JOURNAL OF MECHANICS OF CONTINUA AND MATHEMATICAL SCIENCES
www.journalimcms.org

ISSN (Online) : 2454 -7190, Special Issue, No.-7, February (2020) pp 108-130 ISSN (Print) 0973-8975

ENERGY EFFICIENT AND AUTHENTICATED ROUTING IN MANET FOR EMERGENCY RESCUE OPERATIONS

J. Nandhini[1], K. Mahalakshmi[2], K. K. Savitha[3], A. S. Narmadha[4], Ms. G. Kalaiarasi[5]

[1]Professor, ECE, Jai Shriram Engineering College, Tirupur, Tamil Nadu

[2]Associate Professor, ECE, Kuppam Engineering College, Kuppam, Andra Pradesh

[3]Associate Professor, MCA, Baradhiyar University PG Extension Center, Erode, Tamil Nadu

[4,5]Research Scholar, ECE, Jai Shriram Engineering College, Tirupur, Tamil Nadu

Corresponding Author: nandhoosaran@gmail.com

https://doi.org/10.26782/jmcms.spl.7/2020.02.00008

Abstract

MANET is an emerging technology that allows the users to interact without physical infrastructure irrespective of geographical location. In particular, energy efficient routing is the most important design for network operation due to the effect of increased data rates in wireless networks. The security aspects are to be considered for an efficient routing. The main challenge and research area in MANET is a route path identification, intrusion detection and energy consumption. Energy maintenance is the most important issue to be handled in order to avoid the excess usage of resources by mobile nodes which lead to route path breakup. Due to the lack of central server and infrastructure in MANET, security problems are to be addressed in order to preserve the network from attackers. In this work, techniques are proposed to handle energy efficient routing in the clustered environment while maintaining trustworthiness and security under emergency rescue conditions. Nodes are simulated using NS 2 and performance parameters are compared with existing algorithms.

Keywords: MANET, Security, Authentication, Routing, Energy efficiency, Clustering.

I. Introduction

Device in MANET identifies the existence of additional devices and performs essential set up for the communication and sharing of data. Ad hoc networking uses

The Paper Presented at 14th International Conference on Intelligent System and Control (ISCO'20) Organized by The Department of Computer Science and Engineering, Karpagam College of Engineering, Coimbatore, India

the devices to preserve the connection to the network. It also controls or manages the adding and removing of devices to and from the network. With nodal mobility, network topology changes randomly over time. The network is distributed in which the network organization and message delivery are carried out by nodes. Message routing is a key problem in decentralized environment where the topology varies.

MANETs are constructed from a number of moveable devices and develop a new research trend. MANET's has number of different features such as scalability, fault tolerance and autonomous system that allows the network with or without any trusted authority. These unique features make it suitable for the most significant applications in emergency and rescue operations. During emergency conditions, the needs of distributing the information between the rescuers are very significant. However, since this network is functioning based on wireless settings, it is susceptible to threats and intruders. Information flow in MANET is interrupted and it enhances a security issues in particular information sharing between nodes in emergency condition in MANET. Therefore, a different approach to enhance data security through emergency rescue operation is required.

In order to initiate a rescue operation, a temporary network communication and information communications are made in the afflicted area. Rescuers need to discuss between group members and organize the rescue operation. Information requires to communicate from the teams and the rescue operation center and conversely in order for the rescue work and save lives. By using a small mobile device, the information is transmitted from one rescue group member to another group member. Figure 1 illustrates the rescue operation attained by different afflicted area based on the operation center.

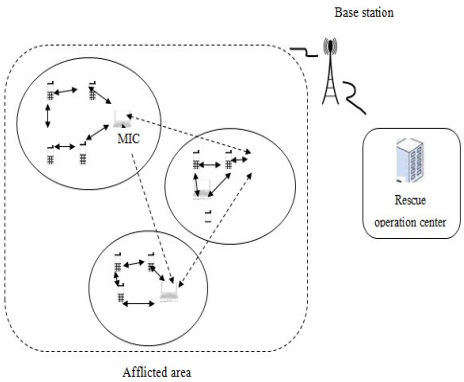

Fig. 1: MANET with Emergency Rescue Operation

Figure 1 reveals that the process of emergency rescue operation in MANET. The Mobile unit transmits networking tools to support routing operations. It has been widely used for supporting the communications between the several mobile devices connected to the Mobile Information Collector (MIC) (i.e. leader) which is in a

stationary condition. It is also broadly used in emergency services such as search and rescue operations. The number of mobile units in ad hoc networks is connected to other units through the wireless communications.

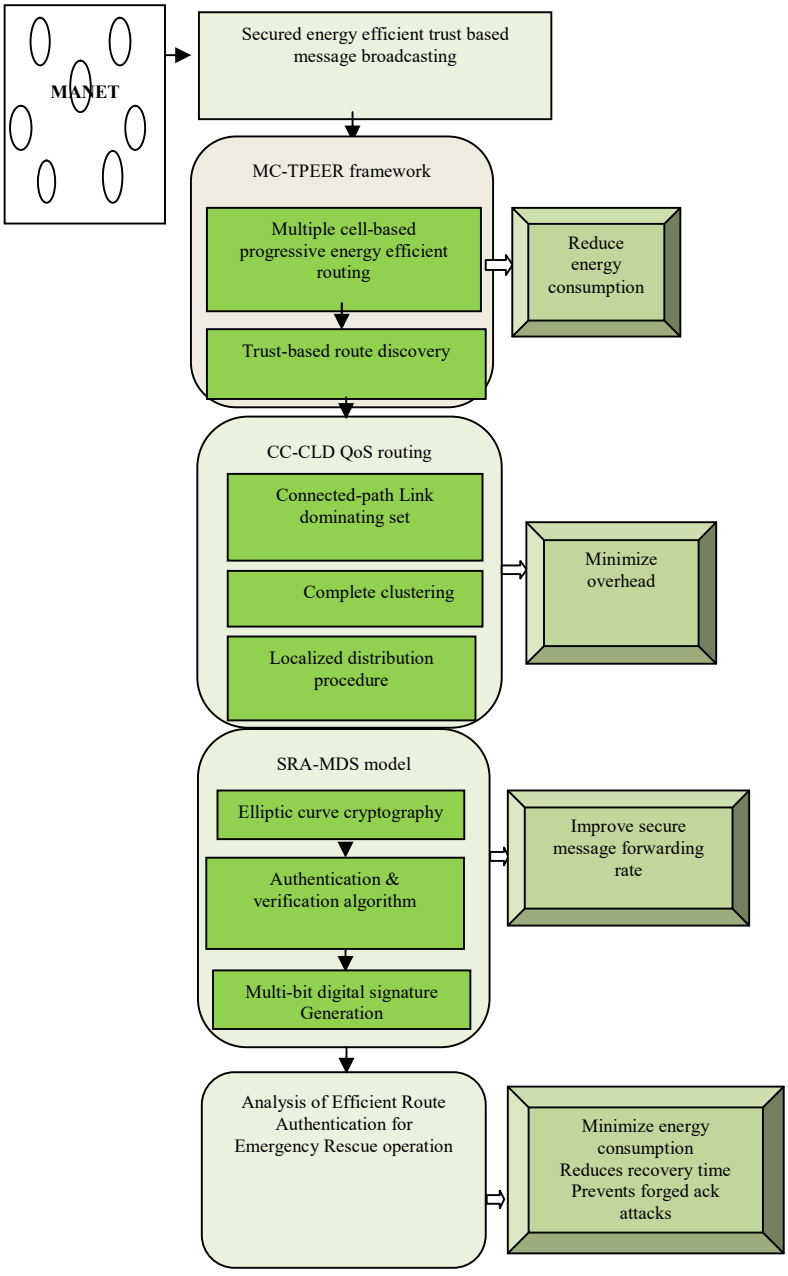

Fig. 2: Block diagram of the proposed method

Figure 2 proposes the block diagram of the proposed method. In rescue operations, the rescue team shares the information between the group members in the afflicted location with secured manner. MANET technique usually allows the team to share the information with each other without any fixed infrastructures. Each team member has the unique controller to distribute their information. This information is distributed to a rescue operation center by way of the mobile base station. In order to improve the emergency rescue operation, three different methods are significantly developed to analyze the efficient route authentication for secured information sharing in MANET.

II. Related Works

Mohamed Mahmoud &XueminShen (2012) briefed a secure payment scheme with low communication and processing overhead for multihop wireless networks. To increase cooperation of nodes, packet transmission management and to implement fairness, report-based payment scheme is designed for multi-hop wireless networks. HaiyingShen&Lianyu Zhao (2013) presented ALERT with an anonymous location-based efficient routing protocol in MANETs. ALERT divides the network field into zones and select nodes in zones as intermediate relay nodes to discover the non-traceable anonymous route.

Ming Li et al. (2015) proposed an energy consumption optimization for multi-hop cognitive cellular networks. Multi-hop Cognitive Cellular Network (MC2N) architecture is designed to use the ever report data transmissions in cellular networks. Pradip De et al. (2010) proposed an energy-efficient Reprogramming of a swarm of Mobile sensors (ReMo). ReMo is an energy efficient, multi-hop reprogramming method designed for mobile sensor networks. ReMo downloads pages using the mobility of the nodes and using a fast transfer of the code.

Seyed Amin Hosseini Seno (2011) briefed an energy efficient cluster based routing protocol for MANETs. With MANET features, all mobile nodes of network join with each other through wireless medium with key features. MadhukarRao et al. (2011) presented an energy efficient reliable routing protocol for MANET. An important difficulty is the routing protocol design. Node failures and link breaks in network results in loss of the network resources. It connects the constant paths, battery power and signal strength of nodes to attain QoS parameters.

Jinhua Zhu &Xin Wang (2011) studied a model and protocol for energy-efficient routing over MANET. An energy-efficient routing protocol execute much worse than a normal routing protocol. The minimum energy routing schemes designed fails to consider the routing overhead and node mobility. Floriano De Rango et al. (2012) discussed link-stability and energy aware routing protocol in distributed wireless networks. Energy awareness for computation and protocol management is an important factor in the plan of protocols and algorithms.

JavadVazifehdan et al. (2014) briefed an energy-efficient, reliable routing with residual energy in wireless ad hoc networks. For wireless ad hoc networks, two energy-aware routing algorithms termed Reliable Minimum Energy Cost Routing

(RMECR) and Reliable Minimum Energy Routing (RMER) are designed. RMECR manages three essential needs of ad hoc networks such as energy-efficiency, reliability and high network lifetime.

Ha Dang &Hongyi Wu (2010) proposed clustering and cluster based routing protocol for delay-tolerant mobile networks. By taking surveys of distributed clustering scheme, a cluster-based routing protocol is presented for Delay-Tolerant Mobile Networks (DTMNs). The main aim is to collect the mobile nodes with same mobility pattern into a cluster.

Tao Shu&Marwan Krunz (2010) briefed coverage-time optimization for clustered wireless sensor networks with a power-balancing approach. Based on the accessibility of location information, optimization formulations are created with deterministic and stochastic systems through Rayleigh fading model for inter-cluster communications. Two mechanisms are designed for attaining balanced power consumption in the stochastic container with a routing-aware optimal cluster mapping and a clustering-aware optimal random relay.

AshishBagwari et al. (2011) briefed routing protocol behavior with multiple cluster head gateway in MANET. The Ad hoc wireless network is a multi-hop network that generates a group of mobile nodes in the shared wireless channel. Karunakaran&Thangaraj (2011) presented a cluster based service discovery protocol for MANET. The nodes contain limited bandwidth resource and include high mobility.

YuvrajKumbharey et al. (2013) briefed Renovated Cluster Based Routing Protocol (RCBRP) for MANET. A new CBRP is discussed to decrease the routing overhead and enhance the routing discovery by joining the inter-cluster on-demand and intra-cluster table-driven routing. It enhances the results in the throughput while compared with the pure AODV Routing protocol.

Surendran Subbaraj & PrakashSavarimuthu (2014) studied Eigen trust-based non-cooperative game model. In MANET, selfish behavior is examined when nodes fail to forward data packets. It is a type of misbehavior that interrupts the network operations. A QoS-constrained Eigen trust-based non-cooperative game model is proposed for securing fault-tolerant ant look ahead routing. It discovers the trusted valid route and look-ahead route pairsin deciding the alternate path in route failure.

Keshav Kumar Tiwari& Sanjay Agrawal (2013) studied a secure reputation-based clustering algorithm for cluster based energy optimized MANET. A secure clustering algorithm proposed is derived from the reputation of threats in clustering. The nodes reputation is used to enhance the security of cluster estimated through joining the presence of the node in the routing process.

Iftikhar Ahmad et al. (2013) proposed improved QoS protocol for real time traffic in MANET. Multimedia applications required to be maintained. A level of QoS support is necessary for real time data. The designed protocol presents the necessary QoS without negative impact on best effort data traffic. An efficient route discovery

mechanism for AODV routing protocol and transmission methods are designed for real time data.

Zhongyuan Qin et al. (2015) discussed an efficient key management scheme based on Elliptic Curve Cryptography (ECC) and AVL tree for large scale wireless sensor networks. A new efficient key management scheme is derived from ECC and AVL tree for large scale WSNs.

Fan-Hsun Tseng et al. (2011) discussed a survey of black hole attacks in wireless MANETs. The intruders employ the loophole to implement their malicious actions as the route discovery process is essential and predictable. The survey of the presented solutions and modern routing methods is discussed. The method also classifies the proposals into a single black hole attack and collaborative black hole attack and examines the group of solutions.

ElhadiShakshuki Nan Jang &TarekSheltami (2013) proposed Enhanced Adaptive ACKnowledgment (EAACK) with a secure intrusion detection system for MANETs. The mobility and scalability of wireless network creates feasibility in various applications. In modern wireless networks, MANET is an essential and distinctive application. The entire single node functions as a transmitter and a receiver. It is essential to increase efficient intrusion-detection mechanisms to preserve MANET from attacks.

Kamal Kumar Chauhan&Amit Kumar Singh Sanger (2012) discussed securing MANETs with key management and routing. In MANETs, a mobile node functions as an end terminal and an intermediate router. A routing protocol is secured that detects the damaging effects of malicious nodes. In key management system, new node and group leader verifies each other before connecting the network. The secure routing protocol permits both communicating parties and intermediate nodes to confirm other nodes and protects message integrity.

AmolBhosle&YogadharPandey (2013) studied secure data using a symmetric encryption in MANET. The MANET has many nodes that communicate with each other without any infrastructure. The security of network is a key issue. To improve the security of network, secured routing protocol AODV is planned with the use of Symmetric Encryption Algorithm (AES). It secures the data and maintains the confidentiality. In addition, node authentication is carried out with IP address, AODV routing protocol and digital signature method.

Sourav Bhattacharya et al. (2015) briefed robust and energy efficient trajectory tracking of mobile devices. Sensor management steps are necessary to present a high and application-changeable level of robustness despite the user's transportation mode. The efficiency of designing technique is carried out with a series of emulation experiments on real world datasets composed from different modes of transportation on mobile devices from two dissimilar platforms.

Ziane Sara &Mekki Rachida (2015) discussed an energy-efficient inter-domain routing protocol for MANETs**.** The outing techniques are based on clustering

techniques, ACO and virtual coordinates. Inter-domain routing proposal is derived from bee's communication to control a dynamic topology in inter ad hoc networks. The key aim is to design an energy efficient inter-domain routing protocol for MANETs with low overhead.

III. Energy Efficient Protocol

A new technique called as MC-TPEER framework is used to minimize the energy consumption on sharing the information through different mobile units during the emergency conditions. Initially, MC-TPEER follows the shortest routing path scheme for minimizing the energy rate for multiple mobile units in message broadcasting between the rescuers. Generally, the different member in every group randomly moves in the afflicted region. Though the mobile information collector is remain stationary at the base center for each group. The movable mobile unit (members) starts by searching the entire shortest route path and picks up the minimal energy consumption path in MANET for sharing the information. This information is collected by the mobile information collector that acts as team leader.

Each leader acts as the central authority for entire mobile units in rescue area. In addition, MIC also acts as a gateway to the rescue operation center that provides information about the area. This helps to select the minimal energy conservation path for information sharing. After the energy efficient path selection, trust based route identification is carried out for secure information sharing between the groups. Each member in a group sends a RREQ message to another member about the afflicted area. The information is shared only by the certain group members and identifies whether the route is a trusted route or not using the threshold value.

The threshold value is attained based on selecting the shortest route path for sharing the information with minimum resource utilization. This helps to reduce the minimum energy consumption. When the route path is identified RREP messages are transmitted through the same route to member in a particular group. However, a stabilized clustering approach is not effectively performed to organize movable mobile nodes for further increasing the information sharing between the groups of rescuers.

IV. Clustering Mechanism

A CC-CLD QoS routing framework is developed to achieve high clustering efficiency in MANET. Initially, a significant operation is carried out to cluster the similar route path; Connected-path Link Dominating set is introduced. The number of movable mobile users (member) form a similar type of route path are clustered together to make a hierarchical control mobile network environment. The mobile users utilize the clustered group for broadcasting the information about the rescue area in a connected path. The connected-path link dominant set consist of the cluster head (mobile information collector) pruning rules to remove the repetition (i.e. unauthorized members). The removal of repetition reduces the collision factor to ensure data sharing between groups of rescuer and preserves the data integrity. In the CC-CLD framework, each group has a unique ID with link path information of start

node point and end node point to minimize the recovery time. Finally, clustering is performed in MANET using a localized distribution algorithm. The distributed movable mobile users are analyzed using the CC-CLD framework. Moreover, link path between connected dominating sets is monitored to group the closely related structure route path with minimal energy consumption rate. However, it fails to handle the efficient route authentication during the information sharing.

V. Authentication Using Cryptography

In order to reduce the unauthorized member and improves the security level during information broadcasting, SRA-MDS model is designed. A wide SRA-MDS model is designed to maintain the access to data and information required during emergency rescue operation. Sender route authentication in MANET is established using ECC schemes. With the application of elliptic curve in SRA-MDS model, it verifies the members using a single cryptographic equation, aiming at reducing the network overhead. Authenticated members are selected for message broadcasting using authentication and verification algorithm. This helps only authenticated member, be a member of the correct group obtain an access to the message requested.

The authentication and verification algorithm is used to reduce the unauthorized members from attaining the requested data. Finally, shared messages are preserved using MDS generation. A single request digital signature with several mobile users is used to highly secure the transmitted message about the rescue area. This Digital Signature generation approach used to differentiate the role between members' of the each group at the emergency rescue operation. This helps to avoid the incorrect data communication between members in the group at the emergency rescue operation. Therefore, this helps to enhance the data security and privacy among the different groups of rescuers.

In order to analyze the performance of three proposed methods MC-TPEER framework, CC-CLD and SRA-MDS model, experiments are conducted in the NS2 simulator tool. The mobility model selected based on the Random Waypoint Model (RWM) to perform multipath packet transmission in MANET. In this random waypoint mobility model, a source node randomly selects the destination node. The RWM uses a different number of mobile nodes for locating the movable nodes. The mobile nodes vary from 10 to 70. The simulation time varies from 300 seconds to 2100 simulation seconds. The nodes are initially placed within a fixed size of 1000 m * 1000 m on network coverage area with a velocity of 0 – 50 m/s in a square area. Three proposed method uses 70 mobile node and 63 data packets for experimental purposes. The mobile nodes use DSR protocol to perform the experiment on randomly moving objects. VBR data flow is used where each node generates 10 packets/seconds with a packet size of 512 bytes. For each state, seven different simulations are performed and the results are averaged.

VI. ANALYSIS OF PARAMETER BASED ON MC-TPEER FRAME WORK, CC-CLD QOS ROUTING FRAME WORK AND SRA-MDS MODEL

Simulation is conducted for proposed MC-TPEER, CC-CLD QoS routing and SRA-MDS model with existing User Authentication and Intrusion Detection in MANET (UA-ID). Simulations are carried out to measure the factors in terms of energy consumption on broadcasting the message, shortest path identification time, trust level on broadcasting the message, recovery time and routing overhead packet delivery ratio, secure message forwarding rate and forged acknowledged attacks.

VI.i Measurement of Energy Consumption

Energy Consumption (EC) on message distribution is measured using the energy consumed by a single mobile node with respect to the total mobile nodes in MANET during the emergency conditions.

Table 6.1 describes the effectiveness of three proposed methods MC-TPEER, CC-CLD QoS routing and SRA-MDS model with existing UA-ID.

Table 1: Energy Consumption

No. of nodes	Energy consumption in Joules (J)			
	UA-ID	MC-TPEER	CC- CLD	SRA-MDS
10	82	55	65	72
20	87	63	72	78
30	93	69	79	85
40	98	74	84	90
50	95	71	80	87
60	107	80	92	98
70	115	85	97	106

Table 1 illustrates the proposed MC-TPEER provides better performance than the other proposed methods and existing UA-ID mechanism.

Figure 3 illustrates the performance of energy consumption on broadcasting the message based on number of mobile units in the transmission afflicted area.

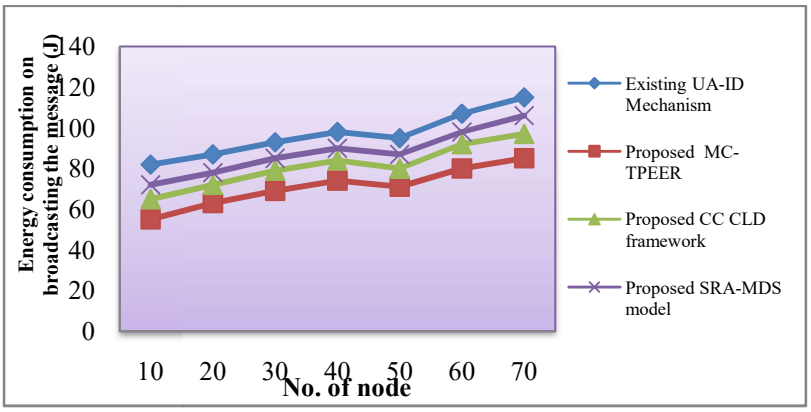

Fig. 3: Energy consumption

The proposed MC-TPEER provides better performance than the other proposed CC-CLD, SRA-MDS model and existing UA-ID mechanism. The results reported confirm that with the increase in the number of mobile units, the energy consumption for path selection also increases but it is not linear. In proposed MC-TPEER model achieves minimum energy consumption. By applying the method, efficient message broadcasting is performed using multiple units in information broadcasting between the rescuers during the emergency condition. In addition, this routing identifies the adjacent members to identify the route path for efficient message sharing with minimum resource utilization. This helps for minimal energy conserving path during the emergency conditions. Therefore the energy consumption rate is reduced by 37% as compared to existing UA-ID. Similarly, the other proposed methods, CC-CLD framework and SRA-MDS model also reduces the energy consumption by 19% and 10% respectively.

VI.ii. Measurement of Shortest Path Identification Time

The shortest path identification time is the time taken to identify the minimum energy conserved path through the intermediate mobile units with respect to the number of mobile users in rescue area.

Table 2 describes the measurement of shortest path identification time based on different numbers of mobile nodes in the range of 10, 20, 30 and 70 respectively.

The results of shortest path identification time using the proposed MC-TPEER, CC-CLD and SRA-MDS model with existing UA-ID mechanism is shown in Figure 4.

Table 2: Shortest Path Identification Time

No. of nodes	Shortest path identification time in milliseconds			
	UA-ID	MC-TPEER	CC-CLD	SRA-MDS
10	19.3	10.5	15.7	13.6
20	25.8	17.3	22.3	20.4
30	32.9	24.1	29.8	27.3
40	33	23.9	29.5	26.9
50	38.3	29.6	35.6	32.7
60	38.4	29.2	35.2	32.1
70	41.6	33.5	38.6	36.1

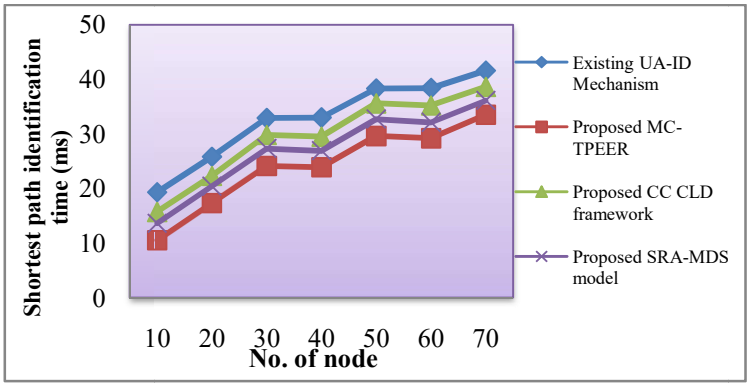

Fig. 4: Shortest Path Identification Time

The proposed MC-TPEER differs from the other methods by the application of Multiple Cell Energy Efficient Routing algorithm with sequence of neighboring mobile users comprising multiple cells with minimum energy conservation path at different time intervals. This helps in reducing the path identification time for sharing the information about the afflicted area using the MC-TPEER framework by 42% as compared to existing UA-ID. Likewise the proposed CC-CLD and SRA-MDS framework produces minimum identification time of 12% and 23% when compared to existing UA-ID mechanism.

VI.iii. Measurement of Average Trust Level

The trust based message broadcasting is obtained using multiple mobile users and Trust-based Progressive Energy Efficient Routing framework. It is measured in terms of percentage (%).

Table 3 illustrates the average value of the trust level on broadcasting the message based on three proposed methods MC-TPEER, CC-CLD and SRA-MDS framework and existing UA-ID mechanism.

Table 3. Average Trust level

Methods	Average Trust level in percentage (%)
UA-ID	62.71
MC-TPEER	78.32
CC-CLD	65.37
SRA-MDS	70.45

Efficient trust based message broadcasting is accomplished for securing the information sharing between the groups. The proposed MC-TPEER framework improves the performance result.

Figure 5 shows the measurement of average value of the trust level on broadcasting the message.

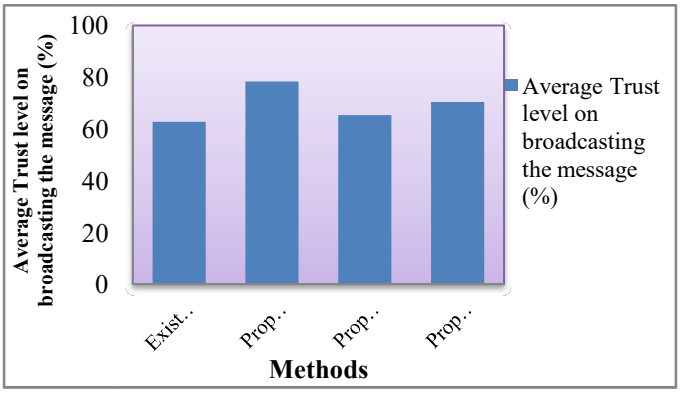

Fig. 5: Average Trust level

Trust level on broadcasting the message is improved using the MC-TPEER framework than the other proposed CC-CLD, SRA-MDS model and existing UA-ID mechanism. This is because of the application of trust-based route discovery algorithm for secure information sharing between the groups. Every member in a group forwards a request message to another member about the afflicted area. The information is distributed only by the particular group members and identifies whether the route is a trusted route or not using the threshold value. The threshold value is used for selecting the shortest route path with minimum resource utilization. This avoids the outside group from sending a request to leader, and improves the trust based information sharing between the rescuers.

This in turn improves the trust level on broadcasting the message using the MC-TPEER framework by 20% when compared to existing UA-ID mechanism. Moreover, the CC-CLD and SRA-MDS framework increases the trust based message distribution of 4% and 11% as compared to existing UA-ID mechanism in MANET.

VI.iv. Measurement of Recovery Time

The recovery time is defined as the amount of time taken to recover accurate route path for information sharing between the group members and collector in emergency rescue operation.

Table 4 illustrates the accurate path recovery time of proposed MC-TPEER, CC-CLD and SRA-MDS framework and existing UA-ID mechanism.

Table 4: Recovery Time

Clustered route path	Recovery time in milliseconds			
	UA-ID	MC-TPEER	CC CLD	SRA-MDS
1	50.25	44.13	35.85	39.65
2	52.35	47.38	39.33	43.44
3	55.41	50.12	42.88	46.54
4	53.67	49.17	41.34	44.37
5	57.68	52.64	44.16	48.26
6	60.67	55.48	47.29	51.34
7	62.23	57.21	49.28	52.89

The CC-CLD QoS routing framework is used to recover the accurate route path for packet transmission in MANET using unique cluster ID. The mobile users utilize the cluster group for broadcasting the information about the rescue area in a connected path. The experiments are conducted using the clustered route path in the range of 1 to 7.

The targeting simulation result of recovery time with respect to number of clustered route path is shown in Figure 6.

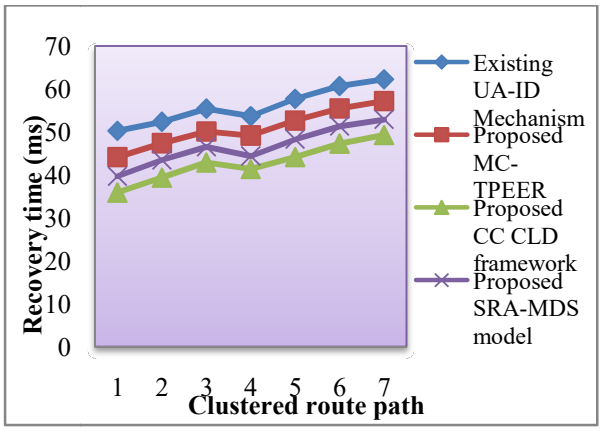

Fig. 6: Recovery Time

Figure 6 provides the visual comparison based on different moving speed of the mobile nodes in MANET. It is also revealed that the proposed CC-CLD framework overcomes the existing approach in that clustering is incorporated with the help of unique ID to easily increase the number of users through different route paths for multiple sources. The connected link path between dominating sets is monitored in the CC-CLD framework to group the closely related structure route path for rapid information sharing during the emergency conditions. This helps to reduce the recovery time for path identification to share the information between group members. For the most different speed rate, the CC-CLD framework attains comparable values than the other methods.

The recovery time is significantly reduced by applying link-path structure for movable mobile users with the help of unique ID. The application of complete clustering in the CC-CLD framework initializes the cluster ID for each group that increases the message broadcasting performance and therefore reduces the recovery time by 31% when compared to existing UA-ID mechanism. The recovery time of proposed MC-TPEER and SRA-MDS framework is also reduced by 10% and 20% when compared to existing UA-ID mechanism respectively.

VI.v. Measurement of Routing Overhead

Table 5 depicts the experimental results for network routing overhead based on the number packets sent varies from 9 to 63.

Table 5: Network Routing Overhead

No.of packet sent	Routing overhead in percentage			
	UA-ID	MC-TPEER	CC-CLD	SRA-MDS
9	56	50	45	40
18	59	54	50	44
27	62	57	53	47
36	61	56	51	45
45	65	60	55	49
54	67	61	56	51
63	68	63	59	53

In order to measure the network overhead, the number of information's are sent between the different mobile users in operational area. The information received at the other member in the group varied according to the three different methods. Compared to other methods, the overhead is reduced in SRA-MDS model.

Figure 7 illustrates the measurement of network routing overhead based on the proposed MC-TPEER, CC-CLD and SRA-MDS framework and existing UA-ID mechanism.

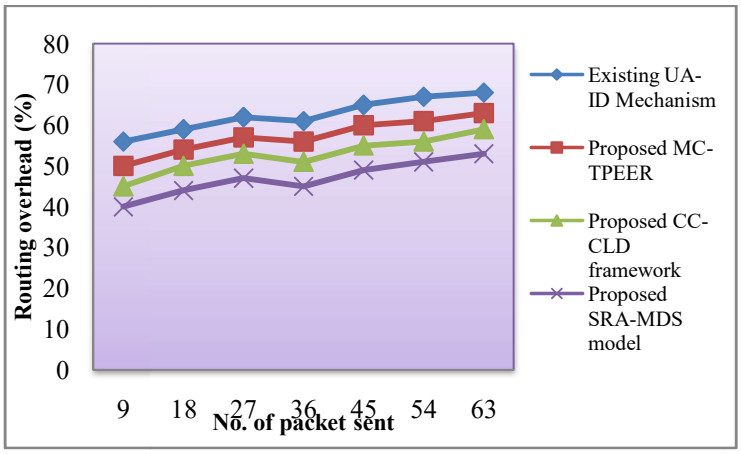

Fig. 7: Network Routing Overhead

The proposed SRA-MDS model comparatively minimizes the routing overhead because of the application of ECC scheme. With the application of elliptic curve in SRA-MDS model, it verifies the number of group members for sharing the information. This cryptography schemes are also used to enhance the data security such as confidentiality, integrity and non-repudiation. It also used to ensure data privacy. Using these components, the SRA-MDS model efficiently authenticates the route and significantly reduces the network routing overhead by 33% as compared to existing UA-ID.

Furthermore, using a single cryptographic equation, the member in certain group identifies information sharing measures of neighboring member, using confidence value and probability measure with minimum network overhead. In addition, the Digital Signature generation approach used to distinguish the role between members' of the each group at the emergency rescue operation. This helps to avoid the incorrect data communication between members in the each group. Thereby, overhead is reduced in SRA-MDS model to enhance the data security. In addition, the proposed MC-TPEER and CC-CLD framework reduces the routing overhead by 9% and 19% as compared to existing UA-ID.

VI.vi. Measurement of Packet Delivery Ratio

Packet delivery measurement of proposed MC-TPEER, CC-CLD framework and SRA-MDS model with respect to data packets being sent is shown in Table 6.

Table 6: Packet Delivery Ratio

No. of packet sent	Packet delivery ratio in percentage			
	UA-ID	MC-TPEER	CC-CLD	SRA-MDS
9	50.78	76.53	69.77	63.24
18	55.64	79.48	72.49	66.54
27	56.12	81.79	75.88	70.14
36	56.14	80.21	75.13	69.13
45	60.33	84.98	79.25	74.24
54	63.47	86.92	80.76	75.41
63	64.56	87.67	82.87	77.45

The packet delivery ratio using proposed MC-TPEER framework uses a mobile unit sharing the message and also supports routing operations in MANET. It has been widely used for supporting the communications between the several mobile devices connected to the mobile information collector. Therefore, the comparative results are shows that the MC-TPEER framework efficiently selects the route for message distribution than the other two proposed methods and existing UA-ID mechanism.

Variation of packet delivery ratio with respect to the number of packets sent in MANET is shown in Figure 8.

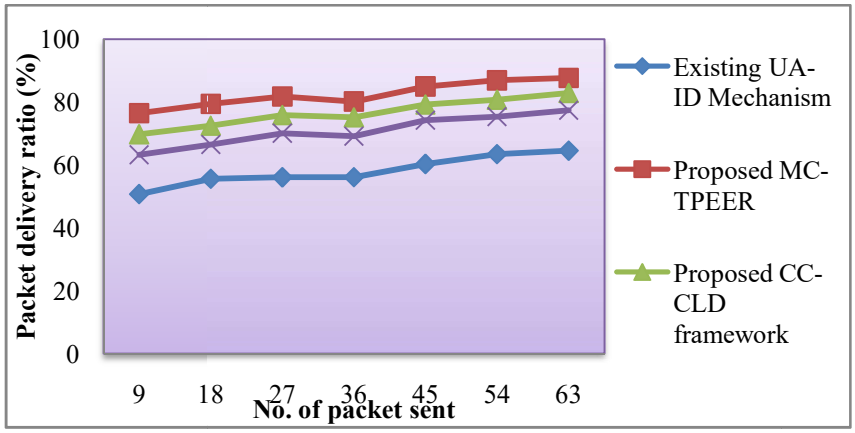

Fig. 8: Packet Delivery Ratio

Simulation result reveals that the proposed MC-TPEER framework significantly outperforms than the other proposed methods and existing UA-ID mechanism because of trust based route discovery for efficient packet transmission. Each member sends a RREQ message to other neighboring members. Therefore, the rescue information is shared between the certain group members and identifies the trusted route path with minimum energy conservation. The rescue group shares the information among each member with secured manner and it's forwarded to the operation center with the help of the base station. Therefore, the proposed MC-TPEER framework effectively identifies the trusted route for efficient packet transmission. This helps to increase the packet delivery ratio by 30% when compared to existing UA-ID mechanism. The CC-CLD framework and SRA-MDS model also increases the packet delivery ratio of 24% and 18% as compared to existing UA-ID mechanism.

VI.vii. Measurement of Secure Message Forwarding Rate

Table 7 shows that the experimental values of message forwarding rate between the rescuers with different number of messages sent on the network.

Table 7:Secure Message Forwarding Rate

No.of messagesent	Secure message forwarding rate in percentage			
	UA-ID	MC-TPEER	CC-CLD	SRA-MDS
5	43.58	49.24	55.32	61.45
10	46.29	52.36	58.35	64.23
15	55.22	61.54	68.24	72.35
20	58.75	64.24	70.25	74.83
25	56.13	62.34	69.37	74.19
30	60.23	66.78	73.51	77.23
35	62.77	68.24	75.17	79.45

At the several iterations, the message forwarding rate among the group members and information collector are secured. The trust based information sharing between the rescuers is improved by improving the members of a particular group or avoiding the outside group to send the request to an information collector. The proposed MC-TPEER, CC-CLD framework and SRA-MDS model is compared with existing UA-ID mechanism. The values reveal that the proposed SRA-MDS model improves the secure message forwarding rate.

Figure 9 depicts the secure message forwarding rate based on different numbers of messages being sent in the range of 5 to 35 with varying sizes.

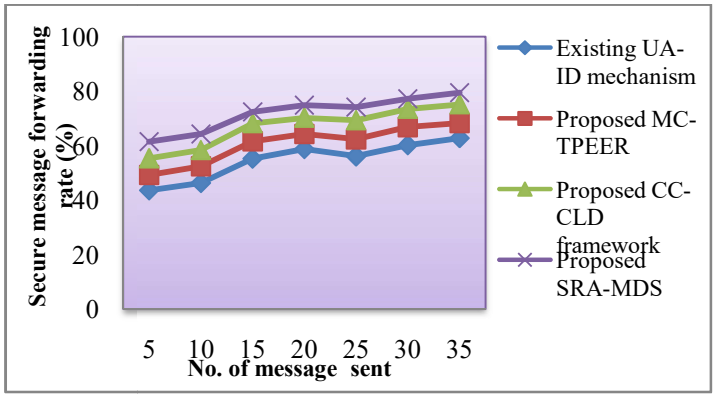

Fig. 9: Secure Message Forwarding Rate

The value of the secure message forwarding rate is increased in proposed SRA-MDS model when compared to other existing technique and other proposed methods MC-TPEER, CC-CLD. In addition, with increasing the number of messages, the secure message forwarding rate is increased. But comparatively, it is higher in SRA-MDS model because of applying authentication and verification algorithm. This algorithm is used to select the group members for secured message broadcasting. The algorithm also helps the authenticated member to obtain access and avoid the unauthorized member to attain the requested data. Therefore, the broadcasted messages are secured and increase the forwarding rate by 24% as compared to existing UA-ID mechanism. Moreover, the proposed MC-TPEER, CC-CLD framework increases the secure message forwarding rate by 10% and 19% compared to existing UA-ID mechanism.

VI.viii. Measurement of Forged Acknowledgement Attacks

A forged acknowledgement attack refers to the rate of unknown members through forged acknowledgement. It is measured in terms of percentage (%).

The comparison of forged acknowledgement attacks is presented in Table 8 with respect to the varying number of message sizes in the range of 64 – 2048 bytes.

Table 8:Forged Acknowledgement Attacks

Message size (bytes)	Forged acknowledgement attacks in percentage			
	UA-ID	MC-TPEER	CC-CLD	SRA-MDS
64	79.35	72.35	68.1	62.78
128	81.98	75.68	70.34	64.74

256	83.12	76.7	72.2	66.87
512	83.98	77.47	73.25	68.38
1024	84.87	78.98	74.2	70.12
2048	85.95	79.66	75.31	71.43

With an increase in the number and size of messages, the forged acknowledgement attacks are also increased. But, comparatively it is reduced using proposed SRA-MDS.

The targeting results of forged acknowledgement attacks with respect to various sizes of message are shown in Figure 10.

A forged acknowledgement attack is measured in terms of percentage (%). The forged acknowledgement attacks are reduced using proposed SRA-MDS model when compared to other existing techniques because of the application of authentication and verification algorithm. Information sharing is performed through the values of sender route authentication and probability measure. During this, the unauthorized member is correctly attained the requested data.

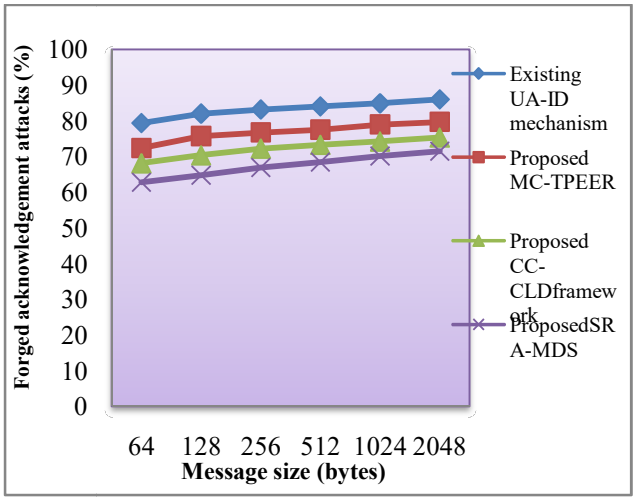

Fig. 10: Forged Acknowledgement Attacks

Therefore, a forged acknowledgement attack is significantly reduced by 23% as compared to existing UA-ID. Similarly, the other two proposed methods MC-TPEER; CC-CLD framework is also reducing the forged acknowledgement attacks of 8% and 15% as compared to existing User Authentication and Intrusion Detection (UA-ID) mechanism in MANET.

VII. Conclusion

A perfect illustration is discussed on analysis of proposed MC-TPEER, CC-CLD framework and SRA-MDS model. Theoretical analysis and experimental result show that the proposed MC-TPEER framework ensures the message broadcasting rate between the rescuer and trust level on broadcasting the message by consuming minimum energy. This MC-TPEER framework also minimizes the shortest path identification time for efficient trust based message broadcasting during the emergency rescue operation. In addition, the CC-CLD framework with Connected-path Link Dominating set, minimizes the ad hoc network routing overhead and reduce accurate path recovery time for efficient information sharing at the rescue emergency conditions. The removal of unauthorized member is to ensure data broadcasting between groups of rescuer and preserves the data integrity. Finally, SRA-MDS model provides better security for message distribution using the ECC scheme.

Moreover, authentication and verification algorithm effectively minimize the forged acknowledgement attacks when compared to the existing methods. This helps to ensure that only authenticated member, go to exact group and also it creates trust between information collector and member in certain group to enhance the secure information broadcasting.

References

I. AmolBhosle&YogadharPandey 2013, 'Applying Security to Data Using Symmetric Encryption in MANET', International Journal of Emerging Technology and Advanced Engineering, vol. 3, no. 1, pp. 426-430.

II. AshishBagwari, Pankaj Joshi, VikasRathi&Vikram Singh Soni 2011, 'Routing Protocol Behavior with Multiple Cluster Head Gateway in Mobile Ad hoc Network', International Journal of Ad hoc, Sensor & Ubiquitous Computing (IJASUC), vol. 2, no. 4, pp. 133-142.

III. Elhadi M Shakshuki Nan Jang &Tarek R Sheltami 2013, 'EAACK: A Secure Intrusion Detection System for MANETs', IEEE Transactions on Industrial Electronics, vol. 60, no. 3, pp. 1089-1098.

IV. Fan-Hsun Tseng, Li-Der Chou & Han-Chieh Chao, 2011, 'A survey of black hole attacks in wireless Mobile Ad hoc Networks', Humancentric Computing and Information Sciences, Springer, vol. 1, no. 4, pp. 1-16.

V. Floriano De Rango, Francesca Guerriero&Peppino Fazio, 2012, 'Link-Stability and Energy Aware Routing Protocol in Distributed Wireless Networks', IEEE Transactions on Parallel and Distributed Systems, vol. 23, no. 4, pp. 713-726.

VI. Ha Dang &Hongyi Wu, 2010, 'Clustering and Cluster-Based Routing Protocol for Delay-Tolerant Mobile Networks', IEEE Transactions on Wireless Communications, vol. 9, no. 6, pp. 1874-1881.

VII. HaiyingShen&Lianyu Zhao 2013, 'ALERT: An Anonymous Location-Based Efficient Routing Protocol in MANETs', IEEE Transactions on Mobile Computing, vol. 12, no. 6, pp. 1079-1093.

VIII. Iftikhar Ahmad, HumairaJabeen& Faisal Riaz, 2013, 'Improved Quality of Service Protocol for Real Time Traffic in MANET', International Journal of Computer Networks and Communications (IJCNC), vol. 5, no. 4, pp. 75-86.
JavadVazifehdan, Venkatesha Prasad, R &IgnasNiemegeers, 2014, 'Energy-Efficient Reliable Routing Considering Residual Energy in Wireless Ad Hoc Networks', IEEE Transactions on Mobile Computing, vol. 13, no. 2, pp. 434-447.

IX. Jinhua Zhu &Xin Wang 2011, 'Model and Protocol for Energy- Efficient Routing over Mobile Ad hoc Networks', IEEE Transactions on Mobile Computing, vol. 10, no. 11, pp. 1546-1557.

X. Kamal Kumar Chauhan&Amit Kumar Singh Sanger, 2012, 'Securing Mobile Ad hoc Networks: Key Management and Routing', International Journal on AdHoc Networking Systems, vol. 2, no. 2, pp. 65-75.

XI. Karunakaran, S &Thangaraj, P 2011, 'A cluster Based Service Discovery Protocol for Mobile Ad hoc Networks', American Journal of Scientific Research, no. 11, pp. 179-190.

XII. Keshav Kumar Tiwari& Sanjay Agrawal 2013, 'A Secure Reputation- Based Clustering Algorithm for Cluster based energy optimized Mobile Ad hoc Network', International Journal of Advanced Research in Computer Science and Software Engineering, vol. 3, no. 5, pp. 232- 236.

XIII. MadhukarRao, G, NadeemBaig, M, Fareed Baba, Md&Kanthi Kumar K, 2011, Energy Efficient Reliable Routing Protocol for Mobile Ad hoc Networks', IEEE International Conference on Electronics Computer Technology, pp. 296-299.

XIV. MenakaSivakumar 2018, "Secured Routing Deterrent to Internal Attacks for Mobile AD HOC Networks", Journal of Engineering Science and Technology Review 11 (1) 1 – 9.

XV. MenakaSivakumar 2018, "Secured Routing Deterrent to Internal Attacks for Mobile AD HOC Networks" Journal of Engineering Science and Technology Review 11 (1) 1 – 9.

XVI. Ming Li, Pan Li, Xiaoxia Huang, Yuguang Fang &SavoGlisic, 2015, 'Energy Consumption Optimization for Multihop Cognitive Cellular Networks', IEEE Transactions on Mobile Computing, vol. 14, no. 2, pp. 358-372.

XVII. Mohamed, MEA Mahmoud &Xuemin (Sherman) Shen 2013, 'A Secure Payment Scheme with Low Communication and Processing Overhead for Multihop Wireless Networks', IEEE Transactions on Parallel and Distributed Systems, vol. 24, no. 2, pp. 209-224.

XVIII. Pradip De, Yonghe Liu &Sajal K Das, 2010, 'Energy-Efficient Reprogramming of a Swarm of Mobile Sensors', IEEE Transactions on Mobile Computing, vol. 9, no. 5, pp. 703-718.

XIX. Seyed Amin Hosseini Seno, Tat Chee Wan &RahmatBudiarto 2011, 'Energy Efficient Cluster based Routing protocol for MANETs', International Conference on Computer Engineering and Applications, IPCSIT, vol. 2, pp. 380-384.

XX. Shengrong Bu, Richard Yu, F, Xiaoping Liu, P & Helen Tang 2011, '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.

XXI. Sourav Bhattacharya, HenrikBlunck, MikkelBaunKjærgaard&PetteriNurmi 2015, 'Robust and Energy-Efficient Trajectory Tracking for Mobile Devices', IEEE Transactions on Mobile Computing, vol. 14, no. 2, pp. 430-443.

XXII. SurendranSubbaraj&PrakashSavarimuthu 2014, 'Eigen Trust-based non-cooperative game model assisting ACO look-ahead secure routing against selfishness', EURASIP Journal on Wireless Communications and Networking, vol. 78, no. 1, pp. 1-120.

XXIII. Tao Shu& Marwan Krunz 2010, 'Coverage-Time Optimization for Clustered Wireless Sensor Networks: A Power-Balancing Approach', IEEE/ACM Transactions on Networking, vol. 18, no. 1, pp. 202-215.

XXIV. YuvarajKumbharey, SuweshShukla&SushilChaturvedi 2013, 'Renovated Cluster Based Routing Protocol for MANET', International Journal of Advanced Computer Research, vol. 3, no. 1, pp. 206-211.

XXV. Zhongyuan Qin, Xinshuai Zhang, KerongFeng, Qunfang Zhang &Jie Huang 2015, 'An efficient key management scheme based on ECC and AVL Tree for large scale Wireless Sensor Networks', Hindawi Publishing Corporation, International Journal of Distributed Sensor Networks, vol. 2015, pp. 1-7.

XXVI. Ziane Sara &MekkiRachida 2015, 'Energy-Efficient Inter-Domain Routing Protocol for MANETs', Elsevier, Procedia Computer Science, vol. 52, pp. 1059-1064.