacks and packet dropping attack based solutions do not address
May Zin Oo and Mazliza Othman [22]	SPMPRP	delay and reducing remaining energy consumption at a same network lifetime also decreasing	security aspects and packet loss and link breakage have not been considered in this work
Chun-Ta Li [23]	ASCPA	advanced smart card based password authentication with low computation cost	increased average delay when enter malicious attacker also network throughput significantly reduced
Wang *et al* [24]	ALCMAC	energy utilization of nodes is reduced with the possibility of link breakage minimized	large network cannot support new protocol due low security and network throughput will be reduced
Zijian Wang *et al* [25]	HHLSP	achieved around 32% energy efficiency	Energy models address only the hidden terminal issue
Hafizul Islamand and Biswas [26]	NPMA	more efficient, secure and flexible than	Congestion and link breakage are also not discussed
Abdulsalam Basabaaa *et al* [27]	A3ACK	Increases packet delivery ratio by 13.3% of high speed	network congestion has slightly increased and remaining energy will be increase
Gopinath and Nagarajan [28]	RERMR	better packet rate, stability rate, delay and routing overhead	lowering of efficiency of the network due to misbehave attacks is not consider
Baojun Huang *et al*	ERUA-KAS	more secure, increased	not achieve perfect user privacy

[29]		delivery ratio and remaining energy	and encryption decryption will take more time
Sengathir and Manoharan [30]	ERC	higher PDR and throughput and also isolate 28% of selfish nodes	malicious node, path increase packet drop, average delay and remaining energy
Parth Patel *et al* [31]	HEAACK	rate of data manipulation and network overhead decreases	malicious node increases the network remaining energy and average delay
Muthurajkumar *et al* [32]	EESRA	reduces energy consumption and routing delay	reduces throughput due to increasing packet loss because of attacks
Gautam, M. and Mahajan, A.R. [33]	DEA	better PDR, reduced packet delay, reduced overheads	attacks and remaining energy is reduced due to finding multipath
Jiann Shen *et al* [34]	OTBR	higher remaining energy and PDR reduced delay	packet loss is increased when network size changes due to malicious attackers
K. Thamizhmaran *et al*, [35]	EA3ACK	reducing tine delay, utilization energy, increased packet delivery ratio and throughput	not suitable for all the environments whenever mobility high automatically performances will be decrees
Neha *et al* [36]	Directional Antenna	improved energy savings using directional antennas	increased packet drop due to misbehaviours
Hamzah *et al* [37]	EAAWS	higher throughput, delivery ratio	Increased delay and remaining energy
K. Anish Pon Yamini *et al* [38]	TSMAC	network lifetime increased due to lifetime maximizing	increase in network overhead and also reduces remaining energy of mobile nodes
K. Anish Pon Yamini *et al* [39]	CPLNC	energy savings up to low energy consumption rate by 80%	delay and packet droppers presence of malicious activities
N.S. Saba Farheen and Anuj Jain [40]	PMNPR	improved routing performance in lower packet traffic and PDR	remaining energy and malicious node detection and correction not considered
Nobuyoshi Komuroa and Hiromasa Habuchi [41]	NCSKSS	improve throughput, delay and achieved the highest throughput	nonorthogonal system energy conception and security attack not considered
V. Nivedita and N. Nandhagopal [42]	RPTC	improve quality of network also increasing the security level	malicious node detection and energy issues is did not considered

4. Conclusion

The fast moving world demands seamless communication facilities, so former types of connectivity's like wired networks, radio waves are becoming obsolete. One of the recent developments in the world of communication technology is the use of MANET which was initially developed for military applications. The rapid use of MANET has results in the identification of several problems. Although the widespread deployment of MANET is still years away, the research in this field continues being very active and imaginative. In this paper, we have review and current surveyed last 15 years leading reputed articles with leading researcher ideas with challenges and more research issues identified in MANET. In this survey is very useful for many researchers in the field of MANET, very well know the above all issues but energy is one of domination issue in mobile ad hoc network. Our future research work is core issues of secure and power aware/energy efficient routing.

Acknowledgment

We would like to thank above researchers and respected internal expected reviewers who give their valuable review comments with suggestions for updating to improve quality of the paper. We would like to thank authorities of the estimated Annamalai University, Cuddalore, Tamilnadu, India and Government College of Engineering, Theni, Tamilnadu, India.

Reference

[1] Perkins, C. and Royer, E. "Ad hoc On-Demand Distance Vector Routing", *Second IEEE Workshop on Mobile Computing Systems and Applications,* February, 1999, pp. 1–11.

[2] RCF 2501 – "Mobile Ad hoc Networking (MANET): Routing Protocol Performance Issues and Evaluation Considerations", *Network Working Group,* Washington, January 1999.

[3] Royer, E. and Toh, C. "A Review of Current Routing Protocols for Ad hoc Mobile Wireless Networks", *IEEE Transactions on Personal Communication,* Vol. 4, No. 2, 1999, pp. 46–55.

[4] Grossglauser, M. and Tse, D. "Mobility Increases the Capacity of Ad hoc Wireless Networks", *IEEE Transactions on Networking,* Vol. 10, No. 4, 2002, pp. 477–486.

[5] Mohapatra, P., and Krishnamurthy, S., "Ad hoc Networks: Technologies and Protocols", First edition, *Springer,* 2004.

[6] Wu, J. and Dai, F. "Efficient Broadcasting with Guaranteed Coverage in Mobile Ad hoc Networks", *IEEE Transactions on Mobile Computing,* Vol. 4, No. 3, 2005, pp. 259–270.

[7] Chan-Ho Min, and Sehun Kim, "On-Demand Utility-Based Power Control Routing for Energy-Aware Optimization in Mobile Ad hoc Networks", *Wireless Personal Communication*, Vol. 41, No. 2, 2007, pp. 259–280.

[8] Jyu-Yuan Lai, and Chih-Tsun Huang, "Elixir: High-Throughput Cost-Effective Dual-Field Processors and the Design Framework for Elliptic Curve Cryptography", *IEEE Transactions on Very Large Scale Integration Systems,* Vol. 16, No. 11, 2008, pp. 1567–1580.

[9] William Chelton, and Mohammed Benaissa, "Fast Elliptic Curve Cryptography on FPGA", *IEEE Transactions on Very Large Scale Integration Systems,* Vol. 16, No. 2, 2008, pp. 198–205.

[10] Sunho Lim., Chansu Yu., and Das, C.R., "Random Cast: An Energy-Efficient Communication Scheme for Mobile Ad hoc Networks", *IEEE Transactions on Mobile Computing,* Vol. 8, No. 8, 2009, pp. 1039–1051.

[11] Peng Zhang., Chuang Lin., Yixin Jiang., Yanfei Fan., and Xuemin Shen., "A Lightweight Encryption Scheme for Network-Coded MANETs", *IEEE Transactions on Parallel & Distributed Systems,* Vol. 24, No. 4, 2009, pp. 1-6.

[12] Zhang Tao., Fan Mingyu., and Zheng Xiaoyu, "Secure and Efficient Elliptic Curve Cryptography Resists Side-channel Attacks", *Journal of Systems Engineering and Electronics,* Vol. 20, No. 3, 2009, pp. 660–665.

[13] Venkateswaran, A., Sarangan, V., La Porta, T.F., and Acharya, R., "A Mobility-Prediction-Based Relay Deployment Framework for Conserving Power in MANETs", *IEEE Transactions on Mobile Computing,* Vol. 8, No. 6, 2009. pp. 750–765.

[14] Burmester, M. and de Medeiros, B. "On the Security of Route Discovery in MANETs", *IEEE Transactions on Mobile Computing,* Vol. 8, No. 9, 2009. pp. 1180–1188.

[15] Jithra Adikari., Vassil S. Dimitrov., and Laurent Imbert., "Hybrid Binary-Ternary Number System for Elliptic Curve Cryptosystems", *IEEE Transactions on Computers,* Vol. 60, No. 2, 2010, pp. 254-265.

[16] Morteza Nikooghadam., Ali Zakerolhosseini., and Mohsen Ebrahimi Moghaddam., "Efficient Utilization of Elliptic Curve Cryptosystem for Hierarchical Access Control", *Journal of Systems and Software,* Vol. 83, No. 10, 2010, pp. 1917–1929.

[17] Manikandan, T. and Sathyasheela, K.B. "Detection of Malicious Nodes in MANETs", *Proceedings of 2010 IEEE International Conference on Communication Control and Computing Technologies,* India, Oct 2010, pp. 788-793.

[18] Karim El Defrawy, and Gene Tsudik, "Privacy-Preserving Location-Based On-Demand Routing in MANETs", *Journal on Selected Areas in Communications,* Vol. 29, No. 10, 2011, pp. 1926-1934.

[19] Ming-Yang Su, "Prevention of Selective Black Hole Attacks on Mobile Ad hoc Networks Through Intrusion Detection Systems", *Computer Communications,* Vol. 34. No. 1, 2011, pp. 107–117.

[20] Nicola Costagliola., Pedro Garçia Lopez., Francesco Oliviero., and Simon Pietro Romano., "Energy and Delay Efficient Routing in Mobile Ad hoc Networks", *Mobile Network Application,* Vol. 17, No. 2, 2011, pp. 281–297.

[21] May Zin Oo, and Mazliza Othman, "Analytical Studies of Interaction between Mobility Models and Single-Multi Paths Routing Protocols in Mobile Ad hoc Networks", *Wireless Personal Communication,* Vol. 64, No. 2, 2012, pp. 379–402.

[22] Chun-Ta Li "A New Password Authentication and User Anonymity Scheme Based on Elliptic

Curve Cryptography and Smart Card", *IET Information Security,* Vol. 7, No. 1, 2013, pp. 3–10.

[23] Wang, X. and Li, J. "Improving the Network Lifetime of MANETs Through Cooperative MAC Protocol Design", *IEEE Transactions on Parallel and Distributed Systems,* Vol. 99, No. 1, 2013, pp. 1-11.

[24] Zijian Wang., Eyuphan Bulut., and Boleslaw K, Szymanski. "Energy-Efficient Location Services for Mobile Ad hoc Networks", *Ad hoc Networks,* Vol. 1, No. 1, 2013, pp. 273-287.

[25] Hafizul Islam, S. K. and Biswas, G. P. "Dynamic ID-based Remote User Mutual Authentication Scheme with Smartcard Using Elliptic Curve Cryptography", *Journal of Electronics,* Vol. 31, No. 5, 2014, PP. 473-488.

[26] Abdulsalam Basabaaa., Sheltamia, Tarek., and Shakshuki, Elhadi. "Implementation of A3ACKs Intrusion Detection System under Various Mobility Speeds", *Proceedings of 5th International Conference on Ambient System, Networking Technologies,* Hasselt, Belgium, June 2014, pp. 571–578.

[27] Gopinath, S and Nagarajan, N. "Energy Based Reliable Multicast Routing Protocol for Packet Forwarding in MANET", *Journal of Applied Research and Technology,* Vol. 13, No. 3, 2015, pp. 374–381.

[28] Baojun Huang., Muhammad Khurram Khan., Libing Wu., Faha, T., Bin Muhaya., and Debiao He "An Efficient Remote User Authentication with Key Agreement Scheme Using Elliptic Curve Cryptography", *Wireless Personal Communications,* Vol. 85, No. 1, 2015, pp. 225-240.

[29] Sengathir, J. and Manoharan, R. "Exponential Reliability Coefficient based Reputation Mechanism for Isolating Selfish Nodes in MANETs", *Egyptian Informatics Journal*, Vol. 16, No. 2, 2015, pp. 231–241.

[30] Parth Patel., Rajesh Bansode., and Bhushan Nemade., "Performance Evaluation of MANET Network Parameters Using AODV Protocol for HEAACK Enhancement", *Proceedings Of 7th International Conference on Communication, Computing and Virtualization,* Mumbai, March 2016, 932-939.

[31] Muthurajkumar, S., S. Ganapathy, S., M. Vijayalakshmi, M., and A. Kannan, A., "An Intelligent Secured and Energy Efficient Routing Algorithm for MANETs", *Wireless Personal Communication,* Vol. 96, No. 2, 2017, pp. 1753-1769.

[32] Gautam, M. and Mahajan, A.R. "A Secure and Trust based On-demand Multipath Routing Scheme for Self-organized Mobile Ad hoc Networks", *Wireless Networks,* Vol. 23, No. 8, 2017 pp. 2455-2472.

[33]Jian, shen., Chen, Wang., Anxi, Wang., Xingming, Sun., Sangman, Moh., and Patrick, C.K.Hung., "Organized Topology based Routing Protocol in Incompletely Predictable Ad hoc Networks", *Computer Communication,* Vol. 99 No. 1, 2017, pp.107-118.

[34] K.Thamizhmaran, M.Anitha and Alamelunachippan "Performance Analysis of On-demand Routing Protocol for MANET Using EA3ACK Algorithm", *International Journal of Mobile Network Design and Innovation,* Vol. 7, No. 2, 2017, pp. 88-100.

[35] Neha, k., Rohit, K., and Rohit, B., "Energy Efficient Communication Using Reconfigurable Directional Antenna in MANET", *Procedia Computer Science,* Vol. 125. No. 2, 2018, pp. 194-200.

[36] Hamzah, A., Mohammad Alsalamin, M., Abdallah, J., Mamoun, M., and Khalid, A.D., "A Secure Energy-Aware Adaptive Watermarking System for Wireless Image Sensor Networks", *Proc. 15th IEEE International Multi-Conference on Systems, Signals & Devices, 2018,* pp. 86-97.

[37] K. Anish Pon Yamini, K. Suthendran and T. Arivoli, "Enhancement of Energy Efficiency using a Transition State MAC Protocol for MANET", *Computer Networks,* Vol. 155, No. 1, 2019, pp. 110-118.

[38] L. Femila and M. Marsaline Beno2, "Optimizing Transmission Power and Energy Efficient Routing Protocol in MANETs, *Wireless Personal Communication,* Vol. 106, 2019, pp. 1041-1056.

[39] N.S. Saba Farheen and Anuj Jain "Improved routing in MANET with optimized multi path routing fine tuned with hybrid modelling", *Journal of King Saud University Computer and Information Sciences,* Vol. 32, No. 6, 2020, pp. 700-708.

[40] Nobuyoshi Komuroa and Hiromasa Habuchi, "Nonorthogonal CSK/SS ALOHA system under MANET environment", *The Korean Institute of Communications and Information Sciences,* Vol. 7, No 3, 2021, pp. 78-84.

[41] V. Nivedita and N. Nandhagopal, "Improving QoS and Efficient Multi-hop and RELAY based Communication Frame Work Against Attacker in MANET", *Journal of Ambient Intelligence and Humanized Computing,* Vol. 12, No. 3, 2021, pp. 4081-4094.