Journal of Cloud Computing:
Advances, Systems and Applications

RESEARCH Open Access

Enhanced security using multiple paths routine scheme in cloud-MANETs

Tao Hai[1,2], Jincheng Zhou[1,3*], Ye Lu[4], Dayang Jawawi[2], Dan Wang[3,5], Edeh Michael Onyema[6] and Cresantus Biamba[7*]

Abstract

Cloud Mobile Ad-hoc Networks (Cloud-MANETs) is a framework that can access and deliver cloud services to MANET users through their smart devices. MANETs is a pool of self-organized mobile gadgets that can communicate with each other with no support from a central authority or infrastructure. The main advantage of MANETs is its ability to manage mobility while data communication between different users in the system occurs. In MANETs, clustering is an active technique used to manage mobile nodes. The security of MANETs is a key aspect for the fundamental functionality of the network. Addressing the security-related problems ensures that the confidentiality and integrity of the data transmission is secure. MANETs are highly prone to attacks because of their properties.In clustering schemes, the network is broken down to sub-networks called clusters. These clusters can have overlapping nodes or be disjointed. An enhanced node referred to asthe Cluster Head (CH) is chosen from each set to overseetasks related to routing. It decreases the member nodes' overhead and improvesthe performance of the system. The relationship between the nodes and CH may vary randomly, leading to re-associations and re-clustering in a MANET that is clustered. An efficient and effective routing protocol is required to allow networking and to find the most suitable paths between the nodes. The networking must be spontaneous, infrastructure-less, and provide end-to-end interactions. The aim of routing is the provision of maximum network load distribution and robust networks. This study focused on the creation of a maximal route between a pair of nodes, and to ensure the appropriate and accurate delivery of the packet. The proposed solution ensured that routing can be carried out with the lowest bandwidth consumption. Compared to existing protocols, the proposed solution had a control overhead of 24, packet delivery ratio of 81, the lowest average end-to-end delay of 6, and an improved throughput of 80,000, thereby enhancing the output of the network. Our result shows that multipath routing enables the network to identify alternate paths connecting the destination and source. Routing is required to conserve energy and for optimum bandwidth utilization.

Keywords Mobile Ad-Hoc Network (MANET), Weighted clustering, Offloading, Energy efficiency, Multipath routing

*Correspondence:
Jincheng Zhou
zjc81@sgmtu.edu.cn
Cresantus Biamba
cresantus.biamba@hig.se
Full list of author information is available at the end of the article

Introduction

With a plethora of applications floating around the web, it is evident that the Internet is quickly progressing. This has been made possible with the help of numerous wireless networking technologies which works in conjunction with the Internet technologies. MANETs is one area that has a lot of potential for researchand application development of wireless networks. In recent times, the field of wireless communication has been blooming. Ad-hoc networks are an exciting and dynamic area of research. Such networks either operate as a stand-alone network, or with an attachment to other networks or the Internet at multiple points. Thus, it paves the way for novel and exciting applications [1]. They can be applied in road safety management, household monitoring, healthcare systems, disaster and rescue operations, defense areas, handling weapons, robotics, etc. [2].

MANETs are majorly deployed for establishing dynamic communication in emergency and rescue operations, military/battlefield environments, intelligent transportation systems, conferences, patient monitoring, smart homes and security sensitive applications. MANETs recently gained popularity for the application of their drones in different areas of environment controlsuch as forest fires, pollution monitoring, and vigilance [3].

In emergency zones, the communication network has to be quickly established, so the use of independent drones that form an ad-hoc network is becoming a remarkable alternative [4]. The primary technical challenge of drone technology is the difficulty in powering the drones for a long service time, since they are battery-constrained and have limited lifespan. Also, each device needs to continuously maintain information for traffic routing. Thus, a reliable communication or a secure routing protocol between different systems constitutes a building block to the data delivery in such drone-based applications.

This study has the objective of developing an energy-efficient routing protocol that allows the reliable and secure exchange of information between modern MANETs. For achieving energy-efficiency, increasing the network lifetime and scalability in dense areas, the clustering approach can be applied. Also, multiple node disjoint paths help in accomplishing reliability, stability and network robustness. For the security of MANETs and minimal delay, mitigating the malicious attacks is essential [22] (Fig. 1).

The major features of a MANET can be characterized as [5]:

- Dynamic topology: They have random and fast-changing topology due to mobile nodes.
- Bandwidth-constrained, variable capacity links: The wireless channel has limited bandwidth and variable capacity due to free space and open media.

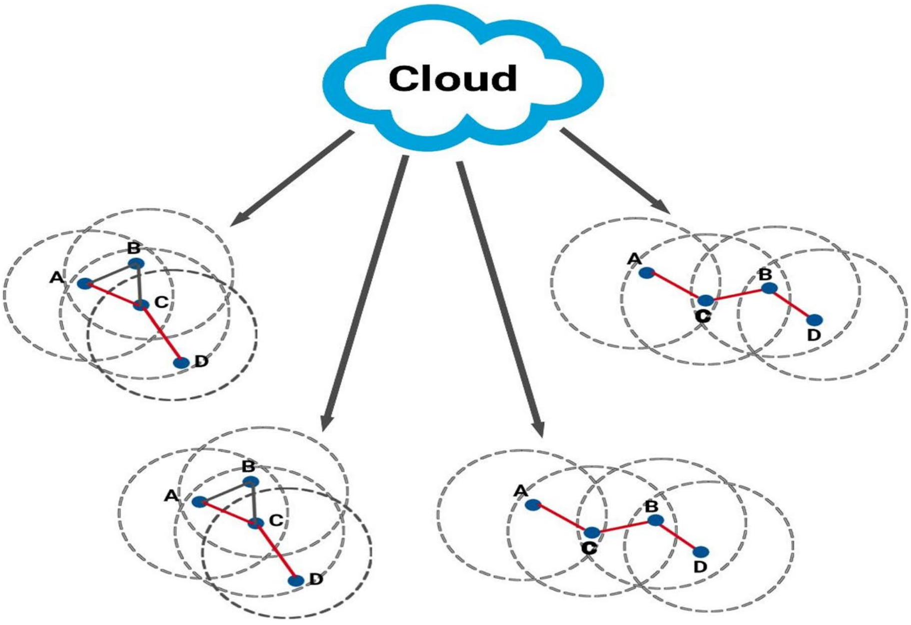

Fig. 1 Cloud mobile ad-hoc networks [22]

- Autonomous behavior: All the nodes in the network are independent, and they act as both host and router while forwarding data.
- Limited power/energy: Nodes are wireless and dependent on battery power for their operation. These device batteries have limited operation duration.
- Limited security: Due to the absence of any central authority and open media, MANETs are highly vulnerable to security threats.

Since the topology of MANETs is dynamic and unstable, these networks face issues of delays and packet loss more than fixed networks. Nodes being mobile, are dependent on batteries which have limited power. Hence, it is essential to explore approaches to save power,make the network energy-efficient, and improve the network lifetime. The nodes in MANETs have unrestricted mobility and can connect to each other without any central monitoring. The management of the network and routing is done by all the network nodes. These characteristics of MANETs make them susceptible to routing and security issues more than the conventional networks. Therefore, effective mechanisms to handle the mobility-initiated issues should be looked into while making the routing decisions.

In large-scale and dense MANETs, clustering is an active techniqueused to managemobile nodes. In a cluster-based framework, the network is classified into groups referred to as clusters [6]. The clusters can have overlapping nodes or be disjoint. An enhanced node referred to asthe Cluster Head (CH) is chosen from each set to oversee tasks related to routing. Clustering decreases the overhead on the member nodes and enhances the performance of the system. The relationship between the nodes and CH may vary randomly, leading to re-associations and re-clustering in a MANET that is clustered.

Previous works were insufficient in resolving the challenge of powering the drones used to form the ad-hoc network. An efficient and effective routing protocol is required to allow networking and to find the most suitable paths between the nodes. The networking must be spontaneous, infrastructure-less, and provide end-to-end interactions. The main objective of this research is the creation of a maximal route between a pair of nodes, and to ensure the appropriate and accurate delivery of the packet. Wired networks' routing protocols are not appropriate for MANETs because their topology is dynamic. Routing must be carried out with the lowest bandwidth consumption, least packet loss, and control overhead, thereby enhancing the output of the network. Multipath routing allows the formation of multiple paths between the source and destination. Multipath routing also aids in the optimum bandwidth utilization and energy conservation of the member nodes. The major applications of multipath routing include techniques to design robust networks, and optimum distribution of the network load.

The security of MANETs [7] is a big hindranceto the smooth operation of the network. Addressing the security issues can ensure that the basic network services, confidentiality, and integrity of the data transmission are met.Characteristics of MANETs like the open medium, dynamic topology, and lack of central monitoring make them prone to several security attacks. Some of the most prominent attacks in MANETs includemodification attacks, fabrication attacks, and impersonation attacks like the black-hole and worm-hole attacks.

Problem definition

The clustering process on MANET nodes allows adaptation to topology changes in the network, thus ensuring the efficient utilization of the available bandwidth and high network throughput. A variety of clustering schemes were developed for making the network energy-efficient and improving the network lifetime. However, for the purpose of data forwarding, and with the increase in the cluster number, energy consumption tends to shoot up. Existing clustering approaches have several drawbacks which include: increased control overhead for the purpose of retaining the backup routes, highly complex approaches, and the recurrent beaconing.

The devices in MANETs operate on limited energy resource i.e., batteries [8]. The uncontrolled mobility of nodes leads to the formation of a network that is highly dynamic and changes its topology rapidly. Thiscan all result in the frequent failure of routes. For nodes to remain connected and be able to communicate for longer times, low delay and high throughput is required from the routing approach used. Existing routing approaches do not provide desirable results under such cases.

The heterogeneous devices forming the MANETs have inconsistent data rates and different processing powers, which may lead to problems in communication. Majority of the existing works on clustering focus on issues such as reducing the energy consumption of mobile devices, reducing the maintenance overhead, and increasing the network lifetime.

In a clustered MANET, all routing from outside the network or internet is directed through the Cluster Head (CH). There may be a difference in the rates at which data is received from the outside service provider and forwarded to the member node. Thus, the communication process experiences unnecessary delay because of the difference in the reception and transmission capacity of the CH. It may also lead to increased packet loss due to buffer overflow at the nodes.

With the node movement and clustering, reorganization of nodes and changes in the network topology occur frequently in MANETs. The rapid dissipation of energy and changes in the nodes' topology may lead to the failure of links. An optimal solution to this problem is missing in existing research. Additionally, the dynamic nature, open medium, and decentralized control of MANETs makes it highly susceptible to attacks. In the traditional works, a trust-based framework is offered by the central parties like Trusted Third Parties (TTP). In the clustering-based frameworks, the cluster head acts as a TTP for providing a secure communication in inter and intra cluster routing. In order to manage the cluster members in the group, the cluster head requires lightweight key management algorithms. To satisfy such objectives, many traditional works proposed different algorithms, but the problems of increased computational complexity, network overhead, inefficient security, unreliability, and reduced network throughput rendered them less useful.

Key contribution

This work aims at designing a routing protocol for MANETs which is energy-aware, provides security and stability, and enhances the chances of successful data transmission in disaster response and rescue applications. The major contribution of the proposed work is the development of an energy-efficient routing protocol that allows a reliable and secure exchange of information between modern MANETs. For achieving energy-efficiency, increased network lifetime and scalability in dense areas, the clustering approach is applied. Also, the multiple node disjoint paths help in accomplishing reliability, stability and network robustness. We attempt to create a maximal route between a pair of nodes, and to ensure the appropriate and accurate delivery of the packet.

Organization of the paper

The rest of this paper is organized as follows: Related work section provides a summary of the previous related works explaining their pros and cons. Proposed work section describes the proposed model, including the clustering scheme for MANETs consisting of cluster head selection, cluster formation and initialization phases; an efficient model for managing data traffic using data offloading; a weighted multipath energy-aware routing scheme, and a secure cryptography mechanism at the end. Results section presents an experimental evaluation of the proposed model with existing works. Conclusion section concludes the work and provides the future scope.

Related work

There are various clustering schemes and routing protocols for MANETs that have been used to address different network-related issues like scalability, energy efficiency, and mobility. Based on the network architecture, node density and mobility patterns, the categories of research for MANETs routing protocols are: cluster-based routing, multipath routing, and secure routing. The work done under these categories are studied for use in secure MANET applications.

Cluster-based routing protocols in MANETs

The most commonly used cluster-based routing protocols [95] for MANETs are energy-based, connectivity-based, mobility-based, and weighted. Some of the existing works based on clustering and cluster-based routing are discussed below:

In [9], SYN, an energy-efficient clustering protocol was proposed. It used the Max-heap tree to model varying levels of energy of the nodes. In [6], the authorsintroduced a Particle Swarm Optimization (PSO)-based protocol for optimizing clusters and conserving energy in ad-hoc networks. It discussed the Zone-based protocol for routing with a corresponding collision-guided broadcasting algorithm that used one-hop clustering [10]. In the MBHC method, the clusters are formed according to the node mobility pattern [11]. The cluster head is selected considering the lowest stability value amongst neighbors. Here, the distance travelled by any two nodes estimate the relative mobility between them over time. It allows the immediate merging of clusters with similar mobility patterns. The mobility pattern is considered an essential measure for cluster formation as two nodes with similar velocity and direction have lower mobility difference and are grouped together in the same cluster. The major advantage of this scheme is the minimization of the cluster number by taking into account the group mobility pattern, and addressing the issue of scalability for routing protocols used in large MANETs. Cluster formation in the EPAC method is done on the basis of the energy requirement for the completion of tasks assigned [12]. The node with the lowest ID, which is dependent on the maximum energy left, is chosen as the cluster head. The algorithm tries minimizing the energy consumed in a cluster and the CH selects transmission loads based on the energy available at the cluster nodes. The major advantage is the formation of energy-efficient and stable clusters. This also reduces the energy drainage and chances of re-clustering. WBDC is a weight-based clustering based on the collective weight metrics: ideal node-degree, mobility, and energy of the nodes [13]. The weight of every node is estimated considering the weighted metrics. The node with the maximum weight amongst the neighbors is made the cluster head. The threshold value determines the re-affiliation process. When the mobility metric value of a node is higher than the threshold value, the node starts to move out of the cluster. The algorithm considers realistic network parameters and includes the flexibility of weighing factor adjustments. Neethu and Singh [14] proposed an approach for re-clustering in MANET routing protocols where security can be a challenge. The process involves the generation and sharing of different keys to all the member nodes. Sung et al. [15] designed a distributed cluster formation scheme which involves algorithms for the creation and maintenance of clusters in high mobility networks. Loutfi [16] discussed the fault tolerant multipath that is mobility-aware using multicast routing protocol for MANETs. The main objective was to enhance the reliability of the routing protocol in spite of the continuous movement of the nodes. The experimental result of the proposed method attained better fault tolerance by means of an enhanced packet delivery ratio and decreased delay. In [17], a new weight-based clustering scheme for improving security of MANETs was designed. In [18], the authors proposed an energy-efficient cloud-based IoE framework to integrate cloud computing with the Internet of Everything and provide valuable services to consumers. The framework is optimized by clustering the IoT networks using a wind driven algorithm.

Table 1 summarizes the cluster-based protocols for routing in MANETs discussed above:

The issues connected with the existing clustering algorithms are: loss of energy when a node continues to be a CH for a long duration of time, and increasing communication overhead as the cluster number increases [95]. Also, the throughput of the network is reduced and energy usage is increased due to the CH re-election.

The major disadvantage of connectivity-based clustering algorithms is throughput reduction as the number of cluster nodes starts increasing. The mobility-based clustering algorithms undergo degradation in performance because of the randomly moving network nodes. The shortcoming of the weighted clustering algorithms is that for clustering to begin, it requires all the member nodes' weight parameter. The energy-based category faces the issue of requirement of increased overhead to select the CHs.

Multipath routing protocols

Routing in MANETs can be quite challenging owing to the node mobility, dynamic topology and constrained resources. To improve end-to-end throughput and achieve balancing of load in the limited resources environment, multipath routing should be adopted [23]. Multiple paths can either be link disjointed or node disjointed. Node-disjoint multipath have an edge over link-disjoint as no matching node exists between any route, which ensures that at least one route remains available whenever node or link failure occurs.

A lot of research has been done on clustered networks applying multipath routing in MANETs. AOMDV (Ad-hoc On-demand Multipath Distance Vector) [19] showcases an extended multipath version of AODV (Ad-hoc On-demand Distance Vector) [24]. It is a simple routing protocol with link disjoint characteristics which aims at discovering loop-free routes. SMR (Split Multipath Routing) protocol uses multipaths that are based on maximum disjointness [20]. As a result, load balancing is required over multiple paths. A new weight metric is used by EIDM for path selection, which combines the remaining energy, interference and packet drop rate, along with mobility of the nodes [25]. An energy-efficient multipath routing protocol MEER (Multipath Energy-efficient Routing)

Table 1 Summary of different categories of cluster-based routing protocols and their issues

Classification of Clustering schemes on the basis of QOS	Names of Protocols	Issues
Energy-Aware Clustering	EPAC [12], SYN [9], E-PSO [6]	High control overhead and delay.
Location/Connectivity-based Clustering	KCLC [19], KCMBC [19], DDVC [20],DDLC [20]	Throughput reduces when the node number increases in the clusters.
Mobility-based Clustering	MBHC [11], MPBC [16], MBDH [21]	Energy not conserved.
Weighted metric Clustering	WBDC [13], WCA [17], IWCA [22]	Complexity and clustering process starts late.

uses an approach of energy control to help the network extend its lifetime [26]. Cluster-based multipath routing (CBMRP) distributes data along multiple paths and helps in reducing traffic congestion [27]. The major objective of routing is to determine paths that have less interference for smooth data transmission. Another multipath routing protocol which is also energy-efficient is ES-CMR (Energy-aware and Stable Clustered-based Multipath Routing protocol) [28]. The protocol works on keeping the energy of the nodes at optimum value, thereby keeping the network stable and enhancing its lifetime.One of the major issues connected with the existing algorithms is that some protocols don't take energy into account or manage energy levels optimally, resulting in the death of nodes. Some approaches don't use multiple paths to distribute network load, thus not utilizing network resources properly. This results in a decrease in the network efficiency,especially during conditions like congestion and link failure. Others don't apply load balancing approach well, creating issues in big MANETs that are energy and power-constrained.

Node disjoint multipath routing protocols

Routing that is multipath and node-disjoint provides better resilience to path changes and increases network stability. Dual Node-Disjoint Paths Routing (DNDR) is an approach that works on enhancing the reliability and robustness of the network [29]. The protocol combines features of the reverse AODV strategy with On-Demand routing to check the availability of routes that are node-disjoint and exhibit low control overhead. It also creates a backup plan for increasing the efficacy of the data salvation process under the condition of link failure. They don't consider the energy while determining the node-disjoint routes. Group mobility-based Multipath Routing protocol (GMR) was designed to support large-sized and highly dense mobile ad-hoc networks [30]. This work handles the mobility of the group by adapting a combination of both intra-group routing and inter-group routing. The group head maintains a routing table which provides the necessary information for discovering routes in intra-group routing. In inter-group routing however, reactive routing along with zone structuring is applied in the network to determine multiple paths that are node-disjoint. The zoning method ensures that every discovered path is matched to a different zone, so that nodes are disjoint in multiple paths. Again, energy conservation is not taken into consideration here. Node-Disjoint Multipath Routing Protocol (NDMRP) is a multipath routing work that is built on AODV protocol [31]. The primary objective of the suggested protocol is determining all node-disjoint paths between any two pair of nodes while reducing the routing control overhead. In this approach, when the source and destination find theinitial route between them, the source initiates the transmission process. Other available backup paths are also determined in parallel with the data transmission occurring on the first route, thus resulting in the minimization of the initial delay as data transfer starts whenever the first path is established. This again doesn't considerenergy or clustering. Also, optimal paths are not considered while choosing path for data transfer. Table 2 summarizes the multipath routing protocols for MANETs discussed above:

Secure routing protocols

In MANETs, any malicious attack in the routing stage of transmission can incapacitate the whole system and interrupt the overall communication. Thus, security plays an important role in the smooth functioning of data communication. There are various existing routing protocols and cryptography mechanisms related to MANETs' security.

FBeeAdHoc was designed to provide secure routing in MANET [36]. Their aim was to investigate the security vulnerabilities and threats against the network. The fuzzy set theory was utilized in this work to identify and detect different types of threats in the network. The attacks considered in this work were forager route-related and scout-related attacks. Both the node trust and route trust were evaluated using the concept of fuzzy logic. PRIME performed an experimental evaluation of AODV and DSDV protocols for the detection

Table 2 Summary of different categories of multipath routing protocols and their issues

Categories of Routing Protocols	Names of Protocols	Issues
Energy-Aware Multipath Routing Protocols	ECNC AODV [32], MBCR [33], MEER [26], MMRE AOMDV [34]	High control overhead and possibility of link failure are the concerns.
Cluster- based Multipath Routing Protocols	CBMRP [27], CBR [35], ES-CMR [28]	Paths are not energy-efficient; error and high overhead while load balancing.
Simple Multipath Routing Protocols	AOMDV [19], SMR [20], EIDM [25], NDMRP [25]	Energy conservation and load balancing not considered.
Node-Disjoint Multipath Routing Protocols	DNDR [29], GMR [30], NDMRP [31], ES-CMR [28]	Energy not considered; scalability is also an issue.

of black hole attacks in MANETs [37, 38]. They stated that the Ad-hoc On-demand Distance Vector (AODV) protocol outperforms the Destination Sequenced Distance Vector (DSDV) protocol by providing better throughput, reduced delay, and increased packet delivery ratio. CBDS developed a Cooperative Bait Detection Approach for the detection of malevolent nodes in MANETs [39]. CBSRP implemented a clustering-based attack detection mechanism for providing security for MANETs [40]. The selection of communication nodes was based on the node location, trust factor, residual energy, mobility, and network throughput. CORMAN designed a scheme to manage keys for securing MANETs better while keeping the mobility overhead low [41]. Here, the Chinese Remainder Theorem (CRT) was utilized to generate the key for removing the malicious nodes. CONFIDANT implemented an energy-efficient geocast forwarding mechanism for increasing the security of MANET [42]. Here, the common three-tier security framework was used for performing the pair wise key establishment and authentication. The suggested protocol utilized the geographical information for forwarding the packets in an efficient way. Also, the multi-hopping scheme was utilized to route the data in a clustered manner, but it failed to improve the level of security by enabling an efficient and reliable communication in the network. Flooding Factor-based Framework for Trust Management (F3TM) in MANETs operates on the concept of flooding messages and utilizing it to recognize the malicious nodes [43]. This is done by deploying an approach for the calculation of trust values of network nodes. This work was validated with the help of Experimental Grey Wolf algorithm, which helped in route discovery. In [44], the authors reviewed methods such as deep learning, artificial intelligence, and machine learning to identify and tolerate faults in cloud computing systems and environments.

Table 3 summarizes the MANETs secure routing protocols discussed above.

Table 3 Summarizing secure routing protocols on the basis of QOS categories and their issues

Classification of Secured Protocols	Names of Protocols	Issues
Packet Delivery Ratio	SE-AODV [45, 46], FBEEADHOC [36], CBDS [39], CBSRP [40]	Introduces latency and high overhead.
End-to-End Delay	SAR [47], RBDR [48], CORE [49], F3TM [43], EAACK [50], ICC [51]	Issues of stability of the links and complex processing.
Routing Overhead	CONFIDANT [42], SPREAD [52], CORMAN [41], PRIME [37]	Latency and link stability.

Summary of the literature review

S/N	Authors	Description
[15]	Sulyun Sung, Yuhwa Seo and Yongtae Shin	This paper introduced a distributed cluster formation scheme which involves algorithms for the creation and maintenance of clusters in high mobility networks.
[6]	Waqar Asif and Saad Qaisar	This paper introduced a Particle Swarm Optimization (PSO)-based protocol for optimizing clusters and conserving energy in ad-hoc networks. Its shortcoming was high control overhead and delay.
[9]	N. Shukla	This paper introduced SYN, an energy-efficient clustering protocol was proposed. It used the Max-heap tree to model varying levels of energy of the nodes. Its shortcoming was high control overhead and delay.
[10]	Sudha, K., Ranjith, J. P., Ganapathy, S., & Sasidharan, M. S. R	This paper introduced the Zone-based protocol for routing with a corresponding collision-guided broadcasting algorithm that used one-hop clustering.
[14]	Neethu, V., & Singh, A. K	This paper introduced an approach for re-clustering in MANET routing protocols where security can be a challenge. The process involves the generation and sharing of different keys to all the member nodes.
[16]	A. Loutfi	This paper discussed the fault tolerant multipath that is mobility-aware using multicast routing protocol for MANETs. Its shortcoming was that energy was not conserved.
[17]	Basurra, S. S., De Vos, M., Padget, J., Ji, Y., Lewis, T., & Armour, S	This paper introduced a new weight-based clustering scheme for improving security of MANETs. Its shortcomings were that the complexity and clustering process starts late.
[19]	S. B. Kulkarni and B. Yuvaraju,	This paper introduced AOMDV (Ad-hoc On-demand Multipath Distance Vector). Its shortcoming is that throughput reduces when the node number increases in the clusters.
[20]	I. Kaur and A. Rao	This paper introduced an SMR (Split Multipath Routing) protocol that uses multipaths based on maximum disjointness. Its shortcomings were that energy conservation and load balancing were not considered.

S/N	Authors	Description
[25]	T. Panke	This paper introduced a new weight metric used by EIDM for path selection, which combines the remaining energy, interference and packet drop rate, along with mobility of the nodes. Its shortcomings were that energy conservation and load balancing were not considered.
[26]	Ammayappan, Kavitha, V. N. Sastry, and Atul Negi	This paper introduced an energy-efficient multipath routing protocol MEER (Multipath Energy-efficient Routing) uses an approach of energy control to help the network extend its lifetime. Its shortcomings were high control overhead and possibility of link failure are the concerns.
[28]	Dr.S.S.Dhenakaran and A.Parvathavarthini	This paper introduced a multipath routing protocol which is also energy-efficient is ES-CMR (Energy-aware and Stable Clustered-based Multipath Routing protocol). Its shortcomings were that energy was not considered, and scalability is also an issue.
[29]	Sunil Taneja,	This paper introduced a Dual Node-Disjoint Paths Routing (DNDR) approach that works on enhancing the reliability and robustness of the network. Its shortcomings were that energy was not considered, and scalability is also an issue.
[30]	ALGhafran, Labdah, and Zulkefli Bin Muhammed Yusof	This paper introduced a Group mobility-based Multipath Routing protocol (GMR) to support large-sized and highly dense mobile ad-hoc networks. Its shortcomings were that energy was not considered, and scalability is also an issue.
[31]	Chatterjee, Mainak, Sajal K. Das, and Damla Turgut	This paper introduced a Node-Disjoint Multipath Routing Protocol (NDMRP) built on AODV protocol. Its shortcomings were that energy was not considered, and scalability is also an issue.
[36]	T. Spyropoulos, K. Psounis, and C. Raghavendra	This paper introduced a FBeeAdHoc to provide secure routing in MANET. Its shortcomings were that it introduces latency and high overhead.
[37]	Xinming, Zhang, Shi Dong, and Zou Fengfu	This paper introduced an AODV protocol for the detection of black hole attacks in MANETs. Its shortcomings were latency and link stability.
[39]	Li, Xuefei, and Laurie Cuthbert	This paper introduced a Cooperative Bait Detection Approach for the detection of malevolent nodes in MANETs. Its shortcomings were that it introduces latency and high overhead.
[40]	Gharib, Mohammed, Zahra Moradlou, Mohammed Ali Doostari, and Ali Movaghar	This paper introduced a clustering-based attack detection mechanism for providing security for MANETs. Its shortcomings were that it introduces latency and high overhead.
[42]	Kim, Jihye, and Gene Tsudik	This paper introduced an energy-efficient geocast forwarding mechanism for increasing the security of MANET. Its shortcomings were its latency and link stability.
[43]	B. Tavli and W. B. Heinzelman	This paper introduced a Flooding Factor-based Framework for Trust Management (F3TM) in MANETs on the concept of flooding messages and utilizing it to recognize the malicious nodes. Its shortcomings were its issues of stability of the links and complex processing.
[11]	R. Morris, J. Jannotti, F. Kaashoek, J. Li, and D. Decouto	This paper proposed the MBHC method where clusters are formed according to the node mobility pattern. Its shortcomings was that energy was not conserved.
[12]	M. Grossglauser and D. Tse	This paper introduced the EPAC method where cluster formation is done on the basis of the energy requirement for the completion of tasks assigned. Its shortcomings were high control overhead and delay.
[13]	M. Steenstrup	This paper introduced WBDC, a weight-based clustering based on the collective weight metrics: ideal node-degree, mobility, and energy of the nodes. Its shortcoming was that the complexity and clustering process starts late.
[38]	He, Guoyou	This paper introduced a DSDV protocol for the detection of black hole attacks in MANETs. Its shortcomings were latency and link stability.
[24]	Chakeres, I.D. and Belding-Royer, E.M.,	This paper introduced AODV (Ad-hoc On-demand Distance Vector), a simple routing protocol with link disjoint characteristics which aims at discovering loop-free routes.

S/N	Authors	Description
[18]	Swarna Priya R. M., SwetaBhattacharya, Praveen Kumar Reddy Maddikunta, Siva Rama Krishnan Somayaji, Kuruva Lakshmanna, Rajesh Kaluri, Aseel Hussien, Thippa Reddy Gadekallu	This paper introduced an energy-efficient cloud-based IoE framework to integrate cloud computing with the Internet of Everything and provide valuable services to consumers.

Proposed work

The proposed work is divided into four phases. First is the increasing of the network stability and energy efficiency in MANETs. This is done using a weight-based clustering scheme that focuses on electing a Cluster Head (CH) by using a weighted approach based on energy and node mobility. In the second part, efficient data traffic management is provided in heterogeneous networks when MANETs are connected to external networks. This is achieved using the data offloading mechanism. The data is offloaded in cases where the nodes in the network either have low data rate or low energy. This results in reduced energy consumption, traffic and better throughput in heterogeneous MANETs. Third is the increasing of the network lifetime and enhancing robustness to failure. This is done by designing a node-disjoint weighted multipath routing protocol where optimal paths are selected from the multiple paths chosen on the basis of a weighted scheme. The final phase issecuring the network against malicious attacks. This is achieved by designing a secure cryptography-based mechanism for MANETs that employs an Elliptic Curve Cryptography (ECC) encryption mechanism that provides security against malicious attacks and gives high throughput. Throughput in MANETs is increased considerably if protected against malicious attacks.

Phase1 –Weight-based energy-aware clustering scheme

Firstly, a clustering approach is designed which enables energy conservation, low communication traffic and overhead, and provides high network stability [47]. It is designed to set threshold valuesfor various parameters in dynamic ad-hoc environment. Environments like these haveunrestrained node movement and low bandwidth wireless channels along with energy limitations. The mechanism proposes the use of two types of CHs:primary and secondary for stable communication in spite of mobility of the nodes. It is an energy-aware and stable clustering mechanism. Here, the CH is chosenusing a weight-based approach that uses ideal energy and mobility parameters. The proposed scheme operates in the following phases:

1. Initialization of the network.
2. Selection of theCluster Head and formation of cluster.
3. Re-clustering and Re-association.

The following sub-sections elaborate these three phases.

The network is broken down into clusters which are made of CHs and cluster member nodes. All the cluster nodes have a unique number called the cluster ID. Every node stores its updated status value i.e., energy and mobility values. At the time of initialization, all the network nodes send HELLO messages. This message is a broadcast message. The objective of the HELLO message exchange is the identification of the transmission range of nodes. The strength of signal obtained between any node pair estimates the distance between them. It allows every node to determine its neighboring nodes, which are within the defined transmission range. It also defines the various messages exchanged during the process. The various steps involved in the initialization phase are as follows:

> Step 1: In the beginning, HELLO messages are periodically sent between network nodes. This process is used to notify neighbors about a node's presence. These messages contain the node ID, and its energy and mobility value.
> Step 2: During neighbor discovery, every node creates a list of its neighbors on the basis of HELLO messages received from different nodes.
> Step 3: After the discovery of neighbors, the process of selection of the Cluster Head begins.

Cluster head selection

The proposed technique uses a weighted metric for the CH selection [17]. The parameters used to calculate the weight are the mobility and energyof a node. Based on the application using the network, the parameters are assigned suitable weights. The sum of the weights of a node must always be equal to 1.

The weight of every node (n_i) presenting the network can be expressed by Eq. (1).

$$\boldsymbol{Weight}\ (\mathbf{n_i}) = \sum \mathbf{W_n} * \ \mathbf{P_n}(\mathbf{n_i}) \tag{1}$$

where for every noden_i:

w_n = weight assigned to n^{th} parameter

P_n = n^{th} parameter value of the node

In the proposed design, P_1 is the energy parameter, and P_2 is the mobility parameter

Hence, for the proposed scheme, Eq. (1) can be redefined by Eq. (2).

$$\boldsymbol{Weight}\ (\mathbf{n_i}) = \mathbf{w_1} * \mathbf{Energy}\ (\mathbf{n_i}) + \mathbf{w_2} * \mathbf{Mobility}\ (\mathbf{n_i}) \tag{2}$$

Once the *Weight* (n_i) values are calculated for all nodes, the node with the highest weight amongst its neighbors is chosen as the primary Cluster Head, and a cluster is formed.

The energy and mobility parameters used for the weighted metric calculation can be explained as follows:

1. Energy (P_1): The ad-hoc network devices have fixed inbuilt energy sources. The battery provides support to the nodes for a limited time. If the nodes have low energy, the network lifetime and throughput is reduced drastically. Therefore, an energy-efficient node's selection as CH is necessary for a stable clustering.

Energy model: Every node's energy is majorly dependent on the following energy used in receiving and sending data.

The scheme uses the following energy model for calculating the energy parameters P_1 [53]:

In time t, energy spent for transmission at a given node is given by Eq. (3) (in Joules).

$$\mathbf{E_{send}}\ (\mathbf{n_i}) = \mathbf{e_{send}}\ (\mathbf{n_i}) * \mathbf{q} / \mathbf{Bw}(\mathbf{n_i}) * \mathbf{total\ Bandwidth} \tag{3}$$

where,

E_{send} (n_i), e_{send}(n_i), Bw(n_i): For node i- energy used for transmitting q bits in time t, energy required for sending a single bit in time t and available bandwidth at time t.

And e_{send}(n_i) and Bw(n_i) are given by Eq. (4) and Eq. (5).

$$\mathbf{e_{send}}(\mathbf{n_i}\ ) = \mathbf{Initial\ energy}(\mathbf{n_i}) * (\mathbf{data\ rate/packet\ size}) * \mathbf{t} \tag{4}$$

$$\mathbf{Bw}(\mathbf{n_i}) = \mathbf{Sum\ of\ packets\ transferred\ till\ time\ t\ /Total\ time\ (t)} \tag{5}$$

Similarly, in time t, energy spent for reception at a given node is given by Eq. (6)

$$\mathbf{E_{rcv}}\ (\mathbf{n_i}) = \mathbf{e_{rcv}}\ (\mathbf{n_i}) * \mathbf{k} / \mathbf{Bw}(\mathbf{n_i}) * \mathbf{total\ Bandwidth} \tag{6}$$

where

E_{rcv}(n_i), e_{rcv}(n_i): same as above.

Hence, total energy E_{total} at any time for a given node (n_i)can be calculated as given in Eq. (7).

$$\mathbf{E_{total}}(\mathbf{n_i}) = \mathbf{E_{send}}\ (\mathbf{n_i}) + \mathbf{E_{rcv}}\ (\mathbf{n_i}) \tag{7}$$

Thus, remaining energyrεm at a node n_i, at any time t, is given by Eq. (8)

$$\mathbf{r\epsilon m}(\mathbf{n_i}) = \mathbf{Energy\ at\ the\ start}(\mathbf{n_i}) - \mathbf{E_{total}}(\mathbf{n_i}) \tag{8}$$

The initial energy is the energy of any node before it joins the network.

2. Mobility (P_2): The ad-hoc network supports node mobility so, frequent path breakages and connection losses occur. For stable clustering, less mobility nodes are required as CH, which can provide continuous connectivity among the nodes.

Mobility Model: To define mobility, it is assumed that in a real-time scenario, the speed of the host will be dependent on its previous speed and that there are no sharp changes in direction. For modeling this scenario, a temporal dependency approach, Gauss-Markov Mobility Model which uses node's correlated velocity is followed [52]. In the model, a mobile node's velocity should be related to time and can therefore be represented as a Gauss-Markov stochastic model. Simulating under a 2D field, this stochastic process can be modeled by Eq. (9):

$$\mathbf{V_t} = \boldsymbol{\alpha} * \boldsymbol{V}_{\mathbf{t-1}} + (\mathbf{1} - \boldsymbol{\alpha}\ ) * \boldsymbol{\mu} + \boldsymbol{\sigma} * \sqrt{\mathbf{1} - \boldsymbol{\alpha} * \mathbf{a})} * \mathbf{W_{t-1}} \tag{9}$$

V_t ,V_{t-1}: velocity of the node at two time instances t and t-1.

W_{t-1}: Random Gaussian process that is uncorrelated and exhibits 0 mean along with σ^2variance.

μ: Asymptotic mean.

σ: Standard deviation which is asymptotic.

α: Level of memory defined by dependency degree.

The value of α is between 0 and 1. α can be varied to model different mobility scenarios.

Once the parameter values have been calculated, the weight of a node is assigned as follows:

- The mobility and energy value parameters are P_1 and P_2.On the basis of a predefined scale, these parameters are assigned a value from 1 to 10. The mobility and energy values are calculated from the equations mentioned above. They are then assigned a fixed number depending on the energy and mobility ranges.
- A higher number is assigned when the residual energy value is high. For low values of mobility, a higher number is given.
- The final values of P_1 and P_2 with their corresponding weights w_1 and w_2 are substituted in Eq. 3.1. The sum of these weights is always equal to 1. The weights' values depend on the behavior of the network and the node.
- Under conditions where the network is energy-strained, the energy parameter is assigned a higher weight. In a highly mobile network, a higher weight is assigned to the mobility co-efficient.

For every set of nodes, their CH is selected using the weighted approach discussed above.

Cluster formation

In the proposed approach, every node in the cluster is at one-hop distance from the CH. All the nodes that fall under a particular range (predefined) of the selected CH become members of that cluster. The nodes lying outside initiate an iterative CH election process which continues till all the nodes either become part of a cluster or become the Cluster Head (CH) themselves. A threshold is also predefined for residual energy of the CH. Once this energy falls below the threshold, a new CH is assigned. Figure 2 below illustrates the flow of CH selection.

Phase 2—Data offloading in clustered MANET for data synchronization

Figure 3 illustrates the proposed data offloading mechanism with energy efficient clustering. Initially, once the network has been created, the neighbors exchange messages and a neighbor table is created. Clusters are created after the CH selection using the weighted scheme. Single-hop clusters with maximum capacity cluster head are designated to transform data received according to the data rate specifications.

To decide if offloading is needed, the following conditions are checked:

- If a node's energy goes below the specified threshold.
- If the rate at which a node processes the data is less than that of the CH.

The CH after receiving data from the external cellular network, has to convert the processing rate of data correspondence to the value of the data rates of the nodes that are a part of the cluster. The data is brokendown on the basis ofmember nodes' data requirements and the MTU size of the connecting link. Before any data transmission, the CH checks if the value of the available link data forwarding rate matches the defined data rate specifications. The data continues until there is no data left at the CH in the offloading queue.

The algorithm for the proposed scheme can be illustrated through the steps below:

Step 1: Initially, the specifications of the nodes are gathered while forming the clusters as described in Proposed work section. These include the energy parameter, mobility parameter, data rate, and link bandwidth.

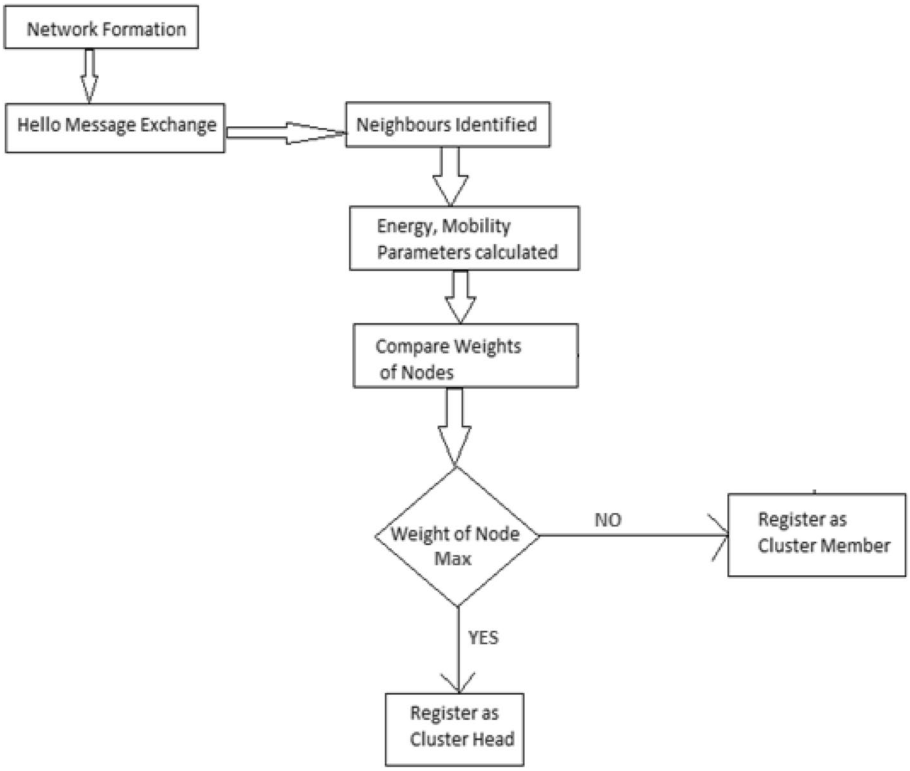

Fig. 2 Cluster formation flow diagram

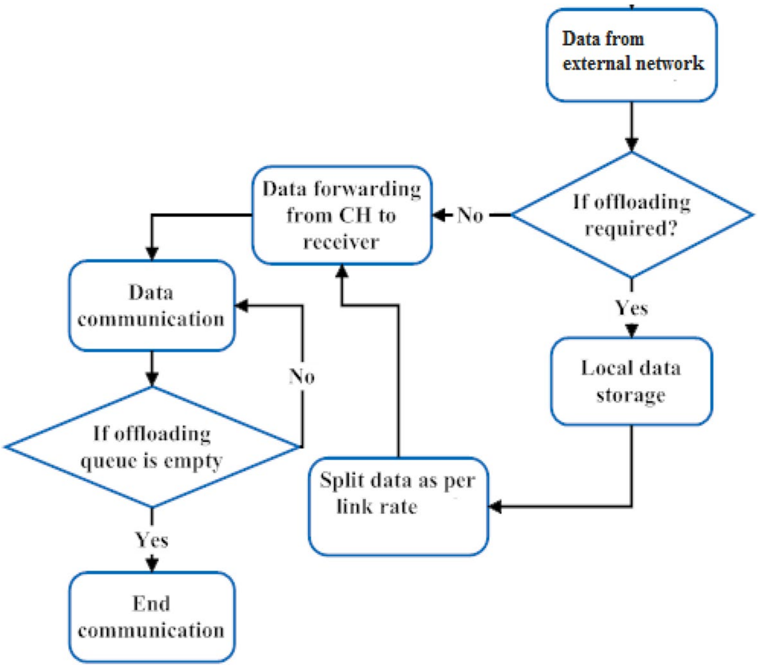
Data from external network
If offloading required?
No
Yes
Data forwarding from CH to receiver
Local data storage
Data communication
No
If offloading queue is empty
Yes
Split data as per link rate
End communication

Fig. 3 Flow for proposed data offloading mechanism with energy efficient clustering

Step 2: The CH verifies the data processing rate and energy of the corresponding member node.

Offloading condition

$$\textbf{Node data process in grate} < \textbf{CH data processing rate} \tag{10}$$

Or

$$\textbf{Node residual energy} < \textbf{10\% initial energy} \tag{11}$$

If either Eq. (10) or Eq. (11) are true, i.e., the nodes have lower data rate than their CHs or if the node's energy is getting low, the process of data offloading begins.

Step 3: The data is downloaded by the CH and stored in its own buffer.
Step 4: According to the data processing rate and link rate of the receiver, the CH later offloads the data to the remaining nodes.
Step 5: The CH takes control of partitioning the data packet, depending on the node requirements. It is done by checking the Maximum Transfer Unit (MTU) of the destination link. It then forwards data stored to the requesting node.
Step 6: Data transmission continues till the buffer at CH becomes empty.

Data traffic management using offloading

Next, the management of the network traffic with data forwarding is done utilizing the data offloading mechanism.

Figure 4 illustrates data traffic management in MANETs. The cluster includes different types of hostswith different data processing rate requirements. In a cluster, a member initializes communication by requesting data coming from the server host passing via the CH. The CH will then be able to receive data coming from the server by utilizing a 4G connection of about 30 Mbps. A mobile device processing capacity is between 2 and 7 megabits per second. In such case, the cluster must perform the data transmission based on the node's requirements as well as the processing power.

To conserve energy and bandwidth of the CH, the nodes with similar requests are grouped together by the CH in order to retrieve data from the server. It can thus avoid wastage of bandwidth and data traffic.

Phase 3 - weighted multipath energy-aware routing

With the movement, clustering and reorganization of nodes in MANETs, topology changes are inevitable. The rapid dissipation of energy and changes in nodes' topology leads to breakdown of paths. An optimal solution to this problem is missing in the existing schemes as explored in the last section.

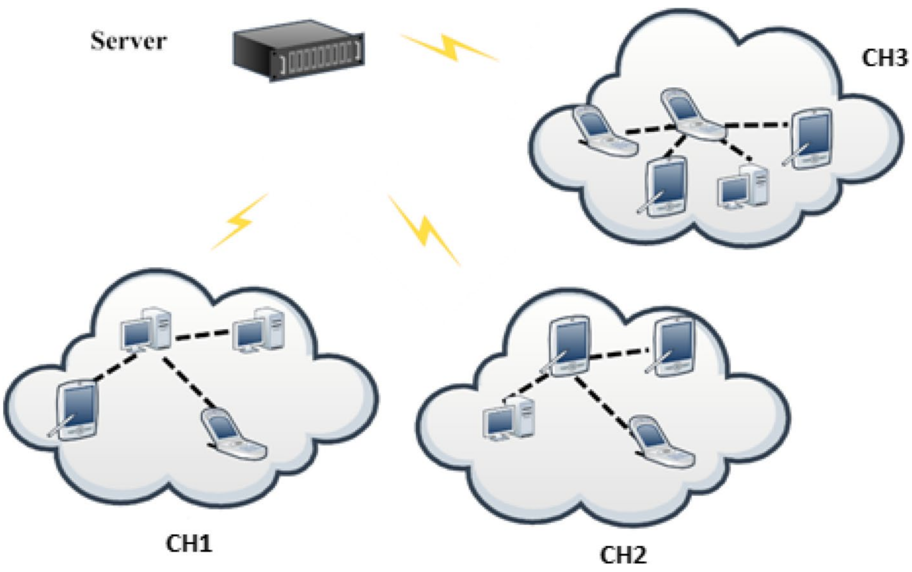

Fig. 4 Traffic management in MANETs

The proposed multipath process uses a weighted approach for selection of paths in networks with clusters, and has the following features:

- It is an energy-aware multipath routing protocol with the objective of establishing multiple optimal paths between node pairs.
- It maintains the backup paths in case of route failures or network breakdown.
- Energy and mobility values are used with weights for the multipath and CH selection. Thus, the network created is more stable and energy-efficient leading to increased network lifetime.
- The energy model uses the energy metric that helps in formation of a network that consumes less energy.
- Mobility of nodes is addressed through the Gauss-Markov mobility model whichhelps in attaining less restructuring of clusters and forming a stable network. This is achieved by choosing relatively fewer mobile nodes for the paths.
- Multiple paths are discovered using the weighted metric discussed in clustering, which is based on the energy and mobility parameters. Optimal paths out of these multiple paths are chosen considering the paths with lower weights.
- The Energy Efficient Clustering Approach (EECA), defined in Chapter 3 and 4, is used as the clustering technique. For routing, traditional Ad-hoc On-demand Multipath Distance Vector (AOMDV) is applied as the base protocol.

In a clustered network, for transmission of data, the cluster member passes the packet it wants to transmit to some other node, to the CH first. If both the source and destination nodesare in the same cluster, intra-cluster routing is applied. If it is part of another cluster, then inter-cluster routing is used. It uses three types of messages, like in other multipath routing frameworks: Route Request Message (*RREQ*), Route Error Message (*RERR*), and Route Reply Message (*RREP)* and [19].

Intra-cluster routing

In cases where both the destination and source are a part of the same cluster, the CH which receivesthe RREQ message from the sender node uses its neighbor table to get the destination details. It then sends back a reply RREP message to the sender node. A list of intermediate nodes between the sender and the receiver is maintained by the RREP message. Therefore, the sender gets the path to the destination which passes through the CH. Inintra-cluster routing, multipath routing is not feasible due to the one-hop distance between the CH and the member nodes.

Inter-cluster routing

In cases of the source and destination being parts of different clusters, the CH that receivesthe RREQ message from the source passes it to every neighbor CH. It is then further passed to neighbor CHs. In the process, addresses are collated, and paths are established following the information logged in at the previous node. On the route, links are set up using the route information of the previous path. The Cluster Head that gets the RREQ message looks for the destination address in its parent cluster. Once any CH finds it, the complete path is formed to the destination and stored. Finally, the RREP data packet at the destination CH uses the reverse path established to reach the source CH. This route goes through the previous neighboring CH on the way back.

In situations where the RREQ packet gets lost or dropped at some point in the network, the route discovery is redone a fixed number of times (depending on the network conditions). If it is still unsuccessful, the process is not repeated and the destination is stored as unreachable [2, 4, 54]. The steps involved used in finding multiple paths and selection of optimal paths during route discovery are described in detail below

Multipath selection

Step 1: The route discovery process is initialized by the source node. It sends the RREQ message to the CH of its own cluster.
Step 2: When a RREQ is received by a CH which is destined to a node in the same cluster, it will uni-cast the RREP message to the sender. If it is for a node outside this cluster however, the RREP is broadcasted to neighbor CHs.
Step 3: Every CH receiving a RREQ message checks its neighbor table for the destination in its own cluster. If it is not in its cluster, it further broadcasts the RREQ message to the neighboring CHs. The CHs during this process will store a list of all nodes that the packets have travelled through in their routing tables. This helps in sending the RREP packets back from the destination to the source with the help of the cumulative reverse path. A given CH can receive the same RREQs from different neighboring CHs. It forwards all such packets to its next neighboring CHs.
Step 4: The CH that has the destination node in its table transmits back the RREP to the sender CH through the cumulative reverse path.
Step 5: This reverse path is then stored in the CH's table.
Step 6: In case the RREP doesn't reach the source within the estimated round-trip time, the RREQ is considered to be lost or damaged.
The lost RREQ is handled by resending the same RREQ. In case of three consecutive unsuccessful attempts, the RREQ is discarded and the destination node is marked as unreachable by the source.
Step 7: During this process, an intermediate Cluster Head can receive multiple RREQs from different neighbors, thus generating multiple routes to the destination. The destination CH forwards all the RREP messages generated on the reverse paths as mentioned in the RREP message.
Step 8: The source CH receives all the multiple RREPs and sends them to the source node.

Optimal path selection

In a fixed time period, all the RREPs received are categorized into either *shortest* or *optimal paths*. The shortest paths are those which have the minimum number of hop counts. The optimal paths are generated using a weighted metric-based on *energy value* and *mobility coefficient* as described by Eqs. (1) and (2).

Parameters (P1 and P2) are assigned appropriate weights that are application-dependent. In applications where more energy saving is required, weight (w1) assigned to energy parameter, (P1) is given higher value, e.g., in military applications. In applications supporting high mobility node e.g., vehicular applications, the weight (w2) assigned to the mobility parameter (P2) is assigned higher values. In totality, the summation of w1 and w2 must be 1.

The total weight of any path is given by the sum of all nodes' weights lying on that path. As mentioned below, the weight W of path p_i, denoted by $W(p_i)$ is defined by Eq. (12) below:

$$\mathbf{W(p_i) = \sum Weight\ (n_i),\ for\ all\ nodes\ on\ the\ path\ p_i} \tag{12}$$

All the paths having weight, $W(p_i)$ above the defined threshold are accepted, and the paths not satisfying a particular predefined threshold for the path weights are rejected. Hence, the selected paths are those paths which satisfy the following weight condition.

Let the weight of the path with maximum weight value be denoted as $Max(W(p_i)$.The path p_i with weight $w(p_i)$ is selected only if it satisfies the Eq. (13):

$$\mathbf{W(p_i) > 0.7 * Max\ (W(p_i))} \tag{13}$$

All the other received paths are rejected. The various steps for the selection of optimal paths are shown in a flow diagram in Fig. 5.

Phase 4- Secure routing through cryptography

The primary aim of the proposed method is to increase thesecurity of MANETs by implementing signature generation and cryptographic mechanisms. The working process of the proposed Secure Cryptography-based

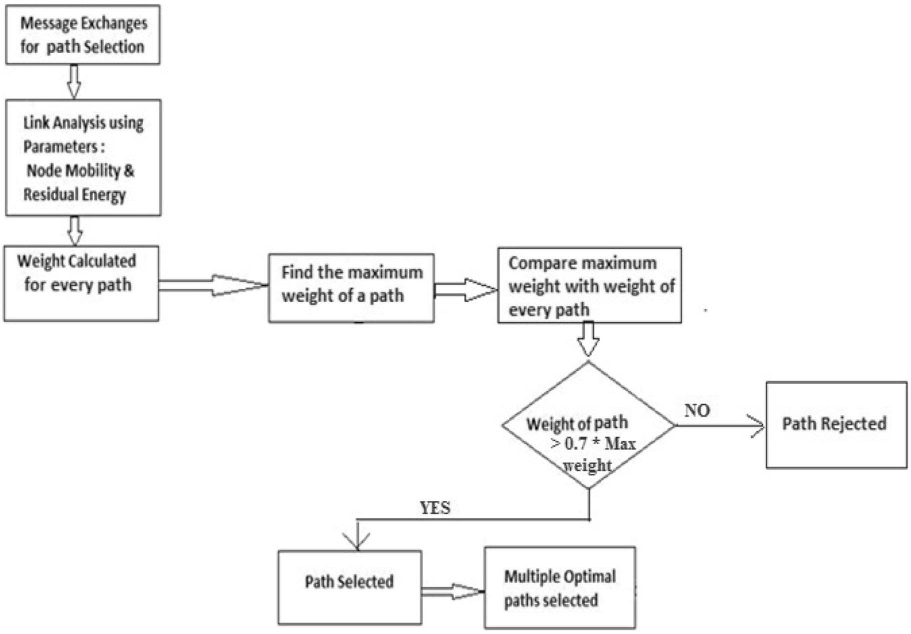
Message Exchanges for path Selection
Link Analysis using Parameters : Node Mobility & Residual Energy
Weight Calculated for every path
Find the maximum weight of a path
Compare maximum weight with weight of every path
Weight of path > 0.7 * Max weight
NO
Path Rejected
YES
Path Selected
Multiple Optimal paths selected

Fig. 5 Flow of the proposed weighted multipath routing

Clustering Mechanism (SCCM) can be described briefly in the steps below:

Step 1: Cluster formation using the weight-based energy efficient approach as discussed in Phase 1 and multipath formation using the Weighted Multipath approach.
Step 2: Public key generation
Step 3: Packet encryption using Elliptic Curve Cryptography (ECC) at the sender side
Step 4: Signing the encrypted message using Schnorr's digital signature
Step 5: Signature verification and message decryption using a private key at the receiver side.

Once the cluster members register themselves with the CH, the key generation and sharing processes are performed in each cluster. When the data transmission request is initiated by the source towards the destination, a secure route is established between them. It uses the proposed weighted multipath routing protocol as the base routing technique.

Before transmission, the original packet is encrypted using the Elliptic Curve Cryptography (ECC) technique. ECC belongs to the category of asymmetric public key encryption that generates smaller and more efficient keys very fast compared to other techniques. It is based on the elliptic curve theory that uses the properties of elliptic curve equation. ECC creates keys by simply generating a random integer in a certain range though securely. These can be used as private keys. The ECC points i.e., pairs of integers coordinates lying on the curve are used as public keys.

Next, the signature is produced for the encrypted data using Schnorr's signature generation technique. Schnorr's digital signature is known for its simplicity. It is based on Schnorr's algorithm and its security is built on the property of un-traceability of discrete logarithmic problem. The ECC encrypted and Schnorr's signed data packet is sent to the destination through the respective Cluster Heads. The destination node on accepting the packet, regenerates the signature for decrypting the original data. During this process, the received packet is verified for correctness. The destination node discards the received packet, and transmits the error report to its CH. Thus, the proposed scheme ensures message confidentiality, integrity and authentication.

Figure 6 below illustrates the flow of various steps through which the proposed protocol works:

Secure data routing

The WMECS protocol is used to perform the multipath routing among the source node and destination node, where multiple paths are selected during data transmission. This provides an alternate path if there is any fault or failure on the selected path. It also reduces the data loss and delay in the network by using multiple paths.

Encryption at the sender

After establishing the secured path between the source and destination, the Elliptic Curve Cryptography technique is utilized to encrypt the data to be sent. ECC offers fast computation and reduced resource consumption for

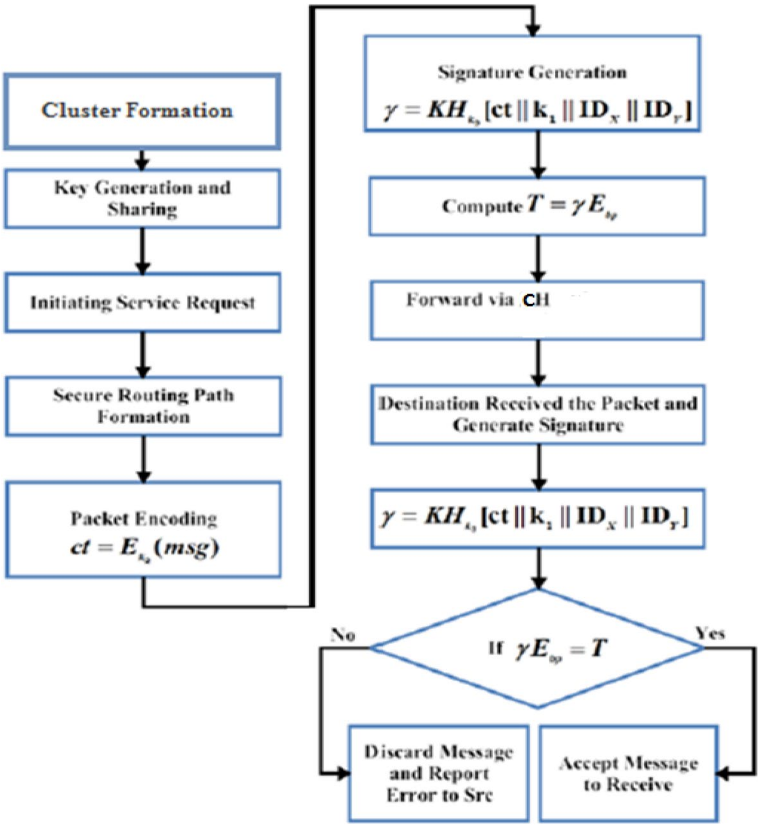
Cluster Formation
Key Generation and Sharing
Initiating Service Request
Secure Routing Path Formation
Packet Encoding
$ct = E_{k_s}(msg)$
Signature Generation
$\gamma = KH_{k_s}[ct \| k_1 \| ID_x \| ID_y]$
Compute $T = \gamma E_{k_p}$
Forward via CH
Destination Received the Packet and Generate Signature
$\gamma = KH_{k_s}[ct \| k_1 \| ID_x \| ID_y]$
If $\gamma E_{k_p} = T$
No
Yes
Discard Message and Report Error to Src
Accept Message to Receive

Fig. 6 Flow diagram for the proposed scheme

cryptographic operations at minimum cost. The power of the ECC algorithm is fully based on the key and the alphabetical table. It also gives a possible outcome for the data by enabling the secure transmission of keys between the communication entities. Different characteristics are symbolized in this technique as the coordinates of the curves. Because of its capability to generate the complex encrypted data that is difficult to decipher by unauthorized user, ECC has been selected for the proposed technique.

Signature generation at the sender

After data encryption, the Schnorr's signature generation algorithm is used for the generation of the signature for the encrypted data. It is a kind of key generation mechanism that integrates both digital signature and public key encryption schemes. It analyzes the discrete logarithmic problem for generating the digital signature, which increases the security of the network. The signature generation process has the following steps:

- Setup
- Key generation at the sender's side
- Key generation at the receiver's side
- Signcryption
- Unsigncryption

In this technique, the source verifies the public key of the packet using the digital certificate. The keys for generating the cipher text are generated using a random integer. The one-way key hash function is deployed in the mechanism to create an encrypted text which is transmitted to the destination with the generated signature. The one-way keyed hash function alters input messages of several lengths into output series of fixed length, called a hash value, which is usually shorter than the input length. Hash values are often used to spot input sequences, i.e., to allot to them some distinctive values that illustrate them.

Results

In this section, the performance evaluation of existing and the proposed mechanismis done using various parameters: Control Packet Overhead, Packet Delivery Ratio (PDR), average end-to-end delay, and throughput. The experiments are conducted in two phases.

In the first phase, the non-ECC-secure existing techniques considered in this analysis are Flooding Factor

Table 4 The simulation parameters

Parameters	Value
Simulation Time	100 s
Topology size	1200 X 1000 m2
Number of nodes	> 100
Pause Time	3–5 s
Max speed	50 m/s
Traffic type	CBR
Packet size	1024bytes
Wireless Channel Capacity	2Mbps
Routing Protocol	Modified AOMDV
Transmission Range	< 250 m (thresh 150 m)
Mobility model	Gaussian Markov
Wireless Standard	802.11b

based Trust Management (F3TM), Cooperative Opportunistic Routing in MANET (CORMAN), and the Protocol for routing in Interested-defined Mesh Enclaves (PRIME).

In the next phase, ECC-secure techniques are considered for evaluation, namely Enhanced Adaptive Acknowledgment (EAACK) which is an ECC-secured Non-Clustered Routing Protocol and Intuitive Clustered Cryptography (ICC) which is an ECC-secured Clustered Routing Protocol. The simulation settings of the proposed environment are depicted in Table 4.

Phase-1

The network performance is analyzed for SCCM and compared with other existing non-ECC secure protocols, namely PRIME, CORMAN and F3TM in the attackers' presence in the network.

Control packet overhead

This signifies the approach's efficiency in the presence of malicious nodes. It is measured in frames/packets. It is calculated based on link maintenance, discovery of nodes and latency. Typically, the generated control packets and received data packets are helpful in finding the overhead ratio of the network. Based on this, the presence of theattacker in the network is identified and blocked as the attacker doesn't have the destination signature.

Figure 7 illustrates the control packet overhead of existing PRIME, CORMAN, F3TM and proposed SCCM protocols with respect to the amount of attackers. When likened to existing techniques, the proposed SCCM efficiently decreased the control packet overhead by transmitting the message through CH and use of an efficient security mechanism.

Packet delivery ratio

Figures 8 and 9 illustrate the PDR of the existing and proposed protocols with respect to the amount of nodes and attackers.

From the above, we noted that if the amount of attackers in the network increase, the PDR of the network decreases. When likened to existing techniques, the proposed SCCM shows better PDR by efficiently blocking the malicious nodes in the network.

It can be seen from the above that with increase in the amount of nodes, PDR stays almost constant for all the

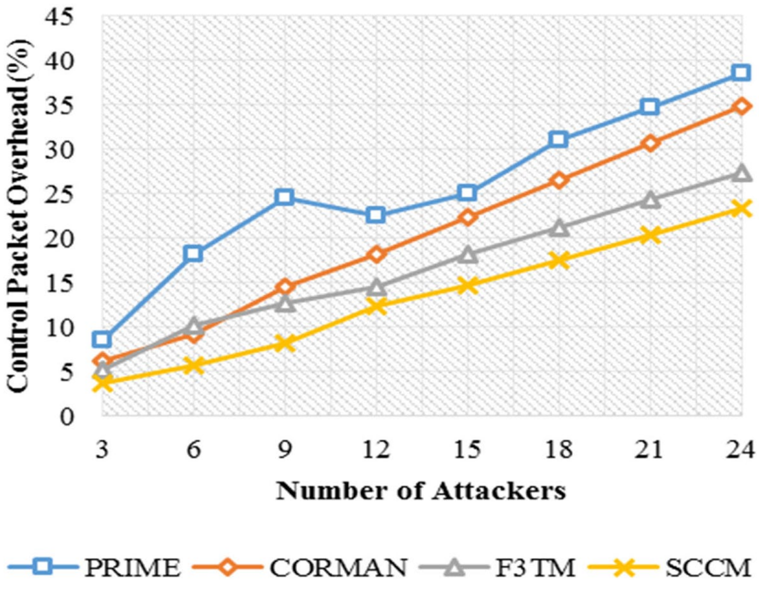

Fig. 7 Control packet overhead vs. attacker nodes

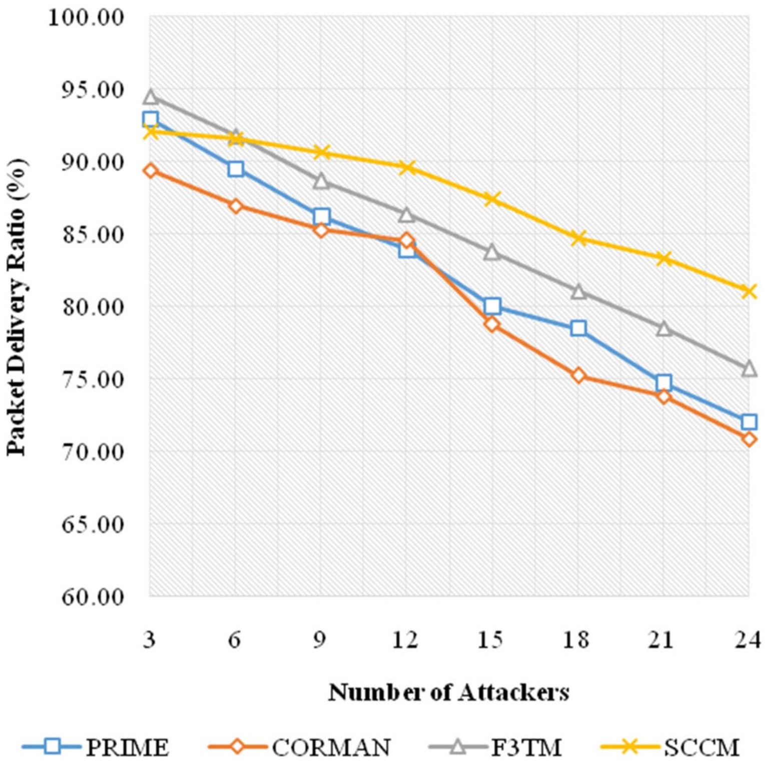

Fig. 8 PDR vs number of attackers

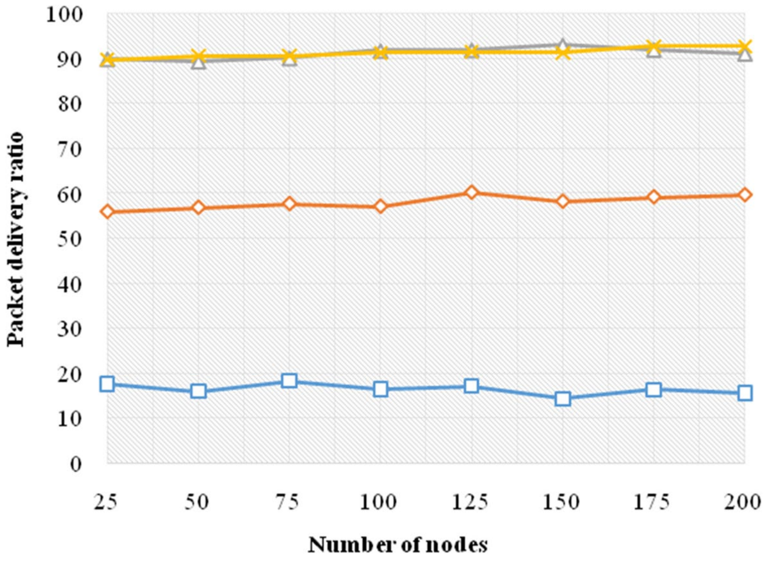

Fig. 9 PDR vs number of nodes

protocols. It is maximum for SCCM as it uses multiple paths for forwarding the packets. So, in case there is any failure, it uses an alternate path for further communication, which improves the PDR.

Average end-to-end delay

Figures 10 and 11 illustrate the average end-to-end delay of the proposed and existing protocols in terms of the amount of nodes and attackers. In this evaluation, it is observed that

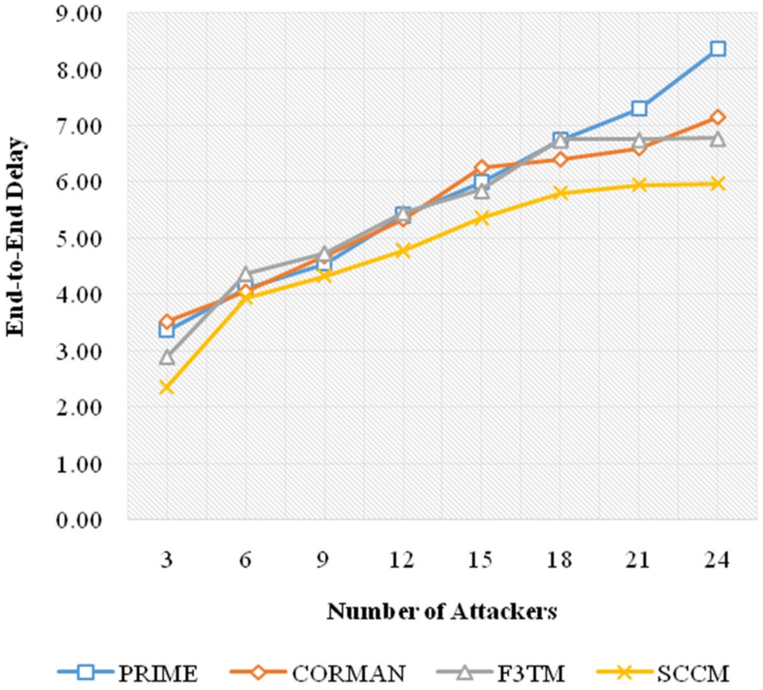

Fig. 10 Average end-to-end delay vs number of attackers

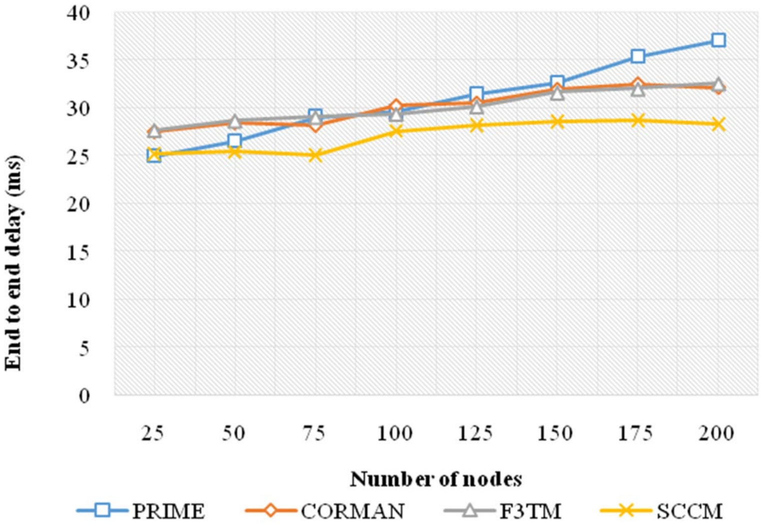

Fig. 11 Average end-to-end delay vs number of nodes

the proposed SCCM provides the lowestend-to-end delay, when likened to existing techniques. This is due to the use of efficient CH, multiple paths and lightweight security for transmission in the proposed scheme.

Figure 12 illustrates the performance of the proposed SSCM technique. It has an improved throughput in the attackers' presence, when compared to the other techniques. This is due to the combined use of clustering, multipath routing, and efficient security that makes the performance better.

Phase-2

The network performance is analyzed for SCCM and compared with other existing ECC-secure protocols, namely EAACK and ICC in the presence of attackers in the network.

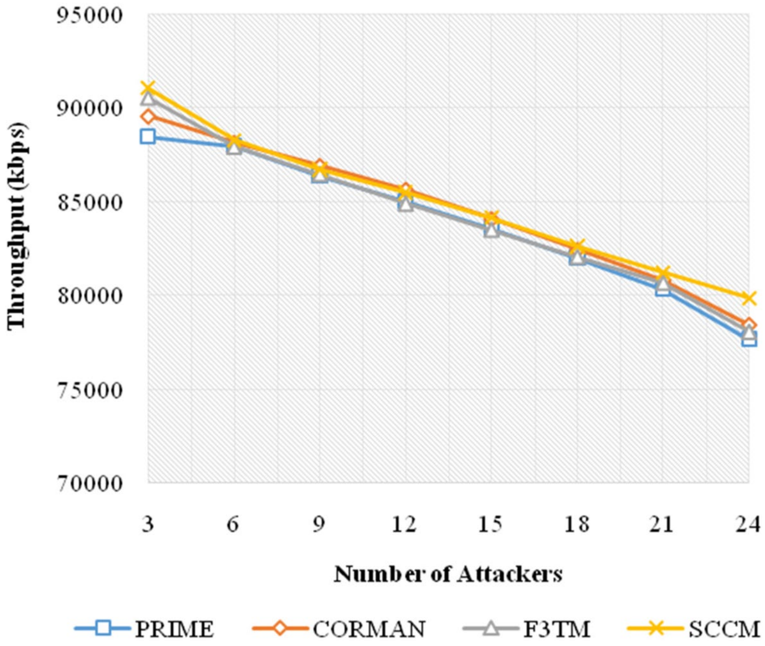

Fig. 12 Throughput vs number of attacker nodes

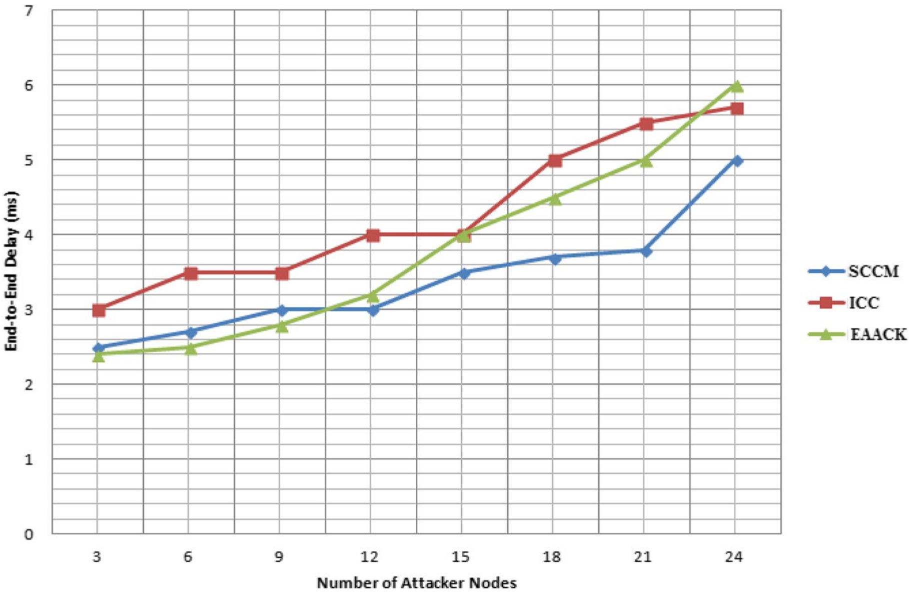

Fig. 13 Average end-to-end delay vs number of attacker nodes

End-to-end delay

Protocols are analyzed for performance with respect to throughput and delay with increase in number of attacker nodes.

Figure 13 describes the average end-to-end delay of both the existing and proposed methods with respect to the amount of attacker nodes. With increase in the amount of malicious nodes, the packet starts getting delays. The result reveals that the proposed SCCM provides less end-to-end delay compared to the other methods due to the use of efficient security and routing.

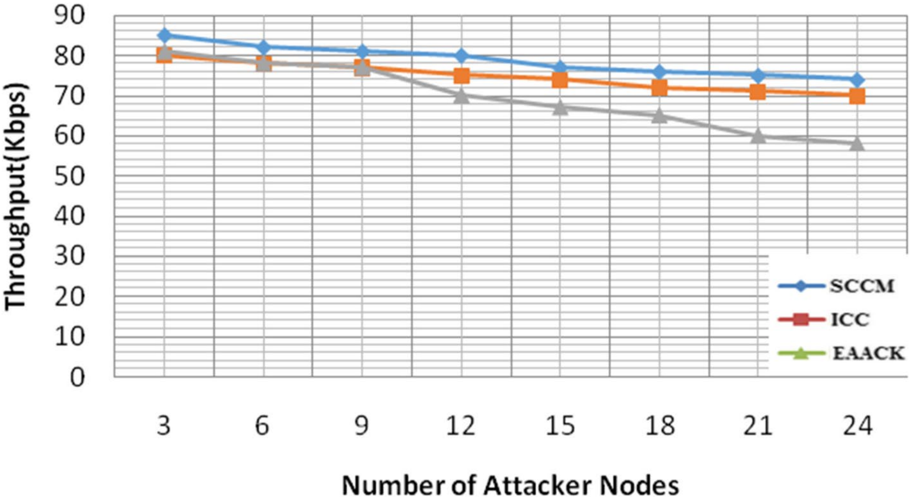

Fig. 14 Throughput vs number of attacker nodes

Throughput

In this analysis, we proved that the suggested SSCM technique has a better throughput when likened to the other techniques. This is due to the combined use of clustering, multipath routing and efficient security.

Figure 14 describes the impact of increase in the amount of attackers on throughput. With increase in theamount of malicious nodes, the throughput starts decreasing for all as packets are dropped. The decrease is lowest in the proposed SCCM technique when compared to the other techniques due to the use of a pool of CHs and multipath routing with an efficient security mechanism.

Conclusion

This work proposes an efficient mechanism, the SCCM, for providing security for MANETs with increased throughput. Message confidentiality and authentication are the major considerations of this work. Here, the WMECS routing protocol is used for the selection of multiple paths during transmission to avoid packet loss and reduce the delay time. Then, the ECC-based encryption mechanism is utilized to encrypt the original packet before transmitting it to the receiver. The Schnorr's algorithm is also employed to produce the signature for the encrypted data, which increases the security of the packet. Once the destination receives the packet, it verifies whether the packet is valid or not. If it is valid, it regenerates the signature using Schnorr's algorithm, and applies the ECC decryption mechanism to decrypt the data. During simulation, several metrics are utilized to test the outcomes of the SCCM technique. The performance analysis is measured in terms of various performance metrics. The performance of the existing techniques is evaluated against the proposed technique for proving the efficacy. It is seen that the proposed frame work performs better compared to the other techniques. In the near future, we shall change the topology of the MANET using algorithm. In this regard, nodes in MANETs are allowed free movement within or outside the network to cause frequent location change, link breaks, and packet goal. The goal is to mitigate the challenges of MANET using our proposed algorithm.

Acknowledgements
We would like to thank anonymous reviewers for useful suggestions. This work was supported by the National Natural Science Foundation of China (No.61862051), UTM Research Fellow (00P27), the Science and Technology Foundation of Guizhou Province (No.ZK[2022]549, No.[2019]1299), the Top-notch Talent Program of of Guizhou province (No.KY[2018]080), the Natural Science Foundation of Education of Guizhou province(No.[2019]203) and the Funds of Qiannan Normal University for Nationalities (No. qnsy2018003, No. qnsy2019rc09, No. qnsy2018JS013, No. qnsyrc201715).

Authors' contributions
Conceptualization by Tao Hai, Dan Wang; Methodology by Dayang Jawawi; Software by Ye Lu and Jincheng Zhou; formal analysis by Dawang Jawani and Edeh Michael Onyema. Investigation by Tao Hai and Dan Wang; Resources and data collection by Jincheng Zhou, Cresantus Biamba; Writing by: Dan Wang, Ye Lu and Tao Hai; Validation by: Michael Edeh and Jincheng Zhou; Funding Acquisition by Cresantus Biamba. The author(s) read and approved the final manuscript.

Funding
The project was supported by the Department of Culture Studies, Religious Studies and Educational Sciences, University of Gävle, Gävle, Sweden.

Availability of data and materials
The supporting data can be provided on request.

Declarations

Ethics approval and consent to participate
The research has consent for Ethical Approval and Consent to participate.

Consent for publication

Consent has been granted by all authors and there is no conflict.

Competing interests

The authors declare no competing interests.

Author details

[1]School of Computer and Information, Qiannan Normal University for Nationalities, Duyun 558000, China. [2]Faculty of Computing, Universiti Teknologi Malaysia (UTM), Skudai, Johor Bahru, Johor 81310 UTM, Malaysia. [3]Key Laboratory of Complex Systems and Intelligent Optimization of Guizhou Province, Duyun 558000, China. [4]School of Computer & Communication, Lanzhou University of Technology, Lanzhou 730050, China. [5]School of Mathematics and Statistics, Qiannan Normal University for Nationalities, Duyun 558000, China. [6]Department of Vocational and Technical Education, Faculty of Education, Alex Ekwueme Federal University, Ndufu-Alike, Nigeria/ Saveetha School of Engineering, Saveetha Institute of Medical and Technical Sciences, Chennai, India. [7]Department of Educational Sciences, School of Mathematics and Statistics, Faculty of Education and Business Studies, University of Gävle, Gävle, Sweden.

Received: 30 August 2022 Accepted: 15 September 2022
Published online: 29 April 2023

References

1. Sakhaee E, Jamalipour A (2008) Stable clustering and communications in pseudolinear highly mobile ad hoc networks. IEEE Trans Veh Technol 56(8):3769–3777
2. Silva L et al (2021) Computing paradigms in emerging vehicular environments: a review. IEEE/CAA J Autom Sin 8(3):491–511. https://doi.org/10.1109/JAS.2021.1003862
3. Huiyao A, Xicheng L, Wei P (2004) A cluster-based multipath routing for MANET. Computer School, National University of Defense Technology, Changsha, China, pp 405–413
4. Huang H, Huang C, Ma D (2020) A method for deploying the minimal number of UAV base stations in cellular networks. IEEE/CAA J Autom Sin 7(2):559–567. https://doi.org/10.1109/JAS.2019.1911813
5. Chatterjee M, Das SK, Turgut D (2009) A weight based distributed clustering algorithm for mobile ad hoc networks. HiPC, LNCS 1970:511–521
6. Asif W, Qaisar S (2011) "Energy and path aware clustering algorithm for mobile ad hoc networks. ICCSA, Part IV, LNCS 6785:133–147
7. Basu P, Naidu W (2012) A mobility based metric for clustering in mobile ad hoc networks," in International conference on Distributed computing systems workshop. pp 413–418
8. Zhong J, Huang Z, Feng L, Du W, Li Y (2020) A hyper-heuristic framework for lifetime maximization in wireless sensor networks with a mobile sink. IEEE/CAA J Autom Sin 7(1):223–236. https://doi.org/10.1109/JAS.2019.1911846
9. Shukla N (2013) Mobile Ad-Hoc Network (MANET): Security Issues Regarding Attacks. in International Journal of Computer Applications (0975–8887), National Conference on Recent Trends in Engineering and Management "NCRTEM-2013
10. Sudha K, Ranjith JP, Ganapathy S, Sasidharan MSR (2015) Secure transmission over remote group: a new key management prototype. Int J Comput Sci Netw Secur (IJCSNS) 15(1):101
11. Morris R, Jannotti J, Kaashoek F, Li J, Decouto D (2010) CarNet: A Scalable Ad Hoc Wireless Network System. Proc. of 9th ACM SIGOPS European Workshop, Kolding, Denmark
12. Grossglauser M, Tse D (2001) Mobility increases the capacity of ad-hoc wireless networks. Proc. of INFOCOM'01. pp 1360–1369
13. Steenstrup M (2001) Cluster-Based Networks. Chapter 4, Ad Hoc Networking, edited by C. E. Perkins, Addison-Wesley
14. Neethu V, Singh AK (2015) Mobility aware loose clustering for mobile ad hoc network. Procedia Comput Sci 54:57–64
15. Sung S, Seo Y, Shin Y (2010) Hierarchical clustering algorithm based in mobile ad hoc networks. ICCSA, LNCS 3982:954–963
16. Loutfi A (2014) An energy aware algorithm for OLSR clustering. Ann Telecommun 69:201–207
17. Basurra SS, De Vos M, Padget J, Ji Y, Lewis T, Armour S (2015) Energy efficient zonebased routing protocol for MANETs. Ad Hoc Netw 25:16–37
18. RM SP, Bhattacharya S, Maddikunta PKR, Somayaji SRK, Lakshmanna K, Kaluri R, Hussien A, Gadekallu TR (2020) Load balancing of energy cloud using wind driven and firefly algorithms in internet of everything. J Parallel Distrib Comput 142:16–26. https://doi.org/10.1016/j.jpdc.2020.0.2.010
19. Kulkarni SB, Yuvaraju B (2016) Challenges and issues of cluster based security in MANET. IOSR J Comput Eng (IOSR-JCE) 18:01–05
20. Kaur I, Rao A (2017) A framework to improve the network security with less mobility in MANET. Int J Comput Appl 167:21–4
21. Jhaveri RH, Patel NM (2015) A sequence number based bait detection scheme to thwart grayhole attack in mobile ad hoc networks. Wireless Netw 21(8):2781–2798
22. Kavitha P, Mukesh R (2018) Detection of impersonation attack in MANET using polynomial reduction algorithm. IJ Network Security 20(2):381–389
23. Singh M, Gagangeet S (2015) A secure and efficient cluster head selection algorithm for MANET. J Netw Commun Emerg Technol (JNCET);2. www.jncet.org
24. Chakeres ID, Belding-Royer EM (2004) AODV routing protocol implementation design. In 24th International Conference on Distributed Computing Systems Workshops. USA, 2004. Proceedings. 7:698–703. IEEE
25. Panke T (2013) Clustering based certificate revocation scheme for malicious nodes in MANET. Int J Sci Res Publ 3:1–5
26. Ammayappan K, Sastry VN, Negi A (2008) Cluster based multihop security protocol in MANET using ECC. In: TENCON 2008–2008 IEEE Region 10 Conference. Hyderabad, India, IEEE, pp 1–6
27. Gupta P (2016) A literature survey of MANET. Int Res J Eng Technol 03(02):95–9
28. Dhenakaran DS, Parvathavarthini A (2013) An Overview of Routing Protocols in Mobile Ad-Hoc Network. Int J Adv Res Computer Sci Softw Eng. 3:251–259
29. Taneja S (2010) A survey of routing protocols in mobile ad hoc networks. Int J Innov Manag Technol 1(3):279
30. ALGhafran L, Yusof ZBM (2015) An efficient load balancing clustering algorithm for mobile ad hoc networks. Int J Comput Commun Instrum Eng (UCCIE) 2(2):215–9
31. Chatterjee M, Das SK, Turgut D (2002) WCA: a weighted clustering algorithm for mobile ad hoc networks. Clust Comput 5:193–204
32. Camp T, Boleng J, Davies V (2002) A survey of mobility models for ad hoc network research. Wirel Commun Mob Comput 2(5):483–502
33. Zhang X (2016) A street-centric opportunistic routing protocol based on link correlation for urban manets. IEEE Trans Mob Comput 1:1–1
34. Grover D, Saini S (2015) A survey on unicast routing protocols in mobile ad-hoc networks. Int J Adhoc Ubiquitous Comput 5:697–702
35. Djemili F, Tolba C (2013) A mixed approach load balancing and efficient energy for multi-path routing in mobile ad hoc networks. In: SENSORS, IEEE, Baltimore, MD, USA, IEEE, pp 1–4
36. Spyropoulos T, Psounis K, Raghavendra C (2010) Performance analysis of mobility-assisted routing. In Proc. MobiHoc '06: 7th ACM International Symposium on Mobile Ad Hoc Networking and Computing. pp 49–60
37. Xinming Z, Dong S, Fengfu Z (2010) Integrated routing metric for mobile ad hoc networks. J Softw 20(11):3077–3085
38. He G (2002) Destination-Sequenced Distance Vector (DSDV) Protocol. Helsinki University of Technology Finland Magazine 135:1–9
39. Li X, Cuthbert L (2014) Stable node-disjoint multipath routing with low overhead in mobile ad hoc networks. In The IEEE Computer Society's 12th Annual International Symposium on Modeling, Analysis, and Simulation of Computer and Telecommunications Systems Volendam, The Netherlands: IEEE, pp. 184-191.https://doi.org/10.1109/MASCOT.2004.1348196
40. Gharib M, Moradlou Z, Doostari MA, Movaghar A (2015) Fully distributed ECC-based key management for mobile ad hoc networks. Comput Netw 113:269–283
41. Moradlu Z, Doostari MA, Gharib M, Movaghar A (2013) Fully distributed self certified key management for large-scale MANETs. In: 2013 IEEE 10th International Conference on Ubiquitous Intelligence. Vietri sul Mare, IEEE, pp 96–102
42. Kim J, Tsudik G (2012) SRDP: Secure route discovery for dynamic source routing in MANETs. Ad Hoc Netw 7(6):1097–1109

43. Tavli B, Heinzelman WB (2004) MH-TRACE: multihop time reservation using adaptive control for energy efficiency. IEEE J Sel Areas Commun 22:942–953
44. Bharany S, Badotra S, Sharma S, Rani S, Alazab M, Jhaveri RH, Gadekallu TR (2022) Energy efficient fault tolerance techniques in green cloud computing: a systematic survey and taxonomy. Sustain Energy Technol Assess 53, Part b:102613. https://doi.org/10.1016/j.seta.2022.102613
45. Ruby B, Onyema EM, Khalid KA, Celestine I, Shahab SB, Tripti S, Amir M (2022) Assessment of dynamic swarm heterogeneous clustering in cognitive radio sensor networks. Wirel Commun Mob Comput 7359210:1–15. https://doi.org/10.1155/2022/7359210
46. Zhao Y, Gupta RK, Onyema EM (2022) Robot visual navigation estimation and target localization based on neural network. Paladyn J Behav Robot 13(1):76–83. https://doi.org/10.1515/pjbr-2022-0005
47. Hong X, Xu K, Gerla M (2002) Scalable Routing Protocols for Mobile Ad Hoc Networks. IEEE Network 16:11–21. https://doi.org/10.1109/MNET.2002.1020231
48. Sinha P, Sivakumar R, Vaduvur B (2001) Enhancing Ad Hoc Routing with Dynamic Virtual Infrastructures. Proc. of the Twentieth Annual Joint Conference of the IEEE Computer and Communications Societies (INFOCOM 2001)
49. Karaoglu B, Heinzelman W (2015) Cooperative load balancing and dynamic channel allocation for cluster-based mobile ad hoc networks. IEEE Trans Mob Comput 14:951–963
50. Salonidis T, Bhagwat P, Tassiulas L, LaMaire R (2001) Distributed topology construction of Bluetooth personal area networks. Proc. of IEEE Infocom'01
51. Chakrabarti S, Mishra A (2001) QoS issues in ad hoc wireless networks. IEEE Commun Mag 39:142–148
52. Kwon TJ, Gerla M (2009) Clustering with power control. Proc. of IEEE Military Communications Conference (MILCOM '99)
53. Lin CR, Gerla M (2007) Adaptive clustering for mobile wireless networks. IEEE J Sel Areas Commun 15(7):1265–1275
54. Onyema EM, Dalal S, Romero CAT et al (2022) Design of intrusion detection system based on cyborg intelligence for security of cloud network traffic of smart cities. Springer J Cloud Comp 11:26. https://doi.org/10.1186/s13677-022-00305-6

Publisher's Note

Springer Nature remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.