International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395-0056
Volume: 06 Issue: 04 | Apr 2019 www.irjet.net p-ISSN: 2395-0072

A Study of AODV protocol For Quick Disaster Recovery

Krishna AV[1], Prof Manoj Kumar G[2]

[1]Research Scholar, Dept of computer science, LBSITW, Poojapura, Kerala, India
[2]Associate Professor,Dept of computer science,LBSITW,Poojapura,Kerala,India

---

Abstract - *DANETs when compared to MANETs have high network density and mobility over time. To maintain a secure communication over DANET, requires the knowledge of mobility and complex key management scheme based on the topology change. When the DANETs are deployed over a disaster area, the establishment of communication services will be challenging task. In a disaster area we cannot predict the path or traffic on a particular period of time due to its nature. The survey is based on modified adhoc networks which have random and quickly changing topology is used for routing purposes. And the proposed system can be deployed with minimal changes on a existing environment. The network path, prediction is done by making use of hierarchical hidden markov model. The data in network aggregated using homomorphic encryption scheme which help us the users to access the validation functions. This reduce the amount of packet transfer ratio with indirectly increases throughput, packet delivery ratio etc. And prediction methodology, it helps to eliminate the malicious activities in a group due to link failure.*

Key Words : ***DANET, homomorphic encryption, malicious node, hidden markov, AODV ,El-gamal Encyrption***

1.INTRODUCTION

Our Earth has suffered a great deal from reoccurring natural disasters that have repeatedly put a strain on peoples lives. A natural disaster is a sudden event, an accident or a natural havoc, that causes great extents of damage or multiple deaths. Over these past years a numerous amount of these disasters has been seen happening all around the world. Tragedies of towns getting torn apart were reported as well as the occurrence of many deaths, disabilities and shelter damage.

Vanets exchange various messages which includes information about hazards, events, traffic details or location of nearby hotels, restaurants etc. This exchanging of information may also contain the driving situations of traffic, weather conditions, road conditions etc. This information exchanges are limited to disaster areas .Our work concentrates on exchanging of information between vehicles(V2V) which is comprised of pre defined headers such as RREQ and RREP .An encrypted information regarding the source is attached with the route request (RREQ) by using El-gamal. Due to the homomorphic nature of this encryption method all the path requests route will be encoded and finally the destination would have the entire path in an encrypted form. A comparison can be done within the header itself for a mismatch that would help to identify the intruders within a path .If packet loss or delays occur then the same can be identified from the header itself thus we can achieve integrity in routing.

2.LITERATURE SURVEY

2.1 AODV Routing Protocol

AODV is a reactive routing protocol for adhoc mobile networks, it provides route between nodes only when the routes are requested by the source node and the network is flexible to allow and leaves based on its demand[1]. During the route construction phase, to establish route by flooding Route Request RREQ packets in the network. This RREQ message forwarding continues until the destination or neighboring nodes find the route to destination. The destination nodes send the Route Reply RREP, it travels the reverse route when the source node receives the RREP packets it checks the destination sequence number which should be greater than destination sequence number of RREQ packets. If RREQ is received multiple times, that are discarded.If a data is flowing and a link breaks is detected a route error message (RERR) is send to the source of the data in a hop by hop fashion. As the RERR propagates towards the source each intermediate node invalidates routes to any unreachable destinations. When the source of the data receives RERR it invalidates the route and re initiative route discovery if necessary.

2.2 Variant AODV Routing Protocol

The protocol and method that were used earlier focused on areas such as modification of AODV and path prediction method. Advance adhoc on demand distance protocol[2]a variant of traditional AODV helps to maintain secure communication between the nodes without any attack from intruders, ie to identify the black hole attacker in the

network. The methodologies used here are divide and conquer method to finding out failure node and intruder node in the network and probability to predict whether the node is intruder or black hole attacker during the transmission. Based on security, the traditional AODV uses public key cryptography of RSA[3].Here security can be provided on both route discovery and route maintenance and uses i)Digital Signature that provides integrity in the routing message(ie non mutable field) ii)Hash Chain ensures the mutable field from miss interruption. AOMDV (Adhoc On Demand Multiple Distance Vector protocol)keeps an alternate route from multiple route reply[4],but it cannot be consider the mobility of network, because of this drawback an enhanced power aware Qos multi path be used, it helps to search a feasible path that satisfy the bandwidth and energy constraints, and search only a shortest path that helps to limit the routing overhead. T2AR(Trust aware adhoc routing protocol) [5] ensures trust awareness between nodes in the dynamic varying topology, proposed routing collects the neighbourlog reports to predict the success or failure rate of packet transfer between the node. The trust value of node in calculated based on energy model calculation, packet sequence ID matching rate and mobility estimation. Vanet is the category of manet ,it is used for communication between nodes in a dynamically varying environment. The route discovery, path maintenance done by AODV routing protocol. Here routing can be modified by applying artificial intelligence (aiAODV)[6] using fuzzy neural network algorithm. The data is flooded through different path by sending RREQ and considering attributes such as distance, overhead, power consumption and expected time for better throughput, packet drop and avoid collision effectively. Modification of aodv protocol on rreq header and rrep header can be explained in ISDSR+[7], it is a centralized approach can generate secret key with the help of key generation center. In this the node which want to communicate send a KREQ message to Key Generation Centre(KGC) to generate a secret key code and returns the key to node by KREP. In the route discovery process ,the node receives SRREQ add its own identity in the received route information and generates a signature using a signature algorithm an node broadcast SRREQ including the signature this steps iterated until it reaches the destination, when this r eached the destination the node verify the received signature via signature algorithm .And in route maintenance of ISDSR+ if any node find disconnection the intermediate node ID and source generate as signature and forward SRERR, then the source node.

2.3 Network Management And Path Prediction

In Vehicular adhoc network path prediction[8] can based on by Trajectory Predictability for Vehicles, feasibility and availability .And also based on a routing frame work which includes vehicles current location through GPS such that communication between neighbours through beacon messages and uses a path selection algorithm and queue management algorithm. In dynamic varying environment, the location of vehicles changes rapidly[9] so that the destination of vehicles can be predicted based on source, present location and moving direction etc. And the paper proposes a vehicular mobility pattern(VMP) by employing the variable order markov (VOM)model. Vehicle clustering is an important task in network management to address the broadcast problem with changing environment[10].Here the paper proposes a pair of algorithms such as sociological pattern clustering(SPC) and route stability clustering (RSC).In SPC it create cluster using nodes and choose the cluster head based on nodes with highest energy level and in RSC it focus on vehicles or nodes communication that means exchange of beacon message between neighbours about the nodes identifier ,location, speed, stability of routes and time stamp etc. The paper also explain how to maintain cluster and overhead due to clustering.

3. PROPOSED SYSTEM

The paper proposes a novel method to recover the data and effectively operate within a limited period of time without any disruption. Modified adhoc networks which have random and quickly changing topology is used here for routing purposes .In a disaster area we cannot predict the path or traffic on a particular period of time due to its nature. Ensuring security and quality of service is the advantage of the proposed method which can used to scale on regular applications also. The proposed system can be deployed with minimal changes on an existing environment. The network path prediction id done by making use of hierarchical encryption schemes which helps the users to access the validation functions. This reduces the amount of packets transfer ratio which indirectly increases the throughput, packet delivery ratio etc.

3.1 Modification Of AODV Routing Protocol

In this protocol functions similar to AODV with the following changes. An identifier attribute is added to the RREQ and RREP request . The identifier is composed of the encrypted form of source node id, destination id ,location, direction velocity. When a RREQ is received by an intermediate node, the route to a source is created .If the receiving node as not received the RREQ before, is not the destination and does not have a current route to the destination , it rebroadcast the RREQ. If the receiving nodeis the destination or has a current route to the destination it generate a RREP. If a data is flowing and a link breaks is detected a route error message (RERR) is send to the sourceof the data in a hop by hop fashion. As the RERR propagates towards the source each intermediate node invalidates routes to any unreachable destinations. when the source of the data receives RERR it

invalidates the route and re initiative route discovery if necessary.

3.2 El_gamal Encryption

The Encryption of header in both source and destination node performed by ElGamal encryption scheme[11]. In cryptography, the ElGamal encryption system is an asymmetric key encryption algorithm for public-key cryptography which is based on the Diffie Hellman key exchange. The system provides an additional layer of security by asymmetrically encrypting keys previously used for symmetric message encryption. This encryption can be defined over any cyclic group . Its security depends upon the difficulty of a certain problem in related to computing discrete logarithms.

3.3 Hidden Markov Model

The movement of nodes within the cluster or cluster to cluster can be predicted by using hidden markov model[12].The Hidden Markov Model (HMM) is a relatively simple way to model sequential data. A hidden Markov model implies that the Markov Model underlying the data is hidden or unknown. The conditional probability P(qijxi) can be rewritten according to Baye's rule:

$$P(q1\ldots qn|x1..xn)= \frac{P(x1\ldots xn|q1\ldots qn)p(q1\ldots.qn)}{P(x1\ldots xn)}$$

The probability P(q1…qn|x1..xn) can be estimated as $_{i=1\,\pi}{}^{n}$ as P(xijqi) if we assume that, for all i, the qi, xi are independent of all xj and qj ,for all j ≠ i.
We get a measure for the probability, which is proportional to the probability, and which we will refer as the likelihood L. P(q1…qn|x1..xn)∞ L(q1…qn|x1..xn)= P(q1…qn|x1..xn).P(q1..qn).With our (first order)Markov assumption it turns to: P(q1…qn|x1..xn)∞ L(q1…qn|x1..xn) $_{i=1\,\pi}{}^{n}$ P(xijqi). $_{i=1\,\pi}{}^{n}$ P(qi|q_i-1).

3.4 Homomorphic Encryption

The proposed method is used to recover the data and effectively operate within a limited period of time. Time period is a critical factor in a disaster area since the energy level of different nodes varying with respect to time .The message transmitted by the nodes during a time period cannot be re transmitted due to the energy failure or due to different energy level of the nodes this makes the re transmission of data nearly an impossible factor .Our method predicts the recovery of data in different communication channel over a period of a time which reduce the re transmission by making use of homomorphic encryption method. Homomorphic encryption[13] is the conversion of data into cipher text that can be analyzed and worked with as if it were still in its original form. It allow complex mathematical operations to be performed on encrypted data without compromising the encryption. In mathematics, homomorphic describes the transformation of one data set into another while preserving relationships between elements in both sets.

4. CONCLUSIONS

The survey is focused mainly on variant of aodv, which helps to maintain communication in disaster affected area. One of the major Challenges for telecommunication network operators to immediately restore communication services in the disaster area. Establishment of communication services during disaster period is a tedious task route prediction , optimized route calculation etc can be done only if the communication equipment functions with out any disruption. There are lot of variant of aodv protocol that functionality can be changed based on security, energy efficiency, quality of services etc. The proposed system mainly focused on an ad-hoc network (multi-hop wireless network)where all nodes cooperatively maintain network connectivity a centralized infrastructure. encrypted by El-gamal method and network prediction can be done by homomorphic encryption. And vehicles or nodes movement can be predicted by hidden markov model. The modified adhoc network with securities which are enabled using these methods shows a remarkable improvement in energy consumption, packet delivery ratio, throughput etc.

REFERENCES

[1] "AODV ROUTING PROTOCOL WORKING PROCESS" Asma Ahmed, A. Hanan, ,Journal of Convergence Information Technology(JCIT) Volume 10, Number 2, March 2015.

[2] "Energy Optimization in DirectionalAdvanced Intruder Handling AODV Protocol in MANET " S.Hemalatha1, P.C.Senthil Mahesh 2018 SWANSEA PRINTING TECHNOLOGY LTD TAGA JOURNALVOL. 14 ISSN: 1748-0345 (Online).

[3] "Hybrid Security Using Digital Signature RSA Encryption for AODVin MANET",Shelbala Solanki, Anand Gadwal, International Journal of Computer Science and InformationTechnologies, Vol. 6 (3) , 2015,2630-2635.

[4] "POWER AWARE QOS MULTIPATH ROUTING PROTOCOLFOR DISASTER RECOVERY NETWORKS",S.Santhi, DSadasivamr.G.Sudha, International Journal of Wireless Mobile Networks(IJWMN) Vol. 3, No. 6, December 2011.

[5] "T2AR: trustaware adhoc routing protocol for MANET",Gayathri Dhananjayan andJanakiraman Subbiah,SpringerPlus (2016) 5:995.

[6] "Neural Network Based Modified AODV Routing Protocol in VANET", Soumen Saha, Utpal Roy and Devadutta Sinha,European Journal of Advances in Engineering and Technology, 2015, 2(10): 17-25

[7] "ISDSR+:Improving the Security and Availability of Secure Routing Protocol",preparation of papers for IEEE Transcations and journal volume 4,2016.

[8] "Driving Path Predication Based Routing Protocol in Vehicular Adhoc Networks",Yong Feng, Feng Wang, Jingjing Liao, and Qian Qian,Hindawi Publishing Corporation International Journal of Distributed Sensor Networks Volume 2013, Article ID 837381, 10 pages.

[9] "A novel vehicular location prediction based on mobility patterns forrouting in urban VANET",Guangtao Xue, Yuan Luo, Jiadi Yu and Minglu Li,Journal onWireless Communications and Networking 2012,2012:222http://jwcn.eurasipjournals.com/content/2012/1/222.

[10] "Social Clustering of Vehicles based on Semi markov process",EEETransactions on Vehicular Technology (Volume: 65 , Issue: 1 , Jan.2016).

[11] "An Encryption and Decryption More Secure Elgamal Cryptosystem",
Mr. Jaydip Thakkar,IJSTE - International Journal of ScienceTechnology Engineering — Volume 1 — Issue 12 — June 2015ISSN (online): 2349-784X.

[12] "Hidden Markov Models",http://www.igi.tugraz.at/lehre/CI.

[13] "Homomorphic Encryption",Monique Ogburna, Claude Turnerb,Pushkar Dahalc,Published by Elsevier B.V.Selection and peer-review under responsibility of Missouri University of Science and Technology Open access under CC BY-NC-ND license.

[14] "Wired and Wireless Network Cooperation for Wide-AreaQuick",Digital Object Identifier 10.1109/ACCESS.2017.2783050Disaster Recovery.

[15] "Mobility Aware Energy Efficient Clustering for MANET:ABio-Inspired Approach with Particle Swarm Optimization",Hindawi Wireless Communications and Mobile Computing Volume 2017, Article
ID 1903190, 12 pages
https://doi.org/10.1155/2017/1903190