Secure On-Demand Routing Protocol for MANET using Genetic Algorithm

D.Suresh kumar
School of Computing Science & Engineering
VIT University
Vellore-632014, Tamilnadu, India

K.Manikandan
School of Computing Science & Engineering
VIT University
Vellore-632014, Tamilnadu, India

M.A.Saleem Durai
School of Computing Science & Engineering
VIT University
Vellore-632014, Tamilnadu, India

ABSTRACT

Mobile ad-hoc network networks are self organizing, very dynamic network which support data networking without an infrastructure. The proposed protocol provides secure and adaptive backup routing protocol for MANET. Genetic algorithm (GA) is used to find the optimal path from the available multiple paths between source and destination to be used in the case of link failure problems. To improve routing mechanism, we use buffer size, end to end delay and shortest path as the parameters for GA in route discovery. GA allows for self-configuration systems and maintains state information about the neighboring network. GA's are able to find, if not the shortest, at least an optimal path between source and destination in mobile ad-hoc network nodes. And we obtain the alternative path or backup path to avoid reroute discovery in the case of link failure or node failure. Furthermore we incorporate self organized key authentication mechanism in order to authenticate every that participates in the network. We use NS-2 simulator to simulate this protocol and we conclude with performance evaluation and comparison with the existing protocol.

Keywords

MANET, Genetic algorithm, backup routes, authentication.

1. INTRODUCTION

Mobile ad hoc network (MANET) is a dynamic topology caused by node mobility leads to poor route stability and thus makes the routing mechanism more complicated. And it is a flexible, self organizing wireless network containing wireless mobile nodes which has no centralized control or any specific infrastructure. Every node that participates in the network acts as both systems and routers. Each move of the host affects the topology of the network and the route of transmission. When the distance between two hosts is more or low quality communication or disconnection may occur. Sometimes link failure is unavoidable when there is a change in network topology or it may affect the quality of sending packets between the nodes.

There are many existing routing protocols available for MANET and those can be categorized as table driven approach (proactive) and on demand routing protocols (reactive) [7]. The reactive routing protocol a route is established only when a source node wants a route to destination node. Here the protocol supports the frequent route discovery mechanism to establish a route and to update that route periodically.

1.1.Related works

The AODV protocol discovers a route when a node wants to establish a route between the source and destination node. It consists of three phase route request phase (RREQ), route reply phase (RREP) and route error phase (RERR). But the performance is been affected when a link or a node fails then the route discovery phase is been reinitiated. The route discovery phase maybe initiated plenty of times since it is a MANET where the nodes move more frequently. The network has many limitations like power consumption, low bandwidth and communication limits, etc. So it is important that the lifecycle of a route and the stability of a route is most important factor in a routing process in MANET.

2. PROPOSED PROTOCOL

To improve the routes stability and to improve the trust on participating nodes, this paper present a secure backup on demand routing protocol for mobile ad hoc network. SBMR discovers multiple routes from source to destination in order to store a backup route to the destination node to be used in case of link or node failure which avoids the reroute discovery phase. The nodes are been authenticated well in order to know that the participating nodes are not intruders to break the link. And to find the optimal paths from the available multiple paths we use genetic algorithm in our protocol. Initially by using the concepts of AODV multipath routing protocol we find multiple paths available from source to destination node and this is described in following section. The architecture of our protocol is shown below in the Fig.1.

2.1.Route discovery

In this phase when a route is required from the source to destination node the source Node broadcasts a RREQ message to its neighbor nodes requesting a route to the destination node. If there is an existing route between the source and destination node in the routing table of neighbor nodes the discovery phase is not needed and the existing path is been used.

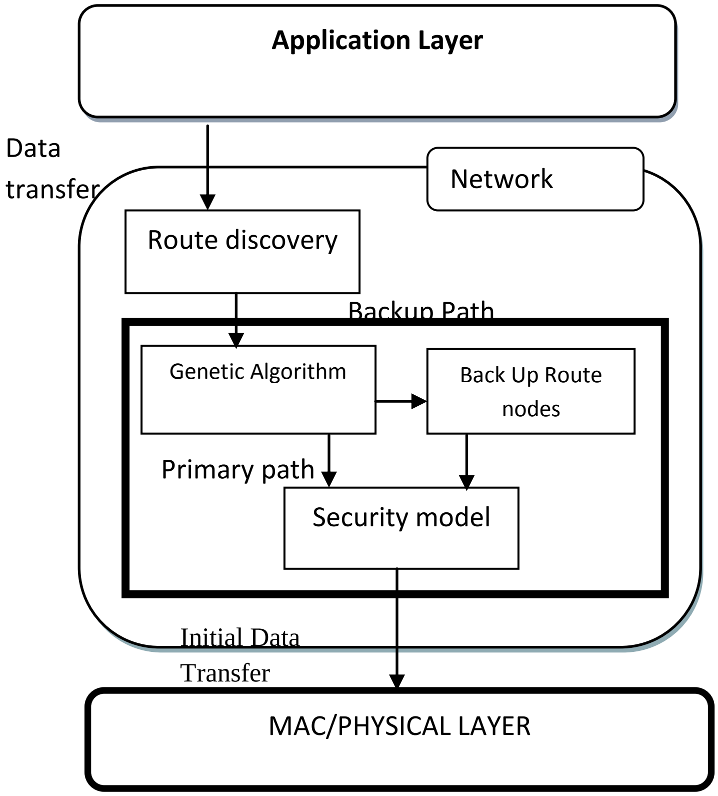

Fig 1: Architecture of secure on demand routing protocol for MANET using GA.

In case if there is no route to the destination node then the New_Route_Discovery [5] process is been executed.

2.1.1. New_route_Discovery process

Source node S broadcasts RREQ (Route Request) to nearby nodes. RREQ includes a sequence number field to distinguish the route request packet from the other packets along with the address contents that it travels from source S to the destination node D. When the intermediate nodes receives the RREQ packet it inserts its own address into the address content field and then transmits the modified packet to its neighboring node. The RREQ cache of the intermediate nodes also records the information that includes the sequence number of the packet and to which nearby node that is been forwarded. If a node receives the RREQ with the same sequence number from its neighbor node then it checks whether the route content of RREQ includes its address if so then it discards that request. Otherwise the node inserts its address into the RREQ packet and forwards it to the neighboring nodes. After the destination node D receives the RREQ packet along with its address contents of the route that it travelled, it send a RREP packet in the same route that it travelled. The source node S may receive multiple the RREP message along with the address that it travelled. And this can be considered as multiple paths to the destination node.

2.2.Implementation of GA

In this section we describe the design of the GA for the SP problem. The design of the GA has components like genetic representation [1], population initialization, fitness function, selection scheme, crossover and mutation. A routing path contains of sequence of nodes in network. The genetic algorithm is applied to paths that is been obtained from the route discovery phase. A routing path is encoded by a string of positive integers that indicating the IDs of the nodes in the network. The length of the string should not be more than the number of nodes present in the network.

2.2.1 Initial population

In GA each chromosome represents a potential solution and this can contain more than one solution initially. The paths obtained from route discovery phase are considered as initial chromosomes.

2.2.2. Fitness function

For an obtained solution we should be able to evaluate its quality accurately which can be done with the help of fitness function. Our goal of using this GA is to find the shortest path, lowest throughput between source and destination and the larger buffer size that the path has. It is important to obtain the shortest path and lowest delay time as the primary concern then we can choose according to the buffer size. The fitness of each chromosome can be calculated as,

$$f(Ch_i) = [\textstyle\sum_{l\in P(s,r)} c_l + c_d]$$

The Ch represents the chromosome fitness value and Cd the delay time taken by each chromosome where Cl represents the cost of the path. The above fitness function is been maximized and involves only shortest path and delay constraint, the buffer size for every path is been checked in the evolutionary process.

2.2.3. Selection scheme, crossover and mutation

Selection plays a key role in improving the quality of population of chromosomes. The selection of chromosome is purely done on the result of fitness function. Crossover is done to find the better solution from current one. Since chromosome are been used as path structure, every time we choose two chromosomes Chi and Chj for crossover. Chi and Chj should have at least one common node mentioned as v. Now we have two paths Chi(s→r) and Chj(s→r). Now we have v in both paths can be mentioned as Chi(s→v) and Chi (v→r), Chj(s→v) and Chj(v→r). Now we exchange the sub path Chi (v→r) and Chj(v→r). The population will undergo mutation after the crossover had been performed. Both crossover and mutation may produce infeasible solution so we check it is acyclic. The crossover can be explained with the following example.

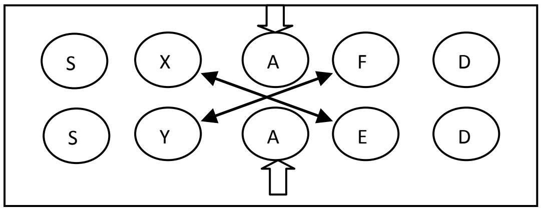

Fig 2: Initial chromosome

In the above example A is the common node in both chromosomes. So by performing GA we obtain new two more chromosomes in order to obtain optimal value.

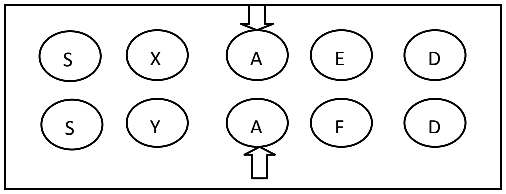

Fig 3: Chromosomes obtained from Initial chromosome

2.3. Backup routing scheme

In this section we discover a backup path from source to destination in case of primary path link failure. By using GA we obtain the optimal path from source to destination, and in the same phase we find an alternate path to be used in link failure. The [2] alternate path will be next best path when compared to the optimal path. By this method when a primary path fails we can recover the connection by utilizing the backup paths. This backup path routing contains three main functions: connectivity management, path discovery phase and path maintenance phase.

2.3.1. Path discovery phase

The backup paths intersect with primary paths to establish a braided path structure. The primary path and backup path are established during the route discovery phase itself when we find optimal path by using GA. The backup paths are geographically closer to the primary paths. And we have discussed enough about route discovery phase we will go now to path maintenance phase.

2.3.2. Path maintenance

The data packets are delivered via the primary path till the primary path is disconnected. When a node detects a link failure, it utilizes the backup path in place of primary path. This is done with the help of RERR message where when a node faces the link or node failure it will send a RERR message to the source node that that initiates the routing process. So the source node chooses the backup path from where the link has broken instead of finding a new route by reroute discovery process. This is explained well in the Fig.3. Where S is source node and D is the destination node and other nodes acts as intermediate nodes. In this diagram the data is been sent initially in the primary path. When the node 'F' faces the link or node failure it sends a RERR message to the source node. Now the source node knows where the failure has occurred and it chooses the backup path that is from 'A' it chooses 'E' as its path and continues to send the data packet. So now there is no necessary for reroute discovery mechanism in case of link failure which avoids time and power consumption.

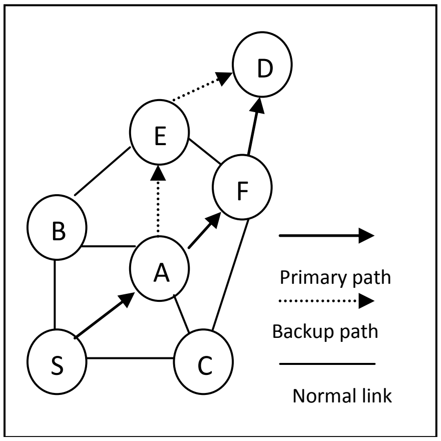

Fig 4: Backup path selection

2.3. Security model

Protecting our network from malicious attacks is an important and challenging issue in a mobile ad hoc network. An intruder node can launch any type of attacks like routing misbehavior or packet forwarding misbehavior or sometimes both attacks also [6]. The routing misbehavior attacks means the malicious node may advertise wrong routing information or a wrong distance metric than its actual size to be or a wrong sequence number. The packet forwarding misbehavior means the malicious node purposely disturbs the data forwarding activity. In order to avoid these attacks we use self organized security mechanism which monitors their neighbor nodes and packet forwarding behavior of its neighbor at all time. So we use a valid token to be carried out by the entire legitimate node which is certified while any node without token are been thrown out of network membership. The legitimate node can renew its token from its neighbor before the token expires. In collaborative monitoring all the nodes within a local neighborhood monitor each other. Token renewal: all the legitimate nodes renew the token with their neighborhood node. Token revocation: The neighbors of a malicious node collaboratively revoke its current token.

2.3.1. Collaborative monitoring

The self organized security mechanism monitors the routing and packet forwarding operations of each node in a fully decentralized and localized manner. Each node overhears the channel, monitors the behavior of its neighbors, and discovers consistent misbehavior as indications of attacks. Moreover, local neighboring nodes collaborate with each other to improve the monitoring accuracy.

2.3.2. Token renewal

Self organized security renewals its token each legitimate node contains the fields like <owner _id, signing_ time, expiration time>. We use public key cryptography primitives to protect the tokens. The public key is known to each the nodes when they join the network, while there is a secret key to sign in the token by a node. Each node contacts its neighbor node to renew its current token before it gets expire. The node that needs to renew its token broadcast a TREQ packet to its neighbor node along with its current token and timestamp. The neighbor node after receiving the TREQ constructs the new token with the expiration time along with the signing time in the TREP then unicasts to the sender that from where it received TREQ.

2.3.3. Monitor Routing Behavior

Our basic idea is to overhear the channel and cross-check the routing messages announced by different nodes. In such protocols, the routing activity of a node is a three-step process: receiving routing updates from neighboring nodes as inputs to a routing algorithm; executing the routing algorithm; and announcing the output of the routing algorithm as its own routing updates. The monitoring task is to verify whether the routing algorithm executed by a node follows the protocol specifications.

2.3.4. Monitor Packet Forwarding Behavior

Each SCAN node also monitors the packet forwarding activity of its neighbors. This is achieved by overhearing the channel and comparing ongoing data transmission with previously recorded routing messages. We currently focus on three kinds of forwarding misbehavior, namely, packet drop, packet duplication, and network-layer packet jamming, and develop simple algorithms to detect each of them. Packet drop means that a node drops the packets that it is supposed to forward for its neighbors; packet duplication means that a node duplicates the packets that it has already forwarded; and packet jamming means that a node sends too many packets and occupies a significant portion of the channel bandwidth.

3. SIMULATION

In this section we evaluate and compare the performance of ordinary genetic algorithm for MANET with secure on demand routing protocol for MANET using GA by using NS-2.

3.1. Simulation environment

In our simulation, the MAC protocol is IEEE 802.11 and the propagation model is two ray ground reflection models. In the below table we list the simulation parameters. The simulation scenario consists of 20 nodes randomly distributed in 500m x 500m square area. Maximum speed of nodes is varied in five different maximum moving speeds: 0/5/10/15/20 m per second. We consider only the continuous mobility case. The transmission range of every node is 100m. There are 20 constant bit rate CBR traffic resource distributed over the network. The CBR data packets are 512 bytes, and the sending rate is 4 packets per second. Simulations run for 300 seconds.

3.2. Simulation

Table 1: Simulation parameters

Parameter	Value	Description
Simulator	NS2	Simulator tool
Simulation time	300s	Maximum execution time
Simulation area	500mx500m	Physical boundary of the network
Number of nodes	20	Nodes participating in the nodes
Transmission range	100m	Frequency of the node
Max speed	0,5,10,15,20 m/s	Speed of nodes
CBR flows	20	Constant Bit Rate link used
Data payload	512 bytes	Packet size
Sending rate	4 packets/s	Max no of sending packets
Movement model	Random waypoint	Network connection

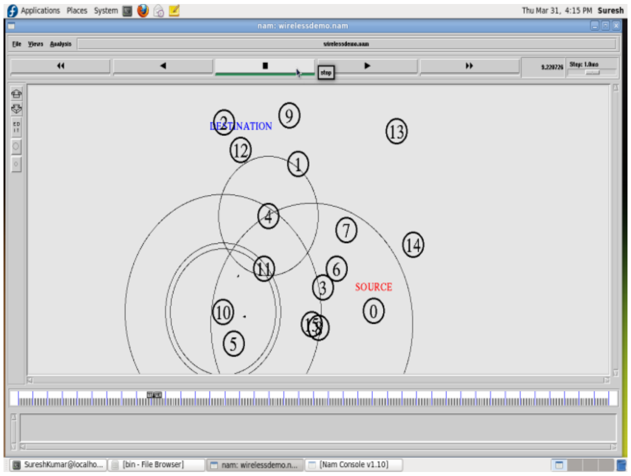

Fig 5: Source node sending packet to destination

This work evaluates the ability of genetic algorithm and proposed secured on demand routing protocol for MANET using GA to provide secured and efficient result.

4. RESULTS

Although the performance of all protocols resembles those in the static case, their performances becomes more apparent at higher speeds.

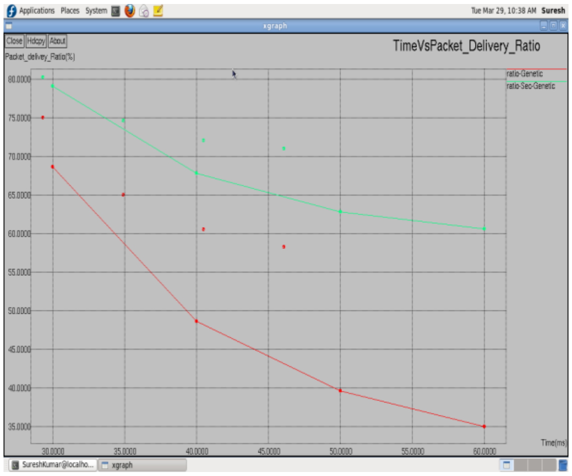

Fig 6: Packet delivery ratio

Fig 6 illustrates the comparison of packet delivery ratio, in which the ordinary genetic algorithm for MANET with secure on demand routing protocol for MANET using GA. Simulation results shows that the packet delivery ratio is more than the ordinary GA because we use security also in our protocols which provides us a confirmation that there is no malicious node present in the routing.

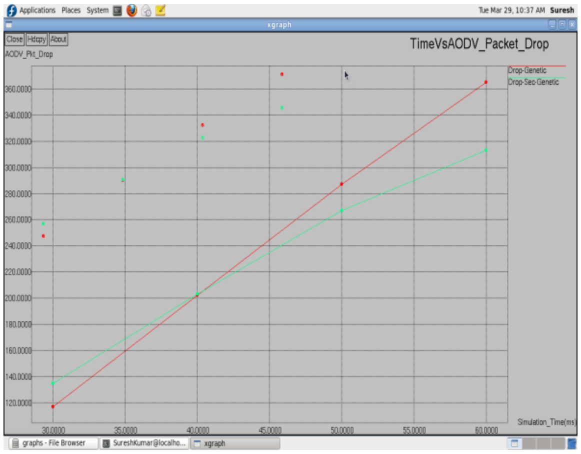

Fig 7: Packets drop

Fig.7 illustrates the comparison of packet drop ratio in the network by using the normal GA for MANET and secure on demand routing protocol for MANET using GA. Initially the there maybe liitle packets loss in our protocol but it will be overcomed in few seconds to give us a better result. Hence by using the backup path no packets will be dropped. No malicous nodes can participate in the network since we use security agent in the network to provide secured routing rotocol.

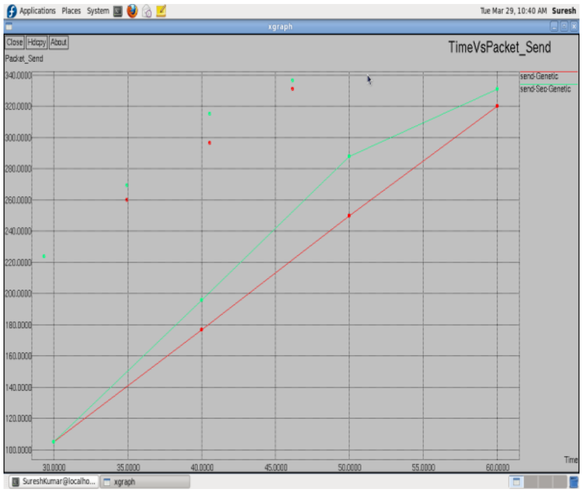

Fig 8: Packets sent from a node

Fig.8 shows the packet sent by secure on demand routing protocol for MANET by GA and ordinary genetic algorithm. The packets sents are more when compared to ordinary GA because we consider buffer size as the parameter in GA to provide maximum data to be sent in a time. So we can transmit more amount of data than the normal routing protocols. So we get a efficient protocol to transmit large amount of data in a small period of time.

5. CONCLUSION

This work presents a secure on-demand routing protocol for MANET using GA. The proposed schemes utilizes the genetic algortihm to find the optimal path from the route discovery. These optimal path are not only shortest path, it is the shortest end to end delay path and that can transmit more amount of data that can be sent in the network. And we use the alternate paths to be used in case of link failure occurs and it avoids reroute discovery to be done. The nodes which are participating in the paths are been authenticate before it enters the routing phase so malicious node which may create linkk failure are been avoided. So we get a efficient routing protocol for MANET that is secured and efficient. We simulate our protocol using NS2 and obtain the result that shows the packet drop ratio is very low and packets sent are high than the existing routing protocols.

6. REFERCENCES

[1] Shengxiang Yang, *Member, IEEE*, Hui Cheng, and Fang Wang, *Member, IEEE*, "Genetic Algorithms with Immigrants and Memory Schemes for Dynamic Shortest Path Routing Problems in Mobile Ad Hoc Networks", in proc. IEEE transactions on systems, man, and cybernetics-part C: applications and reviews, vol. 40, no. 1, January 2010, pp. 52-63

[2] Kilhung Lee, "A backup path routing for guaranteeing bandwidth in mobile ad hoc networks for multimedia applications", in proc. springer multimedia tools appl, 11 January 2011.

[3] Tsung-Chuan Huang, Sheng-Yu Huang and Lung Tang, "AODV-Based Backup Routing Scheme in Mobile Ad Hoc Networks", in proc. IEEE 2010 International Conference on Communications and Mobile Computing, 2010 IEEE.

[4] G.Lavanya,C.Kumar and A.rex Macedo arokiaraj, "Secured backup routing protocol for Ad hoc networks", in proc. IEEE 2010 International Conference on Signal Acquisition and Processing,pp.45-50, 2010.

[5] Luo Chao, Li Ping'an , " An efficient routing approach as an extension of the AODV protocol", in proc. IEEE, vol.1,pp. 95-99,2010.

[6] Hao Yang, James Shu, Xiaoqiao Meng, and Songwu Lu, "SCAN: Self-Organized Network-Layer Security in Mobile Ad Hoc Networks", in proc. IEEE, IEEE journal on selected areas in communications, vol. 24, no. 2, February 2006.pp .261-273

[7] Kun-Ming Yu · ChangWu Yu · Shi-Feng Yan, "An Ad Hoc Routing Protocol with Multiple Backup Routes", in proc. Springer Science+Business Media, LLC. 2009, 1 november 2009.

[8] Qing Chen, Xiaodong Lin, Sherman Shen, Kazuo Hashimoto, and Nei Kato, "A Group-Based Key Management Protocol for Mobile Ad Hoc Networks", in proc. IEEE "GLOBECOM" 2009.

Website

[1] XGraph homepage, URL: http:/www.isi.edu/nsnam/xgraph.

[2] NAM: Network Animator, URL: http://www.isi.edu/nsnam/ns/ns-documentation.html

AUTHORS PROFILE

D. Suresh Kumar is currently pursuing M-Tech in Computer Science and Engineering in VIT University, Vellore India and pursued his B.E from Arunai engineering college affiliated to Anna University. His area of interest includes Mobile Ad hoc network, Semantic web service and Genetic algorithm.

Manikandan K is working as a Asst. professor (Senior) in School of Computing Sciences and Engineering, VIT University, Vellore, India. He was the recipient of academic excellence award. He was the gold medalist of Anna University during his M.E. (CSE). His area of interest include MANET, Sensor networks, Cluster computing.

M. A. Saleem Durai received his MCA from Bharathidasan University, Tiruchirapalli, Tamilnadu, India in 1998; M. Phil. from Madurai Kamaraj University, India in 2008 and pursuing his PhD at VIT University Vellore. He is an Assistant Professor (SG) in the School of Computing Sciences and Engineering at VIT University, Vellore, Tamilnadu, India. He has authored many international and national journal papers to his credit. His research interests include data mining, fuzzy logic, and rough sets. Mr.Saleem Durai is associated with many professional bodies CSI, and IEEE.