International Journal of Engineering and Advanced Technology (IJEAT)
ISSN: 2249-8958 (Online), Volume-8 Issue-6, August, 2019

Contemporary Compendium of Conventions (CCC) in MANET

Purushottam G, Chilveri, M. S. Nagmode

Abstract- Incessantly a self configuring network for mobile devices known as Mobile Ad hoc Network (MANET) are associated wirelessly .In significant networks, this design might perhaps enforce increased computational costs owing to the costly credentials chaining overheads that would not adapt for ad-hoc applications with increased nodes. Here a survey is carried out to express a view on the secure and authentic MANET systems. The literature reviewed is on different and diverse techniques of related to MANET systems. Reviews of 65 papers is presented and stated the significant analysis. At first the analysis depicts various attacks that are contributed in different papers. Subsequently ,various measures like security, cost, simulation time etc are also analyzed. It analyses the encryption method also that is exploited in each paper. This paper further gives an insight regarding the tools adapted ,chronological review and performance achievements in each case. At the end the review extended for the different research issues to investigate further research on secure and authentic MANET system

Keywords—MANET; Authentication Protocols; Security; Attacks; Encryption; Research Gaps

Nomenclature

Acronyms	Descriptions
DoS	Denial of Service
ECC	Elliptic Curve Cryptography
CA	Certification Authority
e2e	end-to-end
PHSs	Personalized Healthcare Systems
CA	Certified Authority
IBBE	Identity-Based Broadcast Encryption
FCS	Fuzzy Commitment Scheme
BSG	Bayesian Signalling Game
CBDS	Cooperative Bait Detection Scheme
LKH	Logical Key Hierarchy
GS	Group Signature scheme
TCP	Transmission Control Protocol
PCA	Principal Component Analysis
DTD	Direct Trust-based Detection
DWCA	Distributed Weighted Clustering Algorithm
SCEEP	Secure Clustering and force Efficient Protocol
DHK	Diffie-Hellman key
DCA	Digital Cross Algorithm
OLSR	Optimized Link State Routing
ACO-CBRP	Ant Colony Optimization based Clustered based Routing Protocol
DTQCAR	Dynamic multi-stage Tandem Queue modeling-based Congestion Adaptive Routing
PDR	Packet Delivery Ratio
ZRP	Zone Routing Protocol
CLPKM	Certificate-Less on-demand Public Key Management
CG	Certificate Graph
HEAACK	Hybrid Enhanced Adaptive Acknowledgement
HEAP	Hop-by-hop Efficient Authentication Protocol
FPNT	Fuzzy Petri Net
MDSR	Modified Dynamic Source Routing Protocol
LIPG	Lagrange Interpolation Polynomial Group
CTPKM	Composite Trust-based Public Key Management
TPR	True Positive Rate
FPR	False Positive Rate
PKC	Public key Cryptography
RSA	Rivest–Shamir–Adleman
AES	Advanced Encryption Standard
IS	Information System

I. INTRODUCTION

MANET [66] [67] exists as one of the vital requirements in the day to day life. Mobile equipment in a MANET are available in several sizes and shapes with varying receiving and sensing capabilities, and they are capable to function across a number of frequency bands. In MANET [68] [69], the mobile equipments are known as nodes that comprise specific features like, mobility, dynamic topology, resource restraint and they are infra structureless. In the MANET surrounding [70] [71] [72], the entire nodes could be able to merge and depart the network by its own, and the communication takes place among one another with the lack of infrastructure. Moreover, the communication is dependent on the nodes [73], which are integrated to transmit packet known as, multi-hop communication. Besides the node mobility, it could pave the way to the deviation in topology, and it also allows low connectivity with one another. Because of the dynamic nature and infrastructure-less property of the MANET [74] [75] surroundings, there exist numerous limitations as mobile devices and nodes could transfer liberally in MANET [76] [77] namely, vulnerabilities of impersonation, modification of sensitive e-commerce

Revised Manuscript Received on October 30, 2019.
* Correspondence Author
Purushottam G Chilveri*, Research Scholar department of E&TC ZCOER ,
Savitribai Phule Pune University , Pune, India.
Dr. M.S. Nagmode, E&TC, Savitribai Phule Pune University, Pune, India.

dealings, eavesdrop of communications channels, DoS, etc. by malevolent insiders [78] [79] [80].

With the enhancement of wireless networks, a user can access the data collected by sensors at in all places, and authentication is a significant concern in the network security [81] [82] [83]. Moreover, a revolutionary efforts on user authentication for sensor nodes by deploying smart card was implemented, and it generated several works [84] [85]. Also, it requires the features of key agreement ,mutual authentication, and anonymity of user, and in addition, it endures from particular attacks like denial of service, password guessing and gateway bypassing attacks and sensor node captivation. ECC was also exploited for authentication purpose in MANET's [86], in which it offers superior security characteristics with reduced performance cost when evaluated with traditional public cryptosystem. On the other hand, these techniques could not accomplish mutual authentication and do not maintain the dependencies on key agreement and user anonymity [87]. Some conventional networks, centralized confidential [88] [89] authorities provide a private security known as the TTP. Typically, there functionality is to ascertain superior trust relationships between participants. In common, a TTP plays a major role in CA, which offers certificates as for public-key authentication. Accordingly, in various setups, the well-established credit relationships are deployed to decide whether other user is responsible for a specific class of activities. However, the actuality is that these solutions are based on a centralized authority that makes them inappropriate for MANET's [90] [91].

In This paper contributes a review related to secure and authentic MANET systems. The survey focuses on various techniques and protocols exploited in MANET sector. Accordingly, the types of attacks, encryption methods, and the adopted tools in each of the adopted papers are reviewed. Moreover, the performance measures and the corresponding achievements are analyzed and chronological review of the adopted works associated with MANET are presented. Finally, the research gaps and issues related to the MANET systems are portrayed in brief. The paper is arranged as follows. In Section no II the related works is discussed done under this topic. Section no III demonstrates the authentication algorithm on MANET with performance analysis, and section IV depicts the assessment on attacks, tools and encryption methods in each work. Accordingly, section V portrays the research gaps and challenges, and section no VI concluding remarks of the paper is presented.

II. LITERATURE REVIEW

In 2008, Yeun *et al.* [1] have authenticated group protocol for e2e security in the MANET surroundings. It also recognizes malevolent hackers by means of the confidential authority who only engages in the protocol if the falsification has been taken place. In 2015, Hamouid and Adi [2] has established a diverse approach by means of ID-dependent cryptography. The presentation and security analysis of the suggested method reveals its effectiveness when distinguished with conventional PGP-like systems. In 2017, Srinivas *et al.* [3] have suggested a novel authentication scheme for WSNs by means of biohashing. Throughout the informal security examination, the suggested method was proved to be secure in opposition to the recognized attacks for authentication protocols.

In 2017, Xiong Li *et al.* [4] has presented a method for nodes in IoT surroundings as three-factor authentication in which fuzzy commitment method was exploited to manage the biometric information of user. On compared over various associated assignments, the implemented method was found to be more appropriate for IoT surroundings. In 2017, Wu *et al.* [5] has implemented a robust authentication for WSNs that faces the widespread security necessities and eradicates the tracking of user details from attackers. Along with the assessment to numerous current approaches and simulation by NS-3, the implemented method was found to be appropriate for PHSs. In 2017, Shyamala and Valli [6] have distributed an authentication protocol for WSNs using mapping function. The computation measures like, communication and message cost, and performance overhead were measured. In 2017, Wu *et al.* [7] have introduced the system of Biswas and Amin, which has exposed formerly unidentified susceptibilities in the approach. Moreover, the security of the implemented method by means of Proverif was presented in addition to the analysis of the superior performance of the system by means of NS-2 simulation. In 2016, Amin and Biswa [8] have illustrated a number of security limitations of the Turkanovic *et al.* [92] protocol. The performance and security investigation makes the scheme more proficient that the suggested policy can be put into practice in real-life application. In 2009, Gil and Goya [9] have suggested a novel self-organized and distributed authentication system for MANETs. Remarkable conclusions were attained from an investigation of simulation analysis such as decreased resources and improved flexibility and improved security in various circumstances. In 2016, Nguyen *et al.* [10] have presented the network trust, and mobility representations, which were rather standard and permit us to attain the delay constituent persuaded only by the security links along a path. Specifically, from both simulations and investigational results, it was identified that, for sparse and largely associated networks, the delay occurred by security connections was very least when distinguished with the entire packet delay. In 2017, Smith *et al.* [11] have introduced a new secure framework known as SUPERMAN. The results of SUPERMAN obtained from simulation when distinguished with, SAODV SOLSR, and IPsec was offered to reveal the appropriateness of the suggested models for security in wireless communication. In 2012, Q. Guan *et al.* [12] have introduced a scheme that concerns on topology and authentication control problems. The simulation outcomes have revealed that the proposed technique can considerably develop throughput in MANETs. In 2011, H. Tang *et al.* [13] has developed a strategy to acquire the best possible method of merging incessant user IDSs and authentication in a distributed approach. Simulation outcome was offered to demonstrate the performance and efficiency of the implemented approach. In 2011, P. Mason *et al.* [14] has established a scheme that offers distributed intrusion detection and combined authentication in MANETs. Moreover, in 2009, J. Liu *et al.* [15] have suggested a design, where multimodal biometrics was deployed for uninterrupted identity establishment, and malicious node detection was designed for sensor nodes to identify the state of security of the system.

Finally, the wide-ranging experimentations have demonstrated the effectiveness of the implemented system.
In 2015, Ghosh *et al.* [16] have presented a low-overhead identity-dependent distributed scheme for secure distribution of addresses(IP) to authenticated sensor nodes of an administered MANET. The final experimental analysis has illustrated that the suggested method performs well with related conventional protocols even with integrated security systems. In 2014, Yang [17] had been suggested a lightweight IBBE approach to meet with security demands as well as the communication overhead of mobile ad hoc network. The experimental results have shown that it has achieved high efficiency and gained high security against chosen cipher text attack. In 2011, Vilhekar and Jaidhar [18] introduced an efficient modified authentication protocol using ECC on MANET for Virtual Subnets. From the experimental results, it could be proved that the computational complexity had been reduced when compared with RSA with the same level of security also produced shorter key size. In 2014, Sheikh *et al.* [19] have adopted a model that concerns on offering efficient and secure real-time voice transmission in MANET surroundings, which remains as a challenging issue. Finally, it was found that novelist's cooperative mesh-dependent MANET execution could be exploited for speedily deployable VoIP transmission with proficient and survivable dynamic network. In 2014, Jian *et al.* [20] have stated that the detection of malicious nodes that launches gray hole as a major demand. The authors have designed a DSR-based routing approach for resolving these issues, and it was named as CBDS. The outcomes of simulation have reviewed that the proposed CBDS was more effective when compared to other security protocols with respect to routing overhead and packet delivery ratio. In 2014, Vijaya et al. [9] have analyzed the behavior and effect of JellyFish attack on TCP-related MANETs. The simulation outcome has reviewed the performance of proposed model under EXata-Cyber simulator with respect to throughput of network, network overhead, and delay. Further, DTD was also developed for removing the JellyFish node. In 2015, Marjan *et al.* [22] had evaluated the vulnerabilities of security under BeeAdHoc, and have developed a security model namely FBeeAd-Hoc that uses the fuzzy set theory as well as digital signature. Finally, the experimental outcome has revealed the performance of proposed work in terms of encountering various threats when distinguished with AODV schemes. In 2014, Saju and philip [23] had developed a model for MANET of key management which is self-organized. The developed architecture comprises of unattched coordinator node, ordinary mobile sensor nodes as well as servers. Here, the nodes that subjected the certificates were evaluated through the EVRC. In 2011, Naveen *et al.* [24], have presented and recognized a distributed weighted clustering scheme for MANETs. The analysis outcomes demonstrate that the presented methodology algorithm performs better than the conventional DWCA scheme. In 2013, Shobana *et al.* [25] had established novel mechanism known as SCEEP for dividing the MANET into a group of two hop clusters, in which a part of node belongs to a single cluster. For balancing the supply consumption, leader election based scheme was exploited for reducing the overall resource costs by means of DHK switch over the system. In 2012, Sandip *et al.* [26] have proposed a secure MANET system, which was more vulnerable to attacks than a disconcerted arrangement that includes insufficient physical sanctuary, power restrained functions and so on. This predictable mechanism would establish the identity of the node and assure the protection of meaningful routing of data in MANETS. In 2013, Rajesh *et al.* [27], have modified the security objectives that has to be attained and moreover, it exploits the cryptographic algorithms namely, distributed cryptography, to offer a highly accessible and key management. Furthermore, here they endeavor to present more security by merging in collaboration models. In 2014, Edna *et al.* [28] have analyzed a model based on security, which was offered by two approaches, namely DCA and the ECC. Here, the security was enhanced at various levels that defer sturdy malicious attacks. In 2013, Gimer et al. [29] have stated that in OLSR networks, the generation of partial link-state data and flooded were exclusively done via MPRs. Finally, they have conducted the simulation, and the results have shown the betterment of the proposed system. In 2017, Teng *et al.* [30] have spotted that the influenced nodes could automatically trace back on finding which node triggers originally. The authors have continued the process in an iterative manner for tracking the fault till they have deduced the damaged log entry. The NetPro provenance could aid the explanation on why this event was abnormal or why such a log entry was damaged. In 2017, Satheesh *et al.* [31] have described the enhanced model for the secured transmission through the initiation of ACO-CBRP. They have finally performed the assessment of performance under various metrics including energy, overhead cost and packet delivery ratio by NS-2 simulator. In 2017, Vadhana *et al.* [32] have developed a defense over Sybil attacks in MANET. Every random familiar node has a RSS values of table that were assessed from the preceding message exchanges on zone for detecting the Sybil attack. The simulation results have shown the presented scheme minimizes the packet drop, thereby maximizing the delivery ratio. In 2018, Usman *et al.* [33] have implemented a new scheme, termed as QASEC for attaining improved throughput by protecting e2e communication in MANETs. QASEC was proficient in opposition to diverse attacks and has a much-improved behavior with regards to related costs, like, encryption, key generation and storage, and communication. In 2016, Sarkar and Raja *et al.* [34] have implemented an energy-efficient and secure multipath routing model depending on a Markov chain for MANETs. The arithmetical results illustrate that the implemented protocol attains noteworthy performance with respect to energy utilization, security, and throughput of routing models. In 2017, Amuthan *et al.* [35] have implemented a DTQCAR depending on the evaluations of average threshold congestion level. On the basis of stochastic constraints, neighbours effort to locate a different path to the destination, which was free of congestion. Finally, the execution outcomes demonstrate that the presented model offers better outcomes in terms of throughput and PDR. In 2015, Dilli *et al.* [36] have executed the ZRP, which was a fusion based MANET protocol and it was simulated using hashing algorithm for data reliability and substantiation of the data that was being transmitted. The established scheme provides an advanced PDR and throughput; however at the cost of the higher e2e delay. In 2009, Nakayama *et al.* [86] have introduced a secure MANET depending on a dynamic learning process.

MANETs were generally created devoid of any chief infrastructures. Finally, the simulation outcomes concerning two varied networks in dimension demonstrate the efficiency of the adopted models. In 2012, Lacey *et al.* [38] have analyzed the application, theory, and outcomes of RIPsec structure, which offers security for a MANET functioning in an aggressive atmosphere. Moreover, the adopted RIPsec approach was examined to reveal its robustness in opposition to a numerous renowned attacks against MANETS. In 2014, Maity *et al.* [39] have offered a self-organized CLPKM protocol that intends at offering the developed verification paths for verification purposes. An extended strand space design was also exploited and analyzed for revealing the exactness of the protocol. The systematic simulation and the performance outcomes substantiate the efficiency of the offered protocol. In 2018, Yaser *et al.* [40] have recommended a model that necessitates a negligible alteration to the routing protocol, and a negligible network overhead. In addition, the performance of the recommended method was assessed, and the attained results point out the supremacy of the anticipated method. The implemented algorithm improves the delivery proportion, and furthermore, it improves the dropped package rates. In 2016, Banoth *et al.* [41] have presented a system based on CA as numerous trust-dependent solutions in MANETs were relied on public key credentials. Further, a trust based process was evaluated and accordingly, the harmful nodes were eliminated. In 2016, Srinivas *et al.* [42] have suggested a model based on MANET that was a compilation of mobile nodes, which interacts with each other, thus forming a wireless network, wherein every sensor node holds a role as router and data packets were forwarded to the desired node. At last, it was revealed how the adopted method alleviates the attacks on nodes. In 2011, Qing *et al.* [43] have adopted a CG-based model in MANET. As MANETs does not include common infrastructure, and it was complicated to offer services on identity establishment. Finally, the efficiency and viability reveal the efficiency of protocol by simulations. In 2007, Nikos *et al.* [44] have presented a MANET-based on the security constraints. Here in this work, the nodes interact between one another by means of wireless radios and functions based on the peer-to-peer network representation. Further, the performance of several protocols that were dependent on challenge-response models were offered from simulation outcomes. In 2016, Parth *et al.* [45] have introduced MANETs based model, which was susceptible to malevolent attackers owing to their wide allocation and open medium. HEAACK was also introduced in this work that adds cryptography method thus offering a protected network and accordingly the rate of network overhead and data manipulation decreases. In 2007, Yuh *et al.* [46] have implemented MANETs as a tremendous technology, which was flexible for establishing in wireless communications. The set-up of two-tier substantiation could avoid interior and exterior attacks, together with black holes and so on. In 2016, Barbara *et al.* [47] have introduced a secure protocol that influences on online social network connections assist users for implementing their trust preference to formulate a money transfer in an uncomplicated way. At last, the investigational results have illustrated the efficiency of the introduced work. In 2008, Akbani *et al.* [48] have suggested an approach to conflict attacks from exterior nodes, and packet identification in wireless networks was analyzed, and an efficient hop-by-hop protocol for identity establishment known as HEAP was proposed. In addition, metrics such as throughput, latency, PDR, memory and CPU exploitation were measured, and it was demonstrated that HEAP executes very well when evaluated to erstwhile schemes. In 2015, Tan *et al.* [49] have introduced a trust analysis based on FPNT model for assessing trust values of MANET nodes. At last, the outcomes illustrate that FPNT-OLSR was very effectual in introducing protected paths. It moreover executes improved performance than conventional models with respect to PDR, overhead and latency. In 2015, Huihua *et al.* [50] have established a technique based on MANETs, for tacking with issues related with unpredictable wireless medium, lack of communications and nodes mobility, thus offering a key establishment scheme in these distinctive network surroundings. In 2015, Sandeep and Satheesh [51] have introduced three diverse network conditions and feasible solutions. Further, an improved design was studied which gives improved outcomes at diverse mobility states with higher rate of PDR. In 2010, Drira *et al.* [52] have suggested a model in MANET based on common key for a group for clustering system. The executed outcomes demonstrate that the suggested solution was proficient and characteristically adapted to the movement of nodes. In 2015, Casado *et al.* [53] have presented a representation for forwarding data in MANETs that was exploited for identifying malevolent packet dropping behaviors. It was remarkably known about the light weightiness and simplicity of the presented methodology. In 2008, Chun *et al.* [54] have adopted a deniable electronic voting substantiation procedure for MANETS that congregates the necessary availabilities of a protected e-voting arrangement. Finally, the presented algorithm offers the capability for better substantiation. In 2013, Mitrokotsa and Christos [55] have examined an approach that appropriately exploits classification approaches in distortion recognition for MANETs. The outcomes point out that the adopted model could be exploited efficiently and it also proves that sequential approaches can include a small, but noteworthy impact for particular classifiers types. In 2015, Sindhuja *et al.* [56] have presented a mobility-based model known as efficient flooding approach for attaining the trust convergence with higher probability. Finally, this approach has offered a handy trade-off among cost, delay, PDR and trust proportion that leads to minimization in uncertainty. In 2014, Mohanapriya and Ilango [57] had modeled a MDSR protocol to identify and avoid the black hole attacks. Here, the modelled method was authenticated to prove the efficiency of implemented intrusion recognition system. In 2012, Hung *et al.* [58] have presented a scheme regarding the routing collusion and misbehavior attack in MANETs, which were the major subjects of this work. Finally, the security examination and simulation outcomes were offered to assess the NACK performance. In 2009, Feng *et al.* [59] have implemented an approach that comprises of two phases, where, the initial stage was to construct a key pre-sharing approach depending on LIPG and hash operation, and the subsequent stage chiefly handles with recovering key in a much secure approach. Finally, the investigational outcomes illustrate that this model can guarantee the MANET security surroundings with enhanced performance.

In 2011, Ghosh and Raja [66] had offered an ID based configuration approach, which could assign IP addresses securely to the certified hosts for a MANET devoid of transmitting over the whole network. In addition, the offered technique was capable to resolve the issues of network together with the departure and arrival of a host securely and efficiently. In 2016, Cho *et al.* [61] have presented a CTPKM with the objective of increasing the performance when extenuating the security susceptibility. Further, the analysis of CTPKM was demonstrated, and it performs both conventional trust-dependent and non-trust- dependent counterparts. In 2013, Cho and Ing [62] have presented and examined a trust management approach for a collection of communication systems, in which self-centred nodes subsists, and system survival was extremely significant to mission implementation. It was illustrated that the presented approach deploys the trade off among unselfish versus selfish behaviours and it performs better and promotes only the unselfish behaviours. In 2009, Rong *et al.* [63] have implemented a pyramidal security scheme in MANET environment based on security. Moreover, the performance evaluation reveals that the method of integrated tree key graph includes betterments when compared with its counterparts. In 2009, Saxena *et al.* [64] have modeled a secure MANET model, as it was necessary to cope with dynamic topology and membership securely and to bootstrap erstwhile significant security primal and services. Also, a novel method was presented, which permits any pair of nodes of MANET to introduce an on-the-fly secure interaction channel resourcefully. In 2014, Wang *et al.* [65] have adopted Game theory based model, which can offer a constructive tool to analyze the security issues in MANETs. Here, the adopted model was a fully disseminated approach and the simulation outcomes were offered to demonstrate the efficiency of the adopted technique.

III. AUTHENTICATION ALGORITHMS ON MANET WITH PERFORMANCE ANALYSIS

Algorithmic Analysis

Various MANET authentication schemes are reviewed in this work as shown in Fig 1, which comprises of several protocols. Accordingly, optimization algorithms include OLSR [19] ACO [31] [51] FBeeAdHoc [22] and Learning algorithms include FCS [4] FPNT [49] Naïve Bayes model [55]. Markov Decision algorithms was adopted in [13] [15] [34] and Clustering algorithms comprises of DWCA [24] SCEEP [25] ECGK [52]. The key exchange algorithms includes DHK [27] [64][62] LKH [50] [63] CTPKM [61]. AODV algorithms was adopted in [23] [26] [40] [43] [45] [53], Flooding algorithms was adopted in [29] [56] and CA algorithms was adopted in [41] [42]. Other miscellaneous protocols includes Burmester–Desmedt key protocol [1], Petersen's self-certified scheme [2], Biohashing [3], Two factor authentication scheme [5] [46], Bilinear mapping function [6], Amin and Biswas scheme[7], Timestamp method [8], GASMAN [9], Poissonization scheme [10], SUPERMAN [11], PCA [37], RIPsec [38], peer-to-peer model [44], HEAP [48] schemes. In addition, models like JATC scheme [12], Dempster-Shafer [14], SDRAC [16], IBBE scheme [5] [46], Trilateration Model [18], DSR [20], DTD method [21], Hashing Algorithm[28], Netpro [30], GS scheme [32], QASEC [33], BSG [35], DTQCAR [36], CLPKM [39], Tidal trust algorithm [47], E-voting protocol [54], NACK [58], LIPG [59], IDDIP [60] and Game theoretic Model [65] are also adopted in different contributions.

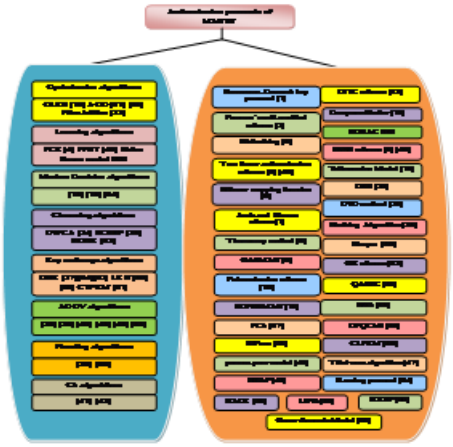

Fig. 1. Diagrammatic representation of the MANET authentication schemes

IV. PERFORMANCE ANALYSIS

The performance analysis of the adopted works is depicted by Table I. From the Table I, the number of nodes has been adopted in 18 papers that have contributed about 27.69% of the reviewed works, and the packet size was adopted in 7 papers that had offered about 10.77% of the entire contribution. Similarly, the total time has been adopted by 24 papers and transmission range has been adopted in 12 papers, which have provided about 36.92% and 18.46% of the reviewed works respectively. Moreover, throughput and latency have been implemented by 6 and 3 papers that contribute about 9.23% and 4.61% of the entire contribution. Accordingly, PDR, overhead, and energy have been adopted by 4, 4 and 4 papers, respectively that offers about 6.15%, 6.15% and 6.15% of the whole contribution. Also, Cost, e2e delay, Bandwidth and other measures have been adopted in 5, 6, 2 and 40 papers, which have offered about 7.69%, 9.23%, 3.08 and 61.54% of the whole contribution.

TABLE I. REVIEW ON VARIOUS PERFORMANCE MEASURES FOR AUNTHENTICATION IN MANET

Citations	Number of nodes	Packet size	Total time	Transmission range	Throughput	Latency	PDR	Overhead	Energy	Cost	e2e delay	Bandwidth	Others
[1]													✓
[2]										✓			✓
[3]								✓		✓			
[4]										✓			
[5]			✓									✓	
[6]			✓						✓				
[7]					✓						✓		
[8]													✓
[9]	✓		✓										
[10]													✓
[11]	✓												
[12]	✓				✓								
[13]			✓										
[14]													✓
[15]													✓
[16]	✓		✓			✓							
[17]			✓										✓
[18]													✓
[19]					✓								
[20]			✓										✓
[21]	✓		✓										✓
[22]					✓						✓		
[23]		✓	✓										
[24]	✓								✓				✓
[25]	✓	✓	✓										
[26]													✓
[27]													✓
[28]	✓		✓										
[29]	✓		✓	✓									
[30]			✓							✓			✓
[31]	✓							✓					
[32]		✓	✓	✓									✓
[33]										✓			✓
[34]					✓						✓		
[35]							✓						✓
[36]	✓	✓							✓				
[37]				✓									✓
[38]		✓	✓	✓									✓
[39]			✓	✓								✓	✓
[40]								✓					✓
[41]	✓	✓	✓										✓
[42]													✓
[43]			✓										✓
[44]													✓
[45]							✓	✓					✓
[46]											✓		
[47]											✓		✓
[48]					✓	✓							
[49]						✓							✓
[50]													✓
[51]							✓						✓
[52]	✓			✓									
[53]				✓									✓
[54]													
[55]				✓									✓
[56]			✓				✓						✓
[57]	✓		✓	✓									✓
[58]	✓	✓	✓	✓									
[59]											✓		✓
[60]			✓	✓									✓
[61]	✓		✓										✓
[62]			✓										✓
[63]													✓
[64]	✓												✓
[65]	✓								✓				

Maximum Performance

The maximum performance attained by each of the adopted papers is given by Table II. From the review, number of nodes adopted in [24] has attained a higher value of 500 and packet size adopted in [41] [58] has attained a higher value of 512 bytes. In addition, total time has attained a higher value of 20s, and it has been adopted by [32], and transmission range has attained a higher value of 250m, and it has been adopted by [29] [32] [38] and [40] respectively. Similarly, throughput, latency, and overhead have attained higher values of 18Mbit/s, 1.1s, and 28.31% and it has been adopted by [18] [49] and [40], correspondingly. The measures like energy, storage cost, e2e delay, and bandwidth have attained higher values of 100J, 50, 0.21KB, 24msec and 2mbps and they have been adopted in [36], [2], [34] and [5] respectively. Also, speed, PDR, probability, transmission delay, and TPR were exploited in [41] [45] [14] and [47], and they have acquired higher values of 25m/s, 0.92%, 1, 1650ms and 22%, correspondingly. In addition, FPR, voltage and key size have attained higher values of 83% and 571 bit, and they have been measured in [53] and [47] respectively.

TABLE II. ANALYSIS ON MAXIMUM PERFORMANCE OF THE REVIEWED WORKS

Sl. no	Performance measures	High achievements	Citations
1	Number of nodes	500	[24]
2	Packet size	512bytes	[41] [58]
3	Total time	20s	[32]
4	Transmission range	250m	[29][32] [38] [40]
5	Throughput	18Mbit/s	[18]
6	Latency	1.1s	[49]
7	Overhead	28.31%	[40]
8	Energy	100J	[36]
9	Storage cost	0.21KB	[2]
10	e2e delay	24msec	[34]
11	Bandwidth	2mbps	[5] [39]
12	Speed	25m/s	[41]
13	PDR	0.92%	[45]
14	Probability	1	[14] [15]
15	Transmission delay	1650ms	[47]
16	TPR	22%	[53]
17	FPR	83%	[53]
18	key size	571 bit	[47]

V. ASSESSMENT ON ATTACKS, TOOLS AND ENCRYPTION METHODS DEALS WITH AUTHENTICATION IN MANET

Analysis on Various Attacks

The analysis on various attacks contributed in authentication protocols in MANET is given by Fig. 2. From the analysis, spoofing attack was adopted in one contribution and man in middle attack, random attack and Sybil attack was offered by 2 contributions. In addition, impersonation attack, replay attack, insider attack, passive attack and security attack has been analyzed by 3 of the contributions. Moreover, black hole attacks, QoS attack, and other attacks have been offered by 7, 13 and 14 contributions respectively.

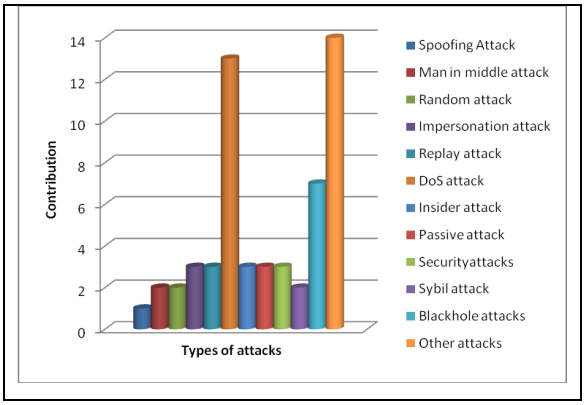

Fig. 1.Review on the various attacks of the adopted works

Review on Experimental Tools

The simulations of the reviewed works are done in various simulators like, MATLAB, AVIPSA, NS-2, NS-3, OMNET++, Linux, Qualnet 4.5, GloMosin, OPNET and so on. Accordingly, MATLAB was adopted in 6 papers that have offered about 11% of the total contribution, and AVIPSA was adopted in 2 papers that had offered about 4% of the entire contribution. Similarly, the NS-2 has been adopted by 20 papers and NS-3 has been adopted in 2 papers, which have provided about 39% and 4% of the reviewed works respectively. Moreover, OMNET++ and Linux have been implemented by 3 and 3 papers that contribute about 6% and 6% of the entire contribution. Accordingly, Qualnet 4.5, and GloMosin have been adopted by 5 and 3 papers that offers about 10% and 6% of the whole contribution. Consequently, OPNET has been adopted in 3 papers, which have offered about 6% of the whole contribution and in addition, various other tools were also adopted in the reviewed works.

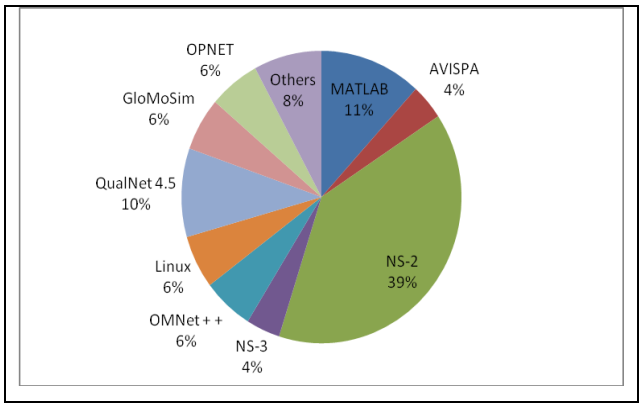

Fig. 2.Analysis on the adopted tools in the reviewed works

Review on the Encryption methods

The encryption techniques, namely, PKC, RSA, AES, Data Encryption Standard, ECC, digital signature and so on were adopted in each of the reviewed works is given by Fig. 3. Here, in the reviewed works, the PKC model has been adopted in 10 contributions, and RSA has been exploited as an encryption criteria in 7 of the reviewed works. Moreover, AES has been implemented in 4 of the adopted works, and digital signature was deployed by 2 of the reviewed works.

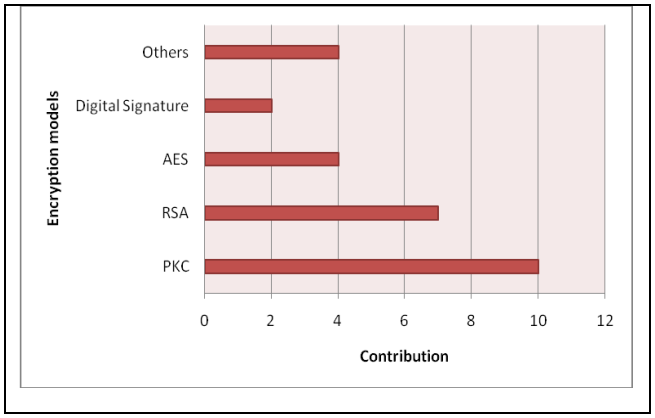

Fig. 3.Review on the adopted encryption methods

Chronological Review

Fig. 4 represents the chronological review and its contributions in percentage for subsequent years. This survey investigates many papers published in different years. Initially, 13 papers areconsidered from the year, 2007-2010.Then in the year 2011-2013 around 17 papers are published. Accordingly, 18 number of papers taken from the year 2014-2015 and the count of papers adopted in the year 2016-2018 was about 17.

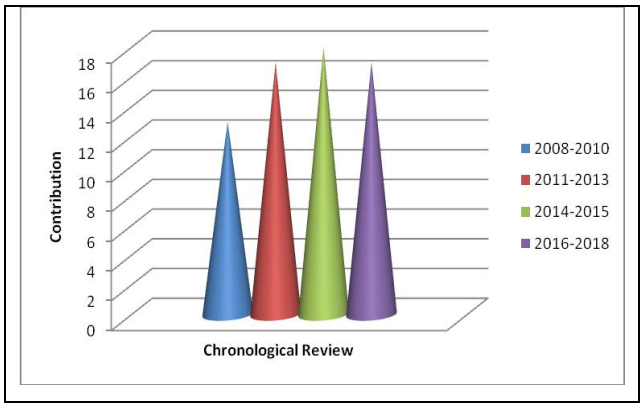

Fig. 4. Graphical representation of the chronological review

VI. RESEARCH GAPS AND CHALLENGES

Security is an essential feature of MANET. It comprises of numerous postulations that are funded sufficiently. In MANET the network operations namely, packet forwarding and routing is done in a self-organizing manner. That is why, security achievement in MANET remains a challenging task. Because of the unique features of MANET, their services have met up with several limitations. For secure MANET, transactions among these services have to be offered, i.e., without transactions, a security system may not be successful. Presenting a trade-off amongst such security services is dependent on network application; however, the complicatedness is to proffer services independently in MANET and providing an assurance to every service.

In addition, nodes are complimentary to shift arbitrarily; as a result, the network topology-that is typically multi-hop may perhaps vary rapidly at random instants. Therefore, it is essential for all pairs of neighboring nodes to combine in the routing crisis so as to evade numerous kinds of feasible attacks in the routing protocol. Thus, there is not such an obvious secure limit in the MANET that can be distinguished with the obvious line of defence in the conventional wired network. In addition, it lacks characteristic of key agreement, mutual authentication and user anonymity, and furthermore endures from certain attacks, like password guessing, gateway bypassing, and sensor node capture and DoS attacks. ECC was also exploited for two-factor authentication protocol in MANET's, in which ECC provides enhanced security characteristics with less performance cost when distinguished with conventional public cryptosystem. On the other hand, such methods could not attain mutual authentication, and does not sustain the operation of key agreement and user anonymity.

The security challenges in MANET also include channel vulnerability, i.e., wireless broadcast by medium permits easy message Injection and eavesdropping. Also, node vulnerability has to be concerned, where nodes do not function from physically protected places and thus easily it falls under attack. In addition, dynamic changes in network topology and security threat under the routing protocols have to be concerned more. Also, computational and power limitations prevent the use of complex encryption algorithms, which remains as a major security issue in MANET.

VII. CONCLUSION

This paper has presented a detailed review on secure and authentic MANET systems that were enumerated in the above sections. Here, various performance measures along with their better achievements were analyzed and described. Moreover, this survey analyzes the issues and complexities associated with security and authentication mechanisms on MANET. In conclusion,

- Different papers on MANET Authentication are reviewed and trivial analysis is declared on various algorithms.
- Analysis mainly focused on various attacks in secure and authentic MANET systems that were reviewed in this paper. Dos attack is most significantly used attack for the analysis and application specific attack is the second largest attack used .
- Subsequently, various adopted tools and encryption models are also analysed .
- The analysis also reviewed the performance measures and the corresponding achievements that were exploited in MANET systems.
- At last, various research issues on the features of secure and authentic MANET systems which can be useful for the researchers to accomplish further research are also presented.

REFERENCES

1. Chan Yeob Yeun, Kyusuk Han, Duc Liem Vo, Kwangjo Kim, "Secure authenticated group key agreement protocol in the MANET environment", Information Security Technical Report, vol. 13, no. 3, pp. 158-164, August 2008.
2. Khaled Hamouid, Kamel Adi, "Efficient certificateless web-of-trust model for public-key authentication in MANET", Computer Communications, vol. 63, pp. 24-39, 1 June 2015.
3. Jangirala Srinivas, Sourav Mukhopadhyay, Dheerendra Mishra, "Secure and efficient user authentication scheme for multi-gateway wireless sensor networks", Ad Hoc Networks, vol. 54, pp. 147-169, January 2017.

4. Xiong Li, Jianwei Niu, Saru Kumari, Fan Wu, Kim-Kwang Raymond Choo, "A three-factor anonymous authentication scheme for wireless sensor networks in internet of things environments", Journal of Network and Computer Applications, 11 July 2017.
5. Fan Wu, Xiong Li, Arun Kumar Sangaiah, Lili Xu, Jian Shen,"A lightweight and robust two-factor authentication scheme for personalized healthcare systems using wireless medical sensor networks", Future Generation Computer Systems, 6 September 2017.
6. Shyamala Ramachandran, Valli Shanmugam,"A two way authentication using bilinear mapping function for wireless sensor networks", Computers & Electrical Engineering, vol. 59, pp. 242-249, April 2017.
7. Fan Wu, Lili Xu, Saru Kumari, Xiong Li, Ashok Kumar Das, "An efficient authentication and key agreement scheme for multi-gateway wireless sensor networks in IoT deployment",Journal of Network and Computer Applications, vol. 89, pp. 72-85, 1 July 2017.
8. Ruhul Amin, G.P. Biswa, "A secure light weight scheme for user authentication and key agreement in multi-gateway based wireless sensor networks", Ad Hoc Networks, vol. 36, Part 1, pp. 58-80, January 2016.
9. P. Caballero-Gil and C. Hernández-Goya, "Self-organized authentication in mobile ad-hoc networks," in Journal of Communications and Networks, vol. 11, no. 5, pp. 509-517, Oct. 2009.
10. D. Q. Nguyen, M. Toulgoat and L. Lamont, "Impact of trust-based security association and mobility on the delay metric in MANET," Journal of Communications and Networks, vol. 18, no. 1, pp. 105-111, Feb. 2016.
11. D. Hurley-Smith, J. Wetherall and A. Adekunle, "SUPERMAN: Security Using Pre-Existing Routing for Mobile Ad hoc Networks," IEEE Transactions on Mobile Computing, vol. 16, no. 10, pp. 2927-2940, Oct. 1 2017.
12. Q. Guan, F. R. Yu, S. Jiang and V. C. M. Leung, "Joint Topology Control and Authentication Design in Mobile Ad Hoc Networks With Cooperative Communications," IEEE Transactions on Vehicular Technology, vol. 61, no. 6, pp. 2674-2685, July 2012.
13. S. Bu, F. R. Yu, X. P. Liu and H. Tang, "Structural Results for Combined Continuous User Authentication and Intrusion Detection in High Security Mobile Ad-Hoc Networks," IEEE Transactions on Wireless Communications, vol. 10, no. 9, pp. 3064-3073, September 2011.
14. S. Bu, F. R. Yu, X. P. Liu, P. Mason and H. Tang, "Distributed Combined Authentication and Intrusion Detection With Data Fusion in High-Security Mobile Ad Hoc Networks," IEEE Transactions on Vehicular Technology, vol. 60, no. 3, pp. 1025-1036, March 2011.
15. J. Liu, F. R. Yu, C. H. Lung and H. Tang, "Optimal combined intrusion detection and biometric-based continuous authentication in high security mobile ad hoc networks," IEEE Transactions on Wireless Communications, vol. 8, no. 2, pp. 806-815, Feb. 2009.
16. U. Ghosh and R. Datta, "A Secure Addressing Scheme for Large-Scale Managed MANETs," IEEE Transactions on Network and Service Management, vol. 12, no. 3, pp. 483-495, Sept. 2015.
17. Yang Yang, "Broadcast encryption based non-interactive key distribution in MANETs", Journal of Computer and System Sciences, vol. 80, no. 3, pp 533–545, May 2014.
18. Ankush A. Vilhekar, C. D. Jaidhar, "Modified Authentication Protocol Using Elliptic Curve Cryptosystem for Virtual Subnets on Mobile Adhoc Networks", Springer Berlin Heidelberg, pp 426-432, 1-3 August, China, 2011.
19. N. A. Sheikh, A. A. Malik, A. Mahboob and K. Nisa, "Implementing voice over Internet protocol in mobilead hocnetwork – analysing its features regarding efficiency, reliability and security," The Journal of Engineering, vol. 2014, no. 5, pp. 184-192, 5 2014.
20. J. M. Chang, P. C. Tsou, I. Woungang, H. C. Chao and C. F. Lai, "Defending Against Collaborative Attacks by Malicious Nodes in MANETs: A Cooperative Bait Detection Approach," in IEEE Systems Journal, vol. 9, no. 1, pp. 65-75, March 2015.
21. VijayLaxmi, ChhaganLal, M.S.Gaur and DeepanshuMehta, "JellyFish attack: Analysis, detection and countermeasure in TCP-based MANET," Journal of Information Security and Applications, vol. 22, pp. 99-112, June 2015.
22. MarjanKuchaki Rafsanjani and HamidehFatemidokht, "FBeeAdHoc: A secure routing protocol for BeeAdHoc based on fuzzy logic in MANETs", AEU - International Journal of Electronics and Communications, vol. 69, no. 11, pp. 1613-1621, 2015.
23. Saju PJohn and PhilipSamuel, " Self-organized key management with trusted certificate exchange in MANET", Ain Shams Engineering Journal, vol. 6, no. 1, pp. 161-170, March 2015.
24. NAVEEN CHAUHAN, LALIT Kumar AWASTI, NAROTTAM CHAND, VIVEK KATIYAR, ANKIT CHUGH, "A Distributed Weighted Cluster Based Routing Protocol for MANET's", Department of Computer Science & Engineering, National Institute of Technology, HAMIRPUR, INDIA.
25. SHOBANA, Suresh, "Safe Clustering and Energy Based Routing for Mobile Ad hoc network", Department of Computer Science, DHANALAKSHMI, SRINIVASAN Engineering college, PERAMBALUR Department of Computer Science, MAR Engineering college, TRICHIRAPPALLI.
26. SANDIP A. Kahate, KAPIL N. Hande, Dept of CSE, G.H. RAISONI "Implementing Authentication Mechanism using Extended Public Key Cryptography in Wireless Network". College of Engineering, G.H. RAISONI College of Engineering, Nagpur (MS) INDIA Nagpur (MS).
27. Rajesh Kumar, RACHANA SINGH THAKUR, NEHARAHINJ, SANKALPRAJORA & DINESHTHAKU "Key Distributed Cryptography using Key Algorithm in MANET", MALWA Institute of Technology, Indore INDIA.
28. EDNA ELIZABETH.N, SUBASREE.S, and S. RADHA, "Enhanced Security Key Management Scheme for MANETS", Electronics and Communication Engineering Department Sri Siva College of Engineering, Chennai .
29. GimerCervera, MichelBarbeau, JoaquinGarcia-Alfaro and EvangelosKranakis, " A multipath routing strategy to prevent flooding disruption attacks in link state routing protocols for MANETs", Journal of Network and Computer Applications, vol. 36, no. 2, pp.744-755, March 2013.
30. Teng Li, Jianfeng Ma and Cong Sun, " NetPro: detecting attacks in MANET routing with provenance and verification", Science China Information Sciences, 2017.
31. S. Satheeshkumar and N. Sengottaiyan, " Defending against jellyfish attacks using cluster based routing protocol for secured data transmission in MANET", Cluster Computing, pp. 1-12, 2017.
32. [32] S. Vadhana Kumari and B. Paramasivan, " Defense against Sybil attacks and authentication for anonymous location-based routing in MANET", Wireless Networks, vol. 23, no. 3, pp. 715–726, 2017.
33. Muhammad Usman, Mian Ahmad Jan, Xiangjian He, Priyadarsi Nanda, "QASEC: A secured data communication scheme for mobile Ad-hoc networks", Future Generation Computer Systems, 12 May 2018.
34. Sajal Sarkar, Raja Datta, "A secure and energy-efficient stochastic multipath routing for self-organized mobile ad hoc networks", Ad Hoc Networks, vol. 37, Part 2, pp. 209-227, February 2016.
35. M. Kaliappan, B. Paramasivan, "Enhancing secure routing in Mobile Ad Hoc Networks using a Dynamic Bayesian Signalling Game model", Computers & Electrical Engineering, vol. 41, pp. 301-313, January 2015.
36. A. Amuthan, N. Sreenath, P. Boobalan, K. Muthuraj, "Dynamic multi-stage tandem queue modeling-based congestion adaptive routing for MANET", Alexandria Engineering Journal, 3 May 2017.
37. H. Nakayama, S. Kurosawa, A. Jamalipour, Y. Nemoto and N. Kato, "A Dynamic Anomaly Detection Scheme for AODV-Based Mobile Ad Hoc Networks", IEEE Transactions on Vehicular Technology, vol. 58, no. 5, pp. 2471-2481, Jun 2009.
38. T. H. Lacey, R. F. Mills, B. E. Mullins, R. A. Raines, S. K. Rogers, "RIPsec – Using reputation-based multilayer security to protect MANETs", Computers & Security, vol. 31, no. 1, pp. 122-136, February 2012.
39. Soumyadev Maity, R. C. Hansdah, "Self-organized public key management in MANETs with enhanced security and without certificate-chains", Computer Networks, vol. 65, pp. 183-211, 2 June 2014.
40. Yaser M. Khamayseh, Shadi A. Aljawarneh, Alaa Ebrahim Asaad, "Ensuring survivability against Black Hole Attacks in MANETS for preserving energy efficiency", Sustainable Computing: Informatics and Systems, vol. 18, pp. 90-100, June 2018.
41. Banoth Rajkumar, G. Narsimha, " Trust Based Certificate Revocation for Secure Routing in MANET", Procedia Computer Science, vol. 92, pp. 431-441, 2016.
42. Srinivas Aluvala, K. Raja Sekhar, Deepika Vodnala, "A novel technique for node authentication in mobile ad hoc networks", Perspectives in Science, vol. 8, pp. 680-682, September 2016.
43. Qing Chen, Zubair Md. Fadlullah, Xiaodong Lin, Nei Kato, "A clique-based secure admission control scheme for mobile ad hoc networks (MANETs)", Journal of Network and Computer Applications, vol. 34, no. 6, pp. 1827-1835, November 2011.

44. Nikos Komninos, Dimitrios D. Vergados, Christos Douligeris, “Authentication in a layered security approach for mobile ad hoc networks”, Computers & Security, vol. 26, no. 5, pp. 373-380, August 2007.
45. Parth Patel, Rajesh Bansode, Bhushan Nemade, “Performance Evaluation of MANET Network Parameters Using AODV Protocol for HEAACK Enhancement”, Procedia Computer Science, vol. 79, pp. 932-939, 2016.
46. Yuh-Ren Tsai, Shiuh-Jeng Wang, “Two-tier authentication for cluster and individual sets in mobile ad hoc networks”, Computer Networks, vol. 51, no. 3, pp. 883-900, 21 February 2007.
47. Barbara Carminati, Elena Ferrari, Ngoc Hong Tran, “Trustworthy and effective person-to-person payments over multi-hop MANETs”, Journal of Network and Computer Applications, vol. 60, pp. 1-18, January 2016.
48. Rehan Akbani, Turgay Korkmaz, G. V. S. Raju, “HEAP: A packet authentication scheme for mobile ad hoc networks”, Ad Hoc Networks, vol. 6, no. 7, pp. 1134-1150, September 2008.
49. Shuaishuai Tan, Xiaoping Li, Qingkuan Dong, “Trust based routing mechanism for securing OSLR-based MANET ”, Ad – H oc Networks, vol. 30, pp. 84-98, July 2015.
50. Huihua Zhou, Minghui Zheng, Tianjiang Wang, “ A Novel Group Key Establishment Scheme for MANETs”, Procedia Engineering, vol. 15, pp. 3388-3395, 2011.
51. J. Sandeep, J. Satheesh Kumar, “Efficient Packet Transmission and Energy Optimization in Military Operation Scenarios of MANET”, Procedia Computer Science, vol. 47, pp. 400-407, 2015.
52. K. Drira, H. Seba, H. Kheddouci, “ECGK: An efficient clustering scheme for group key management in MANETs”, Computer Communications, vol. 33, no. 9, pp. 1094-1107, 1 June 2010.
53. [53] Leovigildo Sánchez-Casado, Gabriel Maciá-Fernández, Pedro García-Teodoro, Roberto Magán-Carrión, “A model of data forwarding in MANETs for lightweight detection of malicious packet dropping”, Computer Networks, vol. 87, pp. 44-58, 20 July 2015.
54. Chun-Ta Li, Min-Shiang Hwang, Chi-Yu Liu, “An electronic voting protocol with deniable authentication for mobile ad hoc networks”, Computer Communications, vol. 31, no. 10, pp. 2534-2540, 25 June 2008.
55. Aikaterini Mitrokotsa, Christos Dimitrakakis, “Intrusion detection in MANET using classification algorithms: The effects of cost and model selection”, Ad Hoc Networks, vol. 11, no. 1, pp. 226-237, January 2013.
56. M. Sindhuja, K. Selvamani, A. Kannan, S. Kanimozhi, “Mobility Assisted Uncertainty Reduction in MANETS Using Forward Node Optimization”, Procedia Computer Science, vol. 48, pp. 408-413, 2015.
57. M. Mohanapriya, Ilango Krishnamurthi, “Modified DSR protocol for detection and removal of selective black hole attack in MANET”, Computers & Electrical Engineering, vol. 40, no. 2, pp. 530-538, February 2014.
58. Hung-Min Sun, Chiung-Hsun Chen, Yu-Fang Ku, “A novel acknowledgment-based approach against collude attacks in MANET”, Expert Systems with Applications, vol. 39, no. 9, pp. 7968-7975, July 2012.
59. Li Feng, Zili Li, Yi Zhang, “Security bootstrap model of key pre-sharing by polynomial group in mobile Ad Hoc Network”, Journal of Network and Computer Applications, vol. 32, no. 4, pp. 781-787, July 2009.
60. Uttam Ghosh, Raja Datta, “A secure dynamic IP configuration scheme for mobile ad hoc networks”, Ad Hoc Networks, vol. 9, no. 7, pp. 1327-1342, September 2011.
61. Jin-Hee Cho, Ing-Ray Chen, Kevin S. Chan, “Trust threshold based public key management in mobile ad hoc networks”, Ad Hoc Networks, vol. 44, pp. 58-75, 1 July 2016.
62. Jin-Hee Cho, Ing-Ray Chen, “On the tradeoff between altruism and selfishness in MANET trust management”, Ad Hoc Networks, vol. 11, no. 8, pp. 2217-2234, November 2013.
63. B. Rong, H. Chen, Y. Qian, K. Lu, R. Q. Hu and S. Guizani, "A Pyramidal Security Model for Large-Scale Group-Oriented Computing in Mobile Ad Hoc Networks: The Key Management Study," IEEE Transactions on Vehicular Technology, vol. 58, no. 1, pp. 398-408, Jan. 2009.
64. N. Saxena, G. Tsudik and J. H. Yi, "Efficient Node Admission and Certificateless Secure Communication in Short-Lived MANETs," IEEE Transactions on Parallel and Distributed Systems, vol. 20, no. 2, pp. 158-170, Feb. 2009.
65. Y. Wang, F. R. Yu, H. Tang and M. Huang, "A Mean Field Game Theoretic Approach for Security Enhancements in Mobile Ad hoc Networks," IEEE Transactions on Wireless Communications, vol. 13, no. 3, pp. 1616-1627, March 2014.
66. J.Sathiamoorthy, B.Ramakrishnan and Usha, "Design of a proficient hybrid protocol for efficient route discovery and secure data transmission in CEAACK MANETs", Journal of Information Security and Applications, vol. 36, Pages 43-58, October 2017.
67. A. Amuthan, N. Sreenath, P. Boobalan, K. Muthuraj, “Dynamic multi-stage tandem queue modeling-based congestion adaptive routing for MANET”, Alexandria Engineering Journal, 3 May 2017.
68. [68] S. B. Lee, G. S. Ahn and A. T. Campbell, "Improving UDP and TCP performance in mobile ad hoc networks with INSIGNIA," in IEEE Communications Magazine, vol. 39, no. 6, pp. 156-165, Jun 2001.
69. K. El Defrawy and G. Tsudik, "ALARM: Anonymous Location-Aided Routing in Suspicious MANETs," in IEEE Transactions on Mobile Computing, vol. 10, no. 9, pp. 1345-1358, Sept. 2011.
70. C. Liu, R. Correa, X. Li, P. Basu, B. T. Loo and Y. Mao, "Declarative Policy-Based Adaptive Mobile Ad Hoc Networking," in IEEE/ACM Transactions on Networking, vol. 20, no. 3, pp. 770-783, June 2012.
71. A. Nadeem and M. P. Howarth, "A Survey of MANET Intrusion Detection & Prevention Approaches for Network Layer Attacks," in IEEE Communications Surveys & Tutorials, vol. 15, no. 4, pp. 2027-2045, Fourth Quarter 2013.
72. K. E. Defrawy and G. Tsudik, "Privacy-Preserving Location-Based On-Demand Routing in MANETs," in IEEE Journal on Selected Areas in Communications, vol. 29, no. 10, pp. 1926-1934, December 2011
73. V. Kulathumani, A. Arora, M. Sridharan, K. Parker and B. Lemon, "On the Repair Time Scaling Wall for MANETs," in IEEE Communications Letters, vol. 20, no. 8, pp. 1623-1626, Aug. 2016.
74. S. Surendran and S. Prakash, "An ACO look-ahead approach to QOS enabled fault- tolerant routing in MANETs," in China Communications, vol. 12, no. 8, pp. 93-110, August 2015.
75. J. Dowling, E. Curran, R. Cunningham and V. Cahill, "Using feedback in collaborative reinforcement learning to adaptively optimize MANET routing," in IEEE Transactions on Systems, Man, and Cybernetics - Part A: Systems and Humans, vol. 35, no. 3, pp. 360-372, May 2005.
76. A. Bader and M. S. Alouini, "Mobile Ad Hoc Networks in Bandwidth-Demanding Mission-Critical Applications: Practical Implementation Insights," in IEEE Access, vol. 5, pp. 891-910, 2017.
77. L. Ritchie, H. S. Yang, A. W. Richa and M. Reisslein, "Cluster overlay broadcast (COB): MANET routing with complexity polynomial in source-destination distance," in IEEE Transactions on Mobile Computing, vol. 5, no. 6, pp. 653-667, June 2006
78. T. R. Andel and A. Yasinsac, "Surveying security analysis techniques in manet routing protocols," in IEEE Communications Surveys & Tutorials, vol. 9, no. 4, pp. 70-84, Fourth Quarter 2007.
79. Z. Zhao, H. Hu, G. J. Ahn and R. Wu, "Risk-Aware Mitigation for MANET Routing Attacks," in IEEE Transactions on Dependable and Secure Computing, vol. 9, no. 2, pp. 250-260, March-April 2012.
80. S. Y. Han and D. Lee, "An Adaptive Hello Messaging Scheme for Neighbor Discovery in On-Demand MANET Routing Protocols," in IEEE Communications Letters, vol. 17, no. 5, pp. 1040-1043, May 2013.
81. Z. Wei, H. Tang, F. R. Yu, M. Wang and P. Mason, "Security Enhancements for Mobile Ad Hoc Networks With Trust Management Using Uncertain Reasoning," in IEEE Transactions on Vehicular Technology, vol. 63, no. 9, pp. 4647-4658, Nov. 2014.
82. S. K. Dhurandher, M. S. Obaidat, K. Verma, P. Gupta and P. Dhurandher, "FACES: Friend-Based Ad Hoc Routing Using Challenges to Establish Security in MANETs Systems," IEEE Systems Journal, vol. 5, no. 2, pp. 176-188, June 2011.
83. N. Mohammed, H. Otrok, L. Wang, M. Debbabi and P. Bhattacharya, "Mechanism Design-Based Secure Leader Election Model for Intrusion Detection in MANET," IEEE Transactions on Dependable and Secure Computing, vol. 8, no. 1, pp. 89-103, Jan.-Feb. 2011.
84. V. Rajamanickam and D. Veerappan, "Inter cluster communication and rekeying technique for multicast security in mobile ad hoc networks," IET Information Security, vol. 8, no. 4, pp. 234-239, July 2014.
85. H. Tang, F. R. Yu, M. Huang and Z. Li, "Distributed consensus-based security mechanisms in cognitive radio mobile ad hoc networks," IET Communications, vol. 6, no. 8, pp. 974-983, 22 May 2012.
86. W. Liu and M. Yu, "AASR: Authenticated Anonymous Secure Routing for MANETs in Adversarial Environments," IEEE Transactions on Vehicular Technology, vol. 63, no. 9, pp. 4585-4593, Nov. 2014.

87. A. Anand, H. Aggarwal and R. Rani, "Partially distributed dynamic model for secure and reliable routing in mobile ad hoc networks," Journal of Communications and Networks, vol. 18, no. 6, pp. 938-947, Dec. 2016.
88. S. Umamaheswari and G. Radhamani, "Enhanced ANTSEC framework with cluster based cooperative caching in mobile ad hoc networks," Journal of Communications and Networks, vol. 17, no. 1, pp. 40-46, Feb. 2015.
89. A. M. Shabut, K. P. Dahal, S. K. Bista and I. U. Awan, "Recommendation Based Trust Model with an Effective Defence Scheme for MANETs," IEEE Transactions on Mobile Computing, vol. 14, no. 10, pp. 2101-2115, 1 Oct. 2015.
90. M. Gunasekaran and K. Premalatha, "TEAP: trust-enhanced anonymous on-demand routing protocol for mobile ad hoc networks," IET Information Security, vol. 7, no. 3, pp. 203-211, Sept. 2013.
91. F. R. Yu, H. Tang, P. C. Mason and F. Wang, "A Hierarchical Identity Based Key Management Scheme in Tactical Mobile Ad Hoc Networks," IEEE Transactions on Network and Service Management, vol. 7, no. 4, pp. 258-267, December 2010.
92. M.Turkanovic,M.Hölbl, “An improved dynamic password based user authentication scheme for hierarchical wireless sensor networks, Elek-tron.Elektrotech, vol. 19, no. 6, pp.109–116, 2013.