IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified
Vol. 7, Issue 5, May 2018

The Enhanced KQuery To Search Neighbor Node in Manet

Gurjit Kaur[1*], **Deepinder Dhaliwal**[2]

Department of CSE, Desh Bhagat university Mandi Gobindgarh, Punjab India[1,2]

Abstract: K Nearest Neighbour (KNN) queries, which recover the k nearest sensor data items associated with a location (location-dependent sensor data) from the location of the query issuer, are useful for location based services in mobile environments. Here, we focus on the Ekquery processing in mobile ad hoc networks (MANETs). Key challenges in designing system protocols for the MANETs include low-overhead flexibility to network topology changes due to node mobility, and query processing that achieves high accuracy of the query result without a centralized server. In this paper, we propose the knodes which find optimal path in network for transmission.

Keywords: MANET, Ekquery, location-dependent sensor data, LBS,Chache Accuracy.

I. INTRODUCTION

Mobile Ad hoc networks or MANETs are the category of wireless networks which do not require any fixed infrastructure or base stations. They can be easily deployed in places where it is difficult to setup any wired infrastructure. As shown in Figure.1.3, there are no base stations and every node must co-operate in forwarding packets in the network.[2]

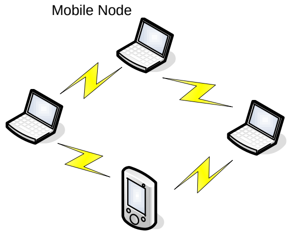


Fig. 1 Basic Structure of MANET

A.Clustering

Thus, each node acts as a router which makes routing complex when compared to Wireless LANs, where the central access point acts as the router between the nodes. A sensor network is a special category of ad hoc wireless networks which consists of several sensors deployed without any fixed infrastructure. The difference between sensor networks and ordinary ad hoc wireless is that the sensor nodes may not be necessarily mobile. Further, the number of nodes is much higher than in ordinary ad hoc networks. The nodes have more stringent power requirements since they operate in harsh environmental conditions. An example of a sensor network is a set of nodes monitoring the temperature of boilers in a thermal plant. Other application domains include military, homeland security and medical care.

Advantages of Mobile Ad hoc Networks

Having discussed the general issues in MANETs, the reason behind their popularity and their benefits will now be discussed.

(a) Low cost of deployment: As the name suggests, ad hoc networks can be deployed on the fly, thus requiring no expensive infrastructure such as copper wires, data cables, etc.

(b) Fast deployment: When compared to WLANs, ad hoc networks are very convenient and easy to deploy requiring less manual intervention since there are no cables involved.

(c) Dynamic Configuration: Ad hoc network configuration can change dynamically with time. For the many scenarios such as data sharing in classrooms, etc., this is a useful feature. When compared to configurability of LANs, it is very easy to change the network topology.

Applications of Mobile Ad hoc Networks

Ad hoc networks have several interesting applications ranging from battlefield to class rooms. In this section, some scenarios of deployment are discussed.

(a) Battlefield: In a battlefield, communication between soldiers and vehicles can be carried out using ad hoc networks. In such networks, the soldier troops might communicate with each other using hand-held devices. The vehicle mounted devices can be equipped with power sources for “recharging” these mobile devices.

DOI 10.17148/IJARCCE.2018.7524

(b) Rescue Operation: In scenarios such as firefighting or avalanche rescue operations, a quick deployment of nodes is required. Ad hoc networks can be used in such scenarios for communication between the workers.
(c) Event Coverage: Scenarios such as a press conference might entail reporters to share data amongst other reporters. In such cases, multimedia traffic might be exchanged between nodes such as laptops, PDAs, etc.
(d) Classroom: In a classroom, students and instructors can set up an ad hoc wireless network to share data using laptops.

General Issues in Mobile Ad hoc Networks
In a mobile ad hoc network, all the nodes co-operate amongst each other to forward the packets in the network and hence, each node is effectively a router. Thus one of the most important issues is routing. This thesis focuses mainly on routing issues in ad hoc networks. In this section, some of the other issues in ad hoc networks are described.
(a) Distributed network: A MANET can be considered as a distributed wireless network without any fixed infrastructure. By distributed, it is meant that there is no centralized server to maintain the state of the clients, similar to peer-to-peer (P2P) networks.
(b) Dynamic topology: The nodes are mobile and hence the network is self-organizing. Due to this, the topology of the network keeps changing with time. Hence the routing protocols designed for such networks must also be adaptive to the changes in the topology.
(c) Power awareness: Since the nodes in an ad hoc network typically run on batteries and deployed in hostile terrains, they have stringent power requirements. This implies that the underlying protocols must be designed to conserve battery life, or in other words, they must be power aware.
(d) Addressing scheme: The network topology keeps changing dynamically and hence the addressing scheme used is quite significant. A dynamic network topology entails a ubiquitous addressing scheme, which avoids any duplicate addresses. Mobile IP is currently being used in cellular networks where a base station handles all the node addressing. However, such a scheme doesn’t apply to ad hoc networks due to their decentralized nature.
(e) Network size: Commercial applications of ad hoc networks such as data sharing in conference halls, meetings, etc. are an attractive feature of ad hoc networks. However, the delay involved in the underlying protocols places a strict upper bound on the size of the network.
(f) Security: Security in an ad hoc network is of prime importance in scenarios of deployment such as battlefield. The three goals of security - confidentiality, integrity and authenticity are very difficult to achieve since every node in the network participates equally in the network

II. PREVIOUS WORK

M.Sc.Ali Abdulrahman et al [2015] [1] An ad hoc network is the cooperative engagement of a collection of mobile nodes without the required intervention of any centralized access point or existing infrastructure. Designing a foolproof security protocol for ad hoc network is a challenging task due to its unique characteristics such as, lack of central authority, frequent topology changes, rapid node mobility, shared radio channel and limited availability of resources. There are a lot of routing protocol for Ad-hoc network such as OLSR, AODV and ZRP; AODV(Ad Hoc On-Demand Distance Vector)is one of such protocols that helps to create and maintain routes in spite of the dynamic network topology. This protocol is vulnerable to a number of security threats that come from internal malicious nodes which have authorization credentials to participate in the network. Malicious nodes deliberately drop data packets and disrupt the correct operation of the routing protocol. .

Saahirabanu Ahamed et al[2015][2] Mobile Ad hoc network is a wireless network without having any fixed infrastructure. It consists of mobile nodes which are free in moving in or out in the network. MANET is make sure mutual confirmation of participants nodes, confidentiality and integrity of exchanged data, availability of the network resources, access control to the communication medium and the anonymity. MANET attacks generally include attempting to drop packets, gaining substantiation or procuring authorization by inserting forged packets into data stream. This paper is presenting energy efficient modified AODV routing protocol using Clustering method in Manet. The protocol deals with various parameters as PDR, energy consumption, average end to end delay, & throughput. This protocol will be detect the K series& improve the energy level of Manet..

Mr. Ramanpreet Singh,et al [2015] [3]has proposed Wireless sensor network comprises of a set of sensor nodes that communicate among each other using wireless links and work in an open and distributed manner because of less number of resources on the nodes. The sensor nodes sense information about an event from the ambiance and then the information is forwarded to a sink node for further processing and analyzing. The sensed information can be forwarded in many ways, earlier uni cast routing was there to a single sink node, but due to the wide variety of WSN applications the presence of multiple sinks is realized which necessitates multicast routing for efficient data dissemination to multiple destinations. For any disaster surveillance or fire handling emergency scenarios various multicast routing

DOI 10.17148/IJARCCE.2018.7524

protocols have been proposed by many researchers. This paper focuses on providing a survey of the existing multicast routing protocols by presenting approach, their advantages and disadvantages. Further a comparative study of various multicast protocols is done on the basis of different parameters to identify different issues and challenges that need to be resolved for each one of them.

B.Kondaiah et al [2015] [4] mobile ad-hoc network (MANET) is a collection of wireless mobile nodes that dynamically self-organize to form an arbitrary and temporary network. The mobile nodes can communicate with each other without any fixed infrastructure. MANET can be set up quickly to facilitate communication in a aggressive environment such as battlefield or emergency situation. The various severe security threats are increasing on the MANET. One of these security threats is K serieswhich drops all received data packets intended for forwarding. In this paper, we are simulating and analyzing the impact of K serieson Ad Hoc O-Demand Distance Vector (AODV) protocol. The simulation is carried on NS-2 and the simulation results are analyzed on various network performance metrics such as packet delivery ratio, normalized routing overhead and average end-to-end delay..

Dilraj singh et al.[2015].[5] Due to its self-organizing nature the Mobile Ad hoc Networks (MANETs) are successfully able to provide a great channel for communication anywhere, anytime in absence of any centralized infrastructure and have a huge potential in actual applications like, in the military, rescue and commercial fields. However, due to its dynamic nature the network they are susceptible to different type of attacks which can hinder smooth functioning of the network. The standard routing protocols for MANETs do not perform well in the presence of nodes that intentionally drop data packets, one such malevolent behavior is launched by black hole nodes. In this paper, we propose a new protocol Enhanced Secure Trusted AODV (ESTA) to cope with the problem of presence of such nodes in network. ESTA is extension of on the broadly used reactive protocol Ad hoc On-demand Distance Vector (AODV). The proposed protocol is multiple path approach combined with the use of trust to eliminate the corrupt paths. The NS-3 based simulation results present that the proposed protocol is efficiently able to thwart the effect of the K seriesin different scenarios and proves to increase the ratio of successfully delivered data packets significantly.

Ravinder Kaur et al [2010 [6] mobile ad hoc network (MANET) is infrastructures less dynamic network consist of a collection of wireless mobile nodes that communicate with each other without the use of any centralized network. Security in MANET is the most important concern for the basic functionality of network. The dynamic topology of MANETs allows nodes to join and leave network at any point. Security of AODV protocol is compromised .By a particular type of attack called black hole attack. A malicious node advertises itself as having the shortest path to the node whose packets it want to intercept. In this paper we are trying to find the secure path for transmission through Digital Signature. Digital Signature is the verification technique.

III.PROPOSED WORK

In our Proposed algorithms the knodes are cached in the network for finding efficient transmission range and these knodes update network routing table periodic table with optimal path for reliable transmission in MANET .

Algorithm
Step 1: Initiate MANET scenario using NS2

Step 2**:** Start with N number of nodes initial elements like no of nodes, neighbor node, kquery.

Step 3: Initialize with N no. of nodes.

Step 4: Implement ENHANCED KQUERY algorithm technique.

Step 5: initially ENHANCED KQUERY algorithm for finding efficient node for transmission

Step 6: In ENHANCED KQUERY algorithm find the distance between nodes

Step7: if node with transmission range distance is find than data is transferred for transmission

Step8: knodes in the network are cached for finding best transmission range in routing table and update routing table periodically

Step9: The enhanced kquery node provide efficient transmission path in network.

IV. RESULT ANALYSIS

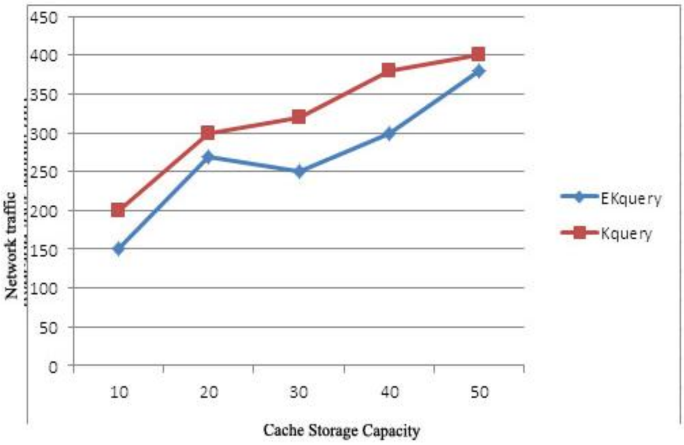


Fig 2 Network Traffic

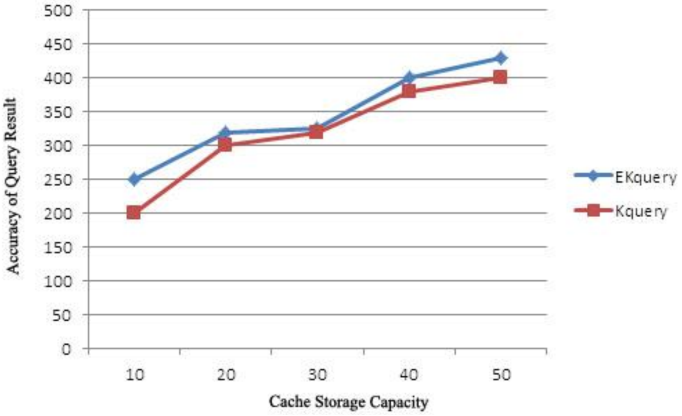
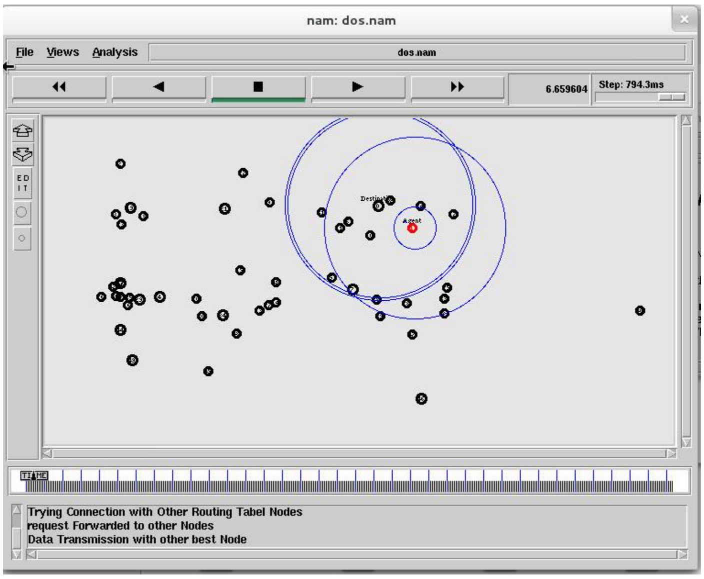


Fig 3 Accuracy of query result

From Fig. 2 and 3, we can see that the network traffic of our Ekseries is average 10% less than that of Kseries when chache is increased Ekseries network Traffic is low and accuracy query result are higher as compared to kseries Technique.

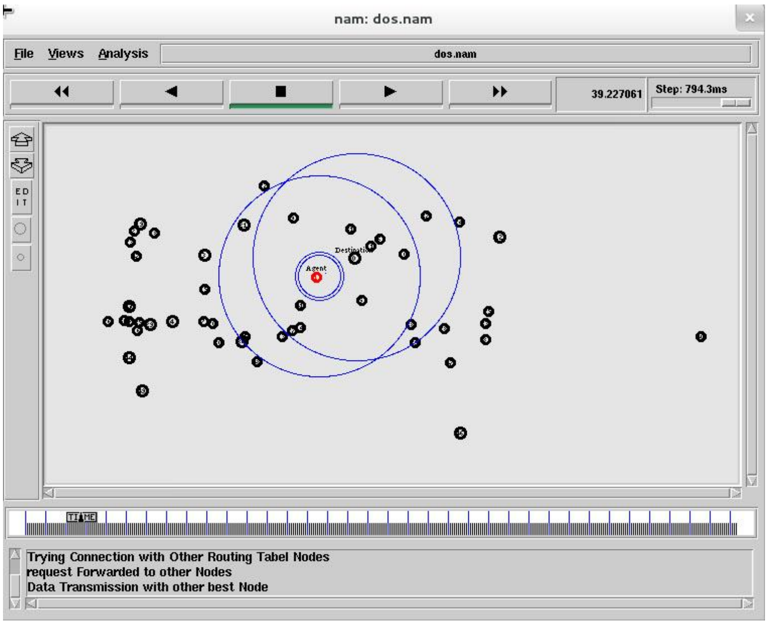
V. SIMULATION SCENARIO



Trying Connection with Other Routing Tabel Nodes
request Forwarded to other Nodes
Data Transmission with other best Node

Fig4. Topology Generated

DOI 10.17148/IJARCCE.2018.7524



Trying Connection with Other Routing Tabel Nodes
request Forwarded to other Nodes
Data Transmission with other best Node

Fig5. Knodes formed for Transmission

Fig4. Cluster Head formed by SLA Technique. The Fig 4,5, shows the automatic ksores nodes finding optimal path in network using ekseries technique and provide better result as compare to kseries technique.

VI. CONCLUSION

In this paper, we explore recent various we proposed knodes Based on the comparison and analysis, we propose a Ekquery base data Transmission with MANET First, we introduce a Knodes for finding optimal path and after finding optimal path it update network with new transmission range which produce better result as compare to kquery

REFERENCES

[1] M.Sc.Ali Abdulrahman Mahmood , Dr. Taha Mohammed Hasan, M.Sc.Dhiyab Salman Ibrahim,, “Modified AODV Routing Protocol to Detect the Black Hole Attack in MANET” (IJARCSSE), Volume 5, Issue 7,July 2015

[2] Swati Pokhariyal , Pradeep Kumar,, “ Shielding algorithm for Detection and Elimination of Black hole/Gray hole Attack in MANETs” (IJMCSA) Volume No.3, Issue No.1, January, 2015

[3] Mr. Ramanpreet Singh, Mr. Ajay Kumar Dogra,, “Performance evaluation of energy efficient modified AODV using clustering method in MANETs” (IJMCSA) Volume No.3, Issue No.1 (IJCSMC), Vol.4, Issue. 5, May 2015

[4] B.Kondaiah, Dr.M. Nagendra,, “A Black Hole Attack on Performance of AODV Routing Protocol in Manets” (IJARCSSE), Vol.5,Issue11 , Nov 2015

[5] Dilraj singh, Dr. Amardeep singh,, “Multipath trust based framework for prevention of black hole attack in Manets” (JATIT & LLS), Vol.80. No.3, October 2015

[6] Ravinder Kaur, Jyoti Kalra,, “Detection and Prevention of Black Hole Attack with Digital Signature” (IJARCSSE), Volume 4, Issue 8,August 2014

DOI 10.17148/IJARCCE.2018.7524