# ENHANCED SECURE ROUTING WITH ENERGY EFFICIENT LINK ESTABLISHMENT AND DISTRIBUTED TIME SEQUENCE ROUTING (DTSR) IN MOBILE ADHOC NETWORKS

A.Ayubkhan
Assistant Lecturer
Omar Al-Mukthar University,Libya
A.R.Mohamed Shanavas Ph.D.,
Associate Professor
Jamal Mohamed College, Tiruchirappalli.
Dr. Khalid Idrissi
Lecturer
Omar Al-Mukthar University,Libya
A. Mohamed Ashar Ali
Assistant Professor
Jamal Mohamed College, Tiruchirappalli



**ABSTRACT:-** The ability of mobile adhoc networks in co-operative routing has more chance of getting variety of attacks. To overcome the problem of routing attacks , there are many approaches has been discussed and we propose a novel distributed time sequence routing (DTSR) approach with energy efficient link management for mobile adhoc networks. In this approach, the nodes uses the secret key generated by Diffie-Hellman approach and shares between them. We are also growing the DTSR routing with both network size and node density. The Diffie-Hellman Key Exchange is one of the more popular and attractive methods of key allocation. It is a public-key cryptographic system whose sole principle is for distributing keys, whereby it is used to switch a single piece of in sequence, and where the value obtained is general used as a session key for a private-key scheme It enables that adhoc nodes can correspond each other securely. The key allocation to adhoc nodes is done by means of two layer process. This paper proposes a key distribution scheme, based on intrusion detection method for using a data broadcast from source to destination on the network. It based high level security and more energy efficient data transmission on their network.

**Keywords:** Distributed Sequence Routing, Key Exchange, Network, Sink Node

## 1. INTRODUCTION:

The network is a capable tool with a wide range of potential applications such as setting monitor, attack detection, patient monitor systems, etc. Adhoc networks are also being deployed for many services applications, such as target track, surveillance, and protection organization. Network typically consist of small, reasonably priced, resource controlled devices that exchange a few words among each other using a multi hop wireless network. Each node, called an adhoc node, has one adhoc, well-established processors, limited memory, and low-power radio, and is usually battery operated. Each adhoc node is responsible for sensing a desired event locally and for relay a remote event sensed

by other adhoc nodes so that the event is report to the end user.

The main characteristics of an adhoc network include

- Power operation constrains for nodes using battery or energy harvesting
- capability to cope with node failures
- Mobility of nodes
- active network topology
- statement failures
- Heterogeneity of nodes
- Scalability to large scale of deployment
- Unattended operation
- Power expenditure.

They are mounted upon public buses circulate within urban environment on fixed trajectory and near-periodic schedule. Namely, sinks motion is not convenient and their routes do not adapt upon specific network deployments. Our only supposition is that adhoc s is deploying in urban areas in proximity to public transportation vehicle routes. As a fair compromise between a small numbers which results in their rapid energy depletion and a large number which results in reduced data throughput. Finally, sink node are grouped in separate clusters. Raw adhoc y data are filtered within individual clusters exploiting their inherent spatial-temporal redundancy. Finally, we assume the unit disk model, which is the most common assumption in adhoc network literature. The underlying assumption in this model is that nodes which are closer than a certain distance (transmission range R) can always communicate. However, in practice, a message sent by a node is received by the receiver with only certain probability even if the distance of the two nodes is smaller than the transmission range.

As a harmful and easy-to-implement type of attack, a malicious node simply replays all the friendly routing packets from a valid node to forge the latter node's identity; the mean node then uses this forged identity to contribute in the network routing, thus troublemaking the network traffic. Those routing packets, including their innovative headers, are replayed without any adjustment. Even if this malicious node cannot openly overhear the valid node's wireless transmission, it can collude with other malicious nodes to receive those routing packets and replay them wherever far away from the innovative valid node, which is known as a wormhole attack. Since a node in a network usually relies solely on the packets conventional to know about the sender's identity, replaying direction-finding packets allows the malicious node to forge

the identity of this valid node. After "stealing" that valid identity, this malicious node is able to misdirect the network traffic.

For instance, it may drop packets received, forward packets to another node not supposed to be in the direction-finding path, or even form a communication loop through which packets are passed among a few mean nodes considerably. It is often difficult to know whether a node forwards received packets correctly even with overhearing technique. Sinkhole attacks are another kind of attacks that can be launched after stealing a valid identity. In a sinkhole attack, a hateful node may claim itself to be a base station through replaying all the packets from a real base station. Such a fake base station could lure more than half the traffic, creating a "black hole". This same technique can be employed to conduct another strong form of attack - Sybil attack: through replaying the routing information of multiple legitimate nodes, an attacker may present multiple identities to the network. A valid node, if compromised, can also launch all these attacks.

The harm of such malicious attacks based on the technique of replaying routing information is further aggravated by the opening of mobility into adhoc networks and the hostile network situation. Though mobility is introduced into adhoc networks for well-organized data collection and various applications, it significantly increases the chance of communication between the honest nodes and the attackers. In addition, a poor network association causes much difficulty in characteristic between an attacker and an honest node with transitory failure. Without proper protection, adhoc networks with obtainable routing protocols can be totally overcome under certain conditions. In an emergent sensing application through Adhoc networks, saving the network from being overcome becomes crucial to the success of the application.

## 2. RELATED WORKS:-

To support quality of service constraints of Manet, there are many routing protocols have been discussed among them the popular Adhoc On demand Distance Vector (AODV) Routing has produced efficient results. But still there are many issues have been identified in literature which is not suitable for dense network conditions [2]. The Aodv routing protocol has the problem of network overhead which is introduced by route discovery and retransmission. Similarly there are few other approaches has been discussed in literature

and most of them suffers with the overhead of power and discovery.

To resolve the problem, we propose a novel energy efficient on demand quadratic midpoint routing using which the neighbor selection is performed at the route discovery. The source node sends hello message to collect the set of neighbors and their location information. The node divides its transmission range into four quarters in geographic region and for each quarter a single neighbor is selected to perform route discovery [3.5]. The node constructs quadratic midpoint route request and multicast to the representative for each geographic quarter.

The same will be repeated for each neighbors of neighbor and sends the route request packet to find the destination node. Whenever a node performs a node displacement it intimates the movement to all the neighbors through which set of packets being received which will be used for next transmission. The proposed approach produces efficient results and reduces the rate of retransmission which increases the throughput of the network [6]. It cause change in network topology, and therefore, it appreciably degrade the presentation of a routing protocol. Several direction-finding protocol studies are base on node lifetime and link lifetime. The major object here is to evaluate the node time and the link lifetime utilize the lively nature, such as the energy drain rate in addition to the relative mobility opinion rate of nodes. These two presentation metrics are included by Route lifetime-prediction algorithm.

As follow select the least lively route with the best lifetime for unrelenting data forward. Node Lifetime in addition to link lifetime forecast methods, the exponentially weighted moving average technique is used to approximation the energy use up rate. The handset can measure the symbol strength when it receives the packet from dispatcher in same power level and then it calculates the distance stuck between two nodes by apply the radio spread model. Once adhoc nodes have been deployed, there will be minimal physical intervention and monitoring. But, when nodes are deployed in a hostile situation and there is no manual monitor, it creates a security concern. Nodes may be subjected to various corporeal attacks [8]. The network must be able to alone detect, tolerate, and/or avoid these attacks. One imperative physical

attack is the opening of cloned nodes into the network. When service hardware and operating systems are used, it is easy for an adversary to capture genuine nodes, make clones by copying the cryptographic information, and deploying these clones back into the network [7].

Due to the incomplete exactitude of the timestamp change used, the algorithm uses time interval as a lower and upper bound for the exact value. Judgment of timestamps relies on special intermission arithmetic; hence there are cases when the temporal order of timestamps cannot be strong-minded [10]. One characteristic feature of this come within reach of is that the timestamp conversion has the next rightness property: the partial ordering of event timestamps in the local time of a give node reported by the algorithm is a subset of the total ordering of the times of the event in real time.

## 3. PROPOSED SYSTEM:-

Distributed Time Sequence Routing has used to send the data professionally and quickly on to their network. In this algorithm to find out the exact node locate route as well as straight path in the system base on the time. DTSR is to transfer the data in to without any alteration. Availability parameter means connectivity and functionality in the network organization layer. Connectivity is the physical connectivity of network elements. Loss is the part of packets lost in transportation from sender to target during a specific time interval, spoken in percentage. Have to improve the network throughput, system delivery ratio, and ease of use, data loss. As a result, the DH algorithm should be used with a form of authentication such as certificates to ensure that symmetric keys are recognized between nodes. The steering metrics are evaluated in disparate literatures to indicate the implication and measure purpose of recurrent routing protocols. In absolute surveys all along with the categorization of these metrics by means of their thorough classifications are discuss in detail.

**DTSR working principle:**

**Routing Phase for neighbor node address:**

**If** (source have Neighbor hop address) **then**

Route 1 = selected route

**Else**

Route 2 = selected route

**If** (route2 have key means) **then**

Route 2 = selected sink node

**Else**

Route 1 = selected route

.While HT=True

Receive Hello reply message.

Update neighbor table Nb.

Nb=$\int_{i=1}^{\sum HRep} \sum Nb +$

$\{Node.ID, Loc.x, Loc.y, S.E, D\}$

**If** (route 1 = route 2) **then**

Neighbor hop−count Energy consumption for a route in no of sink nodes

**If** Neighbor hop energy high **then**

Route 1 = selected route

**Else**

Route 2 = selected route

**End if**

**End if**

**End if**

**End if**

A network is a collection of nodes that are dynamically and arbitrarily located in such a manner that the interconnections between nodes are capable of changing on a continual basis. In order to facilitate communication within the network, a routing protocol is used to discover routes between nodes. In our network to using a movable nodes from one place to another, that time the attacker to hack the data on network. The Diffie-Hellman Key Exchange is one of the more popular and interesting methods of key distribution. It is a public-key cryptographic system whose sole purpose is for distributing keys. By the diffe Hellman key method the source's to use the separate keys for the each user in network, using these key the source node will transmit the data for destination.

**LINK ESTABLISHMENT ALGORITHM FOR ONE HOP AND MULTI HOP:**

For l < N (neighbor

**Initialization Phase**

Tr Transmission range of node i

**If** (source have neighbor transmission range) **then**

Direct communication with Sink Node

**Else**

Send data to common node in network

**If** (Critical Data) **then**

Send data to other route

**End if**

**End if**

**End for**

The key distribution to sensor nodes is done by means of two layer process. This paper proposes a key distribution scheme, based

on intrusion detection method for using a data transmission from source to destination on the network. It based high level security and more energy efficient data transmission on their network.

## 4. RESULT AND DISCUSSION:

To analyze performance of the DTSR by using path connected Networks. The replication surroundings produced in NS-2, in that provide keep up for a wireless Mobile Ad hoc networks. NS-2 was using C++ language and it has used for OTCL. It came as extension of Tool Command Language (TCL). The execution approved out using a cluster environment of 19 wireless mobile nodes rootless over a simulation area of 1200 meters x 1200 meters level gap in service for 10 seconds of simulation time.

Then also used into MAC layer models. The network based data processing or most expensive and data communication level on their performance on the network. The sources create multiple packets and its sending to the destination node; each data has a steady size of 512 bytes.

| **Parameters** | **Value** |
|---|---|
| version | Ns-allinone 2.28 |
| Protocols | DTSR |
| Area | 1200m x 1200m |
| Broadcast Area | 250 m |
| Transfer model | UDP,CBR |
| Data size | 512 bytes |

## 5. RATIO GRAPH:

The ratio of throughput, delivery, delay performance overall network presentation improve network routine and packet delivery ratio and cut packet delay. To improve the performance of Efficient, to reduce the network delay and end delay is calculated to avoid the traffic model system. Here we have using a shared buffer model for reduce the network delay and avoid the traffic on network, so we have a better result compare with existing method.

D = (Tr –Ts)

Tr - receive Time

Ts -sent Time

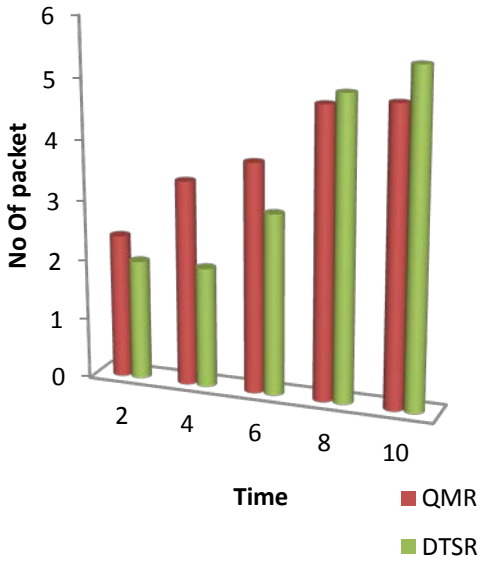


**Fig 3: Comparison of existing system and proposed system throughput**

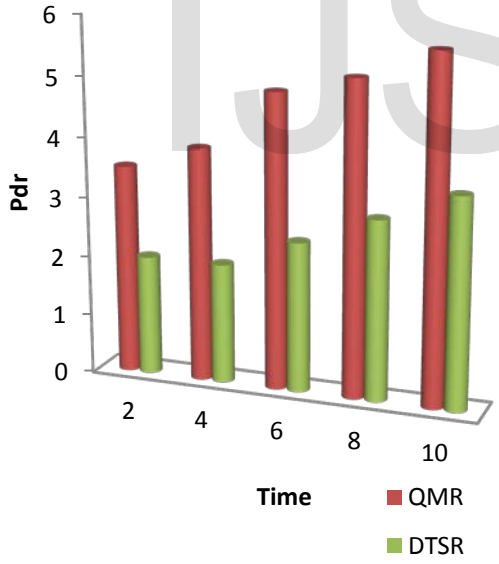


**Fig 4: Comparison of existing system and proposed system packet delay**

**The Data Delivery Fraction:-**

The packets delivered from starting place to purpose on their network. The active communication energy required transmitting or receiving packets through transmission control or load distribution and also the energy consumption can be minimized on the network.

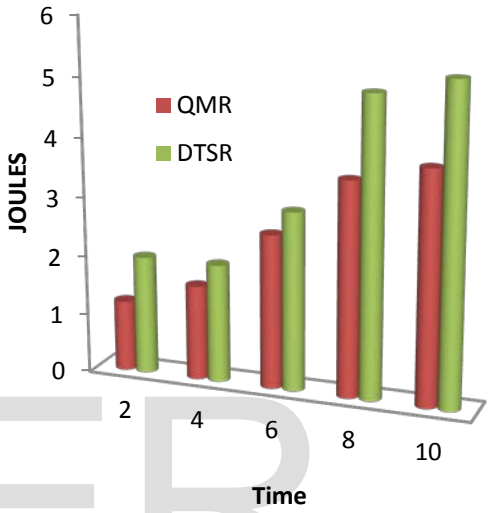


**Fig.5. Comparison of existing system and proposed system delivery ratio**

It's calculated by in-between the quantity of data recognized by conclusion state from side to side the measure package originated from starting point on set of connections.

PDF = (Pr/Ps)*100

Where Pr is total Data received & Ps is the total data sending on their network.

**5.1 Energy consumption:-**

The energy level on the network is most important one of the quick data transmission on their network. its calculated from their each node energy consumption is must of the network. if any node none to data transmit that node to save the energy on the network. the cluster head take more energy to send the data from source to destination on the network.

Energy consumption = no of packets * initial energy level

Remained energy = energy consumption – no of packets in node

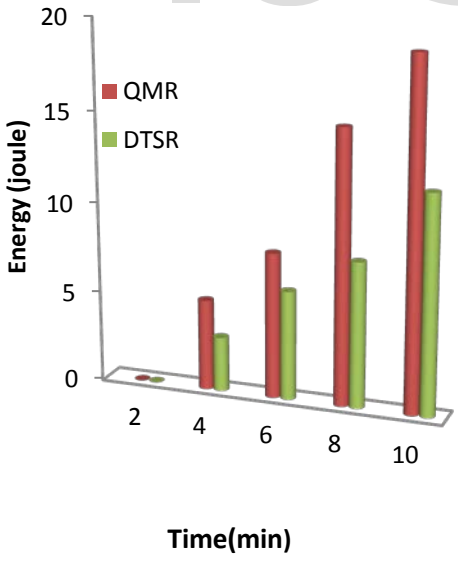


**Fig 6: Comparison of Energy consumption on network**

**5.2 Network Density:-**

In a network, the things that are connected are usually called "*nodes*". "Network density" describes the portion of the *potential* connections in a network that are *actual* connections. A "*potential connection*" is a connection that could potentially exist between two "nodes"

$$\text{Network Density} = \frac{\text{Actual connections}}{\text{Potential connection}}$$

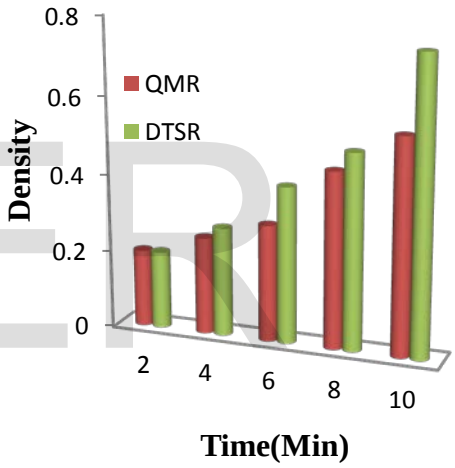


**Fig 7: Network density model on network**

## 6. CONCLUSION:

In our work we have using a neighbor discovery data collection to distributed time sequence for energy-efficient data gathering. It uses logical coordinates to infer distances, and establishes data reporting routes by greedily selecting the shortest path to the destination reference. In addition, mobile node is

capable of tracking multiple mobile sinks simultaneously through multiple logical coordinate spaces. Using the key that is an optimization to the location aided for location based data transmission on their network. It has mainly focused on this method to improve the network performance and energy consumption model on the network.

**REFERENCES:**

[1] Qiang Tang ,"Weaknesses in two group Diffie-Hellman key exchange protocols", 2nd July 2005.

[2] John Paul Walters, Zhengqiang Liang, "Wireless Sensor Network Security: A Survey", jan 2006.

[3] Aniket Kate, Greg Zaverucha, and Urs Hengartner, "Anonymity and Security in Delay Tolerant Networks", March 26, 2007.

[4] Mario Cagalj, Srdjan Capkun and Jean, "Key agreement in peer-to-peer wireless networks", jun-2008.

[5] Jean-Fran, Anton Stiglic, "Security Issues in the Diffie-Hellman Key Agreement Protocol", feb-2002.

[6] Sye Loong Keoh, Emil Lupu and Morris Sloman "Securing Body Sensor Networks: Sensor Association and Key Management", October 2005.

[7] Yongdae Kim, Adrian Perrig, "Tree-based Group Key Agreement",april 2009.

[8] Victor C. Zandy and Barton P. Miller, "Reliable Network Connections", September 23-2002.

[9] Wenliang Du* , Jing Deng†, Yunghsiang S ,"A Key Pre-distribution Scheme for Sensor Networks Using Deployment Knowledge", 7-sept-2004.

[10] Tony Chung and Utz Roedig, "DHB-KEY: An Efficient Key Distribution Scheme for Wireless Sensor Networks",march-2008.