International Conference on Systems, Science, Control, Communication, Engineering and Technology 2016 [ICSSCCET 2016]

ISBN	978-81-929866-6-1
Website	icssccet.org
Received	25 – February – 2016
Article ID	ICSSCCET090

VOL	02
eMail	icssccet@asdf.res.in
Accepted	10 - March – 2016
eAID	ICSSCCET.2016.090

Enhancement of Network Security in Snack Routing Strategy Using Trust Agent

M S Gowtham[1], R Sarath Kumar[2]
[1]Karpagam, Institute of Technology, Coimbatore,
[2]Sri Krishna College of Engineering and Technology, Coimbatore

Abstract — *Routing plays an important role for the efficient communication among the nodes. The problem associated with MANET is continuous topology changes which leads to more control message overheads .Snack Routing Strategy (SRS) is used to continuously inform about the topology changes to all the nodes in the network without any advertisement messages by using artificial snack which flows across the network. SRS reduces the network bandwidth overheads and end-to-end delay. But it suffers from security issues arise and some malicious nodes also may take part in the communication. For that trust agent is added to the mobile nodes, communication between the nodes takes place if those nodes enforce same set of policies. Before a node to join in the network, it verifies its trustworthiness of enforcing required set of policies. Our extensive ns-2-based simulation results have shown that the proposed scheme provides better performance in terms of packet delivery fraction, normalized routing overhead and throughput based on maximum speed, number of sources and pause time.*

1. INTRODUCTION

Mobile ad hoc networking is to support robust and efficient communication among mobile nodes. It consists of dynamically and rapidly changing network topology with bandwidth limited wireless link. A MANET consists of mobile nodes which are free to move arbitrarily across network area. MANET may operate in isolation, or may have gateways and interface with a fixed network. It acts as a "stub" network when connects to a fixed internetwork. Stub networks carry traffic originating for internal nodes.

MANET nodes are equipped with wireless transmitters and receivers using antennas which may be Omni directional for broadcast, highly-directional, steerable type. At a given point in time, depending on the nodes position and their transmitter and receiver coverage patterns, transmission power levels and co-channel interference levels, ad-hoc network exists between the nodes. This ad hoc topology may change with time as the nodes move or adjust their transmission and reception parameters [1].Throughput of wireless communications with the effect of multiple access, fading, noise, and interference conditions makes less than maximum transmission rate.

Some or all of the nodes in MANET may rely on batteries or other exhaustible means for their energy. For these nodes, optimization of energy may be conserved. Mobile wireless networks are generally more prone to physical security threats than are fixed-cable nets. The increased possibility of eavesdropping, spoofing, and denial-of-service attacks should be carefully considered. Existing link security techniques are often applied within wireless networks to reduce security threats. The decentralized nature of network control in MANETs provides additional robustness against the single points of failure of more centralized approaches. The need for scalability is not unique to MANETS.

Due to the lake of administration capability, a MANET is easy to be deployed without any pre-installed infrastructure [5]. Accordingly,

Cite this article as: M S Gowtham, R Sarath Kumar. "Enhancement of Network Security in Snack Routing Strategy Using Trust Agent". *International Conference on Systems, Science, Control, Communication, Engineering and Technology 2016*: 466-474. Print.

MANETs are sometimes called multi hop communication networks. Proactive Protocols [7,8] keep track of routes for all destinations in the ad hoc network, as the routes can be assumed to exist in the form of tables. The main advantage is that Communications with arbitrary destinations experience minimal initial delay from the point of view of the application. The disadvantages of proactive protocols are that Additional control traffic is needed to continually update stale route entries.

Reactive Protocols acquire routing information only when it is actually needed [9-10]. The advantage is that due to the high uncertainty in the position of the nodes, however, the reactive protocols are much suited and perform better for ad-hoc networks [2]. The disadvantages of reactive protocols include high latency time in route finding and excessive flooding leading to network clogging.

Proactive and reactive protocols not provide a guarantee for short waiting time before the transmission of data packets [4]. This is because the source node does not know which neighbor to select as the next hop for the packet due to the unpredictable change in the network topology [5]. Therefore, discovering and maintaining a route using reactive routing protocols is difficult as the source node has to find the route to the destination [6-7]. A hybrid routing protocol tries to combine the advantages of both proactive and reactive protocols [8]. Zone Routing Protocol (ZRP) [11, 12], which divides the network into several routing zones with each node belongs to any one of the zone. Each node proactively maintains a routing table for nodes within its zone and reactively finds a route to its destination node if the destination lies beyond its zone radius. Most of the routing protocols suffer from control packet flooding, which results in a scalability problem.

The new routing strategy for ad hoc networks, which is called Snack Routing Strategy (SRS).

SRS is to continuously inform the network mobile nodes with any changes in network topology without overloading the network by a huge number of control messages. SRS is hybrid routing because routing information of each node is continuously updated using artificial snacks. Advantage of SRS includes no periodic routing advertisement messages, minimizes the mobility impacts on the routing efficiency, conservation of battery power, minimizes the end-to-end delay of data transmission as it accurately guarantees the shortest path from the source to destination.

It is ineffective that malicious nodes also take part in communication and it may possible that the newly joint malicious node distract the process of informing the topology changes to all other nodes. For that, in order to provide the security to the network trust agent with policy enforcement mechanism is used.

There are several security policies available in traditional distributed system [17] [18]. Trust agents is normally using for improving the security in MANET but it is insufficient level because of only known to be trusted nodes only communicates with each other. So Trust agent with policy enforcing mechanism is proposed to enhance the security level [16]. By this approach each node having a trust agent which possess set of policies. Policy enforcing mechanism creates a trusted multitier network. In this method it is also possible that nodes can be member of multiple multitier networks simultaneously. Policy enforcement takes place uniformly without any prior trust with other nodes.

This paper consists of following sections: Section 2 explains the proposed routing mechanism. Section 3 explains the detailed design of Snack Routing Strategy. Section 4 deals with trust agent with policy enforcing mechanism Section 5 explains the result obtained by simulation. Section 6 represents the conclusion of the work.

2. Samanet

MANET does not possess proper infrastructure so it suffers from the problem of administration capabilities. Even though MANET is more flexible for making temporary communication among the neighbor, due to lack of administration degrades the communication efficiencies due to continuously changing topology. So it is necessary to include the administration capability for reliable communication.

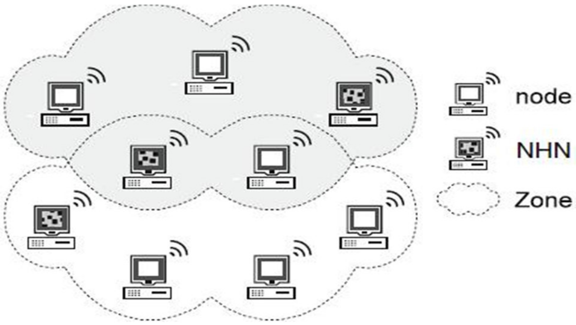

Figure 1 A SAMANET with three NHNs

Cite this article as: M S Gowtham, R Sarath Kumar. "Enhancement of Network Security in Snack Routing Strategy Using Trust Agent". *International Conference on Systems, Science, Control, Communication, Engineering and Technology 2016*: 466-474. Print.

A new generation of MANET called Semi-Administrated Mobile Adhoc Networks (SAMANETs). A node in SAMANETs act as both a terminal and router. Some of the nodes are added with additional capabilities which are called Network Header Nodes (NHNs) which is used to improve the network routing. Due to NHN acts as the central point which is responsible for making routing decisions in the network. So the already existing route can be continued if shortest path available. NHN is a mobile node that can act as terminal or router; it has no control over other nodes. It can able to change the routing decisions if it acts as intermediate node for connection between source and destination. It has own set of security issues.

3. Snack Routing Strategy

SAMANET has additional capabilities of continuously changing topology feature of MANETs. It is used to find a route from source to destination and also to identify which one is shortest. The aim of SRS is to find the shortest path between source and destination, minimize the advertisement messages in order to achieve scalability and short convergence time to establish the route.

SRS is to continuously inform the network mobile nodes with any changes in network topology without any changes in network topology without any large amount of control messages. This is achieved by snack routing strategy by using a control packets called ―snack(s)‖, which is continuously moving among the network. Snack consists of three parts they are header, snack body, and the footer. Destination address are stored in the header, the nodes which are visited by snacks is updated in snack body and the footer consists of snack ID and the snack age .Every network consists of limited number of snack which flow across the network. In order to identify the snack number snack ID is provided. If the snack body is full then new snack is create. NHN is responsible for creating the snack, any node can able to delete the snack if the snack body is full as shown in figure 1. Due to that limited number of snack flowing across the network. So the transfer of data packets without affecting the network speed, limited usage of bandwidth and small amount of time to setup a route between two nodes.

3.1 SRS Algorithm

The snack migration deals with how a snack chooses the next node to reach next hop to destination. The snack is mainly to update the topology changes in snack body. When a snack reaches a node, checks the age of the snack. If the snack body reaches a maximum length α, the last part of the registered snack β is copied as the first part of new snack with the condition that α>β. This process is to identify the dynamic change of network topology. The newly picked sequence of length β is record in its sequence table (ST).The sequence starts with initial value then degrades with time.

The snack will allow to migrate it to the next node only it to the next node only if age less than α, which is maximum number of hops to be allowable. By knowing the stored sequence able to identify up-to-date topology of the network as illustrated in figure 2.

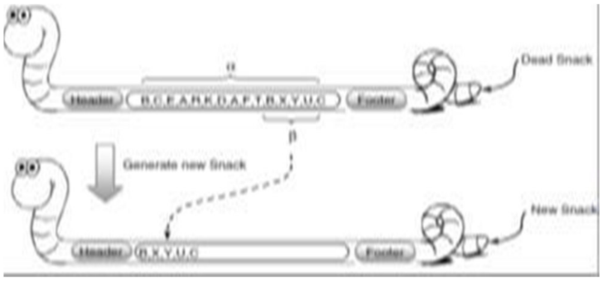

Figure 2 Creating a new snack carrying the fresh sequence of the disposed one

The Snack route learning and maintenance algorithm is given by

1. SAMANET is partially connected graph G=(V,E)
2. Current node ni
3. Sequence table & fill route table of ni
4. If node=destination
    a. send ACK to previous node Otherwise
    b. Find the next hop using routing table
5. If ACK is not received Send route error packet to previous node.
6. If node =source Use call back mechanism to discover route

Cite this article as: M S Gowtham, R Sarath Kumar. "Enhancement of Network Security in Snack Routing Strategy Using Trust Agent". *International Conference on Systems, Science, Control, Communication, Engineering and Technology 2016*: 466-474. Print.

3.2 Route Learning Procedures

Each node in the SAMANETs maintain four tables in its internal cache, which are i) Sequence Table (ST),ii) Routing Table (RT),iii) Connection Table(CT),iv)Intent Table (IT) Path sequence obtained by set of nodes which is visit by foraging snack is record in Sequence Table. Routing Table stores the available route from one node to the other one in the network as learned from ST.CT stores the existing active connection between source and destination that use the node as intermediate.IT deals with forming a route from remote source with remote destination and stores the intent an entry in the nodes' sequence table consists of triple (Snack_ ID, Sequence, Seq _ Fresh ness).On the other hand, an entry in the nodes' routing table consists of triple (Network_ , Route, Route_ Fresh ness),hence, each entry in RT(x) represents the shortest available route that connects x to another network node with a corresponding freshness values. For changing in network topology, the freshness value of each route changes with time. Predict the possible routes to other nodes by collected sequence value that stored in ST.

Three possible methods to discover new routes and update old ones. These are (i) receiving a snack, which add a path sequence to the nodes' sequence table,(ii) sequence expiration, which takes place as soon as the sequence freshness values reaches zero, which may also delete or update in RT, and (iii) a mobile nodes enter or leave the zone of the node .

If the node leave from the zone, its necessary to delete the route from current node to the leaved node and also delete the updating route of that node. The route learning process is to enter the routing table with valid path from one node to another node with routing interval ω. The algorithm tries to discover the shortest valid route from the node to every node in the network. Even though route learning procedure is more efficiency, it suffers from route failure to the remote node. The source node can cooperate with the nodes located within its transmission range (zone) to reach such remote destination node.

3.3 Cooperative Route Discovery Scheme (CRDS)

SRS relies on CRDS as source node communicates with neighbor to setup connection to the destination. CRDS consists of two types of control packets, that are Forward Worm (FW) and Backward Worm (BW). FW tends to show the availability of route to destination and discover another one when that route is no longer availability.BW is to source node to start to transmission of data as FW discovers a valid route.

A node receiving a FW for first time creates a record in CT. It consists of record in CT consists of Source Address, Connection ID, Next Hop, and Previous Hop. Duplicate FWs is the forward worms with the same source address and connection identifier which are discarded by setting the Duplicate_ Error flag. The previous node deactivates the connection to the link. For the transfer of packets to the destination next hop value is used and to obtain route error packet during link failure, previous hop is used. To avoid overflow, the route which not Longley used are removed from CT. When FW reaches a node it checks for shortest path. If its exists, freshness is compared with that of the original worm route, and then the fresher route is followed by the worm. The rejected route can be used in next hop if valid path available to destination. Due to the movement ability of the network nodes, the next hop may be change continuously. At this time, FW tries to switch to the previously rejected route , if no alternative route, node x will switch to the callback mechanism to discover new routes to Destination .Once the FW reached, destination node reads the information carried by FW, kills FW, and generates a BW, moving in the reversed route. Once BW reaches the source, the source can start the transmission to the destination immediately. If BW fails then it checks the Routing Table (RT) for finding valid route to destination, if there is no path means then source node follows callback mechanism to find new route.

3.4 Callback Mechanism

Callback procedure is the steps to be carried out when worm not follow the roué which enter in its body if there is no alternate route availability. During this mechanisms two procedure can be follow which are i) store the route which has been visited by receiving worm, ii) send its intent to the destination. All the nodes within the zone search their routing table for valid path to its destination. The obtained routes are sending back to source node to compare the alternative route to choose the fresher one. Generate a new worm with same ID which follows the new route. Then send the message to its neighbor to cancel the records in all Intent Tables (IT).

Suppose if no alternate route is found to the destination node within the zone, all nodes in zone broadcast their corresponding intents to make connection to its destination until a route is found. When the route is identified with same Intent_ID then, Intent Reply Message (IRM) generates by corresponding node. Route sequence to destination to reach source by IRM moves in backward direction.

3.5 Link Failure and Route Maintenance

Route maintenance is process of maintaining the route which are created by route discovery process .It deals with monitoring the operation of route which are currently in use. Route discovery process made again if any fault is detected. Topology of MANET changes continuously, which leads to route discovering process changes suddenly. To overcome this, once the route between two nodes is set, the data packet is responsible to maintain the route.

SAMANETs use a hop-by-hop acknowledgement at the data link level in order to provide early detection and retransmission of lost and corrupted packets. In each hop the route entry is made only if it is valid for long time, so the route maintenance can be easily achieved. If the transmission problem occurs the intermediate node sends a route error packet to the previous node across the route. As the route error packet is received by a node, the next hop is calculated by reading the previous hop value of the CT entry of that route. The route error packet propagated until reach the original source node of the packet encountering a transmission error. When the route error packet is received by the source, the source immediately stops transmission, and then uses the call back mechanism to discover another route to the destination node.

4 Trust Agents with Policy Enforcing Mechanism

For policy enforcing mechanism each node possesses a trust agent, which is to protect the policy enforcement for being communication between nodes. When a node joins in a trusted tier a trust key is provided to new node by the agent in order to proving the execution of same set of policies. If a new node wishes to join in network it first communicate with the tier manager then to all other nodes in the network. A tier is made by node begins to enforce the tier policy. It creates tier key which is to authenticate for communication. The first member of tier is originator, which broadcast an invitation to its neighbor .The tier originator sets the size of tier by setting a TTL value in the request message. The TTL value decreases by after joining of each node in the tier and if reaches zero, it stops forwarding invitation message.

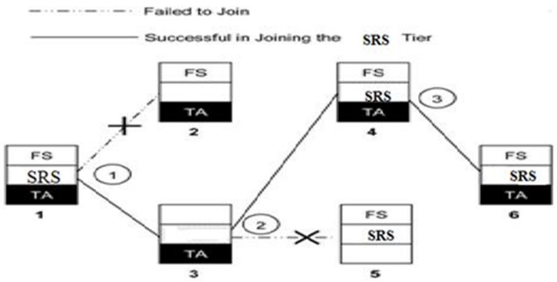

Figure 3 Creation of Trust Agents on nodes

If the neighbor node decides to join the tier, it rebroadcast the invitation as same as routing tier creation. Once the node does not join in tier, it just forwards the invitation message to its neighbor and it acts as router for communication with other tier member.

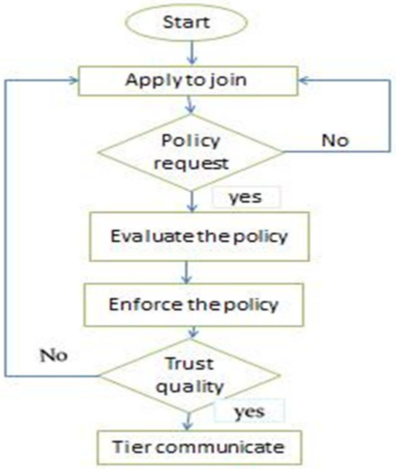

Figure 4 Flow diagram of policy enforcing mechanism

Tier manager is to create, join and merge in to tier. The tier creation process is made but formation of tier key by tier manager. It's also possible that communication between one tier manager to another manager. Both tier manager and enforcer must be trusted. This can be achieved by code base. For joining the new node in tier it verifies the trust worthiness and enforces the tier policy as illustrated in figure 3.

Advantages of this mechanism are i) policy enforcement in multitier networks are distributed without relying on any central trusted points. ii) trusted networks are self-organized i.e. able to establish and manage without predefined deployment. iii) flexible enforcement of policies.

Cite this article as: M S Gowtham, R Sarath Kumar. "Enhancement of Network Security in Snack Routing Strategy Using Trust Agent". *International Conference on Systems, Science, Control, Communication, Engineering and Technology 2016*: 466-474. Print.

5. Simulation Environment

A simulated network with 50 nodes is considered and the random way point mobility scheme is employed to model the node movement. More specifically, at the beginning of the simulation, the nodes are randomly placed on a simulation area of 1000m ×1000 m .Results reported in this paper are performed under ns-2 network simulator. It provides a suitable simulation environment for protocols which require a system programming language that can efficiently manipulate bytes, packet headers and implement algorithms. Simulations are run by considering SRS, DSR and AODV [14-15] routing protocols. In order to get realistic performance, the results are averaged for a number of scenarios. In this paper, we focus on the impact of network performance in terms of throughput, packet delivery rate, routing overhead.

Table I Simulation Parameters

Parameters	Values
Simulator	NS-2.34
Simulation area	1000m X 1000m
Simulation time	900s
Traffic type	CBR
Mobility model	Random waypoint
Max .snack age	20
Route learning interval	200s
Protocols used	SRS,AODV,DSR
Mechanism	Trust agent with policy Enforcement

5.1 Simulation and Results

In this section, the proposed protocol is based on compare performance of reactive routing protocol DSR and AODV with hybrid SRS based on various metrics. The evaluation is made based on the following parameters:

Packet Delivery Fraction: It is the ratio of data packets delivered to the destination to those generated by the sources.

Routing Overhead (RO): It is the total number of control or routing packets generated by routing protocol during the simulation.

Normalized Routing Load (NRL): Number of routing packets transmitted per data packet delivered at destination.

Average End-to-End Delay: It is defined as the time taken for a data packet to be transmitted across an MANET from source to destination.

Through put: Through put of the routing protocol means that in certain time the total size of useful packets that received at all the destination nodes.

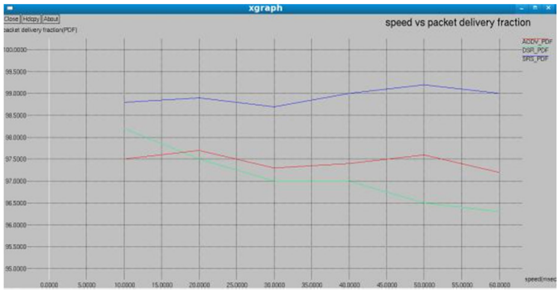

Figure 4 Speed vs. Packet Delivery Fraction

The packet delivery fraction for DSR, AODV, and SRS was measured using several pause times as shown in figure 4. But the packet delivery fraction starts to gradually degrading in the case of DSR and AODV when there is increase in number of sources (40) and with

Cite this article as: M S Gowtham, R Sarath Kumar. "Enhancement of Network Security in Snack Routing Strategy Using Trust Agent". *International Conference on Systems, Science, Control, Communication, Engineering and Technology 2016*: 466-474. Print.

the increase in speed of nodes. SRS outperforms all other algorithms as the foraging snacks update the nodes‟ routing tables with up-to-date routing information.

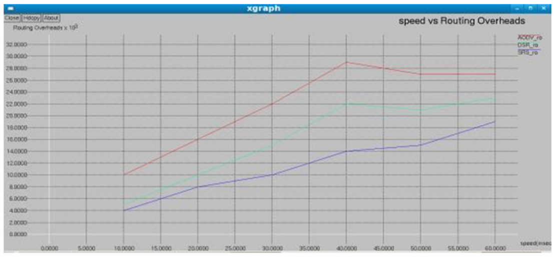

Figure 5 Speed vs. Routing Overheads

DSR protocol has significantly low routing overhead than AODV when the mobility is increased. When number of sources is low (10), the performance of the three routing protocols is similar regardless of mobility as shown in figure 5. Further, DSR always have a lower routing overhead than AODV this may happened due to the use of the routing cashes, which are used to reduce flooding. SRS outperforms both DSR and AODV due to its awareness of the continuous network topology changes.

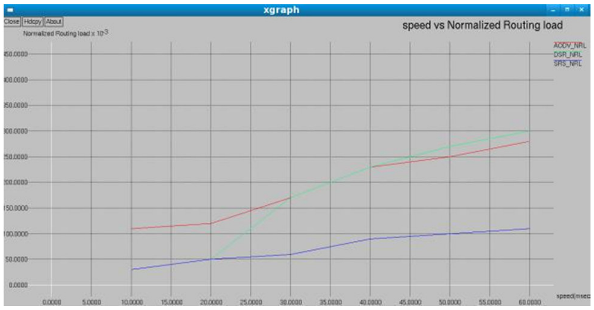

Figure 7 Speed vs. Average End-To-End Delay

Delay in DSR is too much higher than AODV and SRS especially with the increase of network load (e.g., 40 sources) as illustrated in figure 7. Over all in case of real time packet delivery, SRS is the best choice, then AODV. On the other hand, DSR produces more delay due to route caching. Although DSR can respond a route quickly, it yields a long delay when a route is rebuilt. This is because when source node receives RERR packet, it will try to find alternative routes from the route cache. If alternative routes are not available, the source node, then, will enter route discovery phase to find new routes.

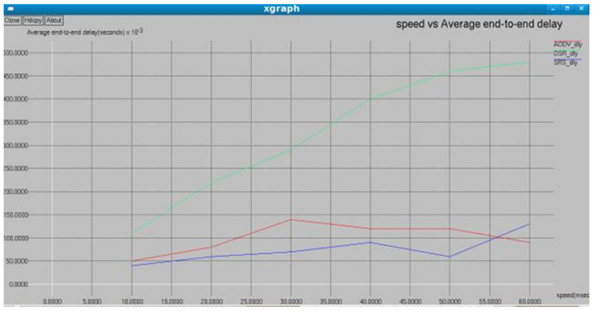

Figure 6 Speed vs. Normalized Routing Loads

SRS introduces a consistent behavior even with changing the movement speed and number of connections (sources). It outperforms both DSR and AODV in almost all cases as illustrated in fig 6. On the other hand, with low number of sources (10) and low mobility, DSR performs better than AODV. But when the mobility increases, AODV perform better than DSR in most cases.

Cite this article as: M S Gowtham, R Sarath Kumar. "Enhancement of Network Security in Snack Routing Strategy Using Trust Agent". *International Conference on Systems, Science, Control, Communication, Engineering and Technology 2016*: 466-474. Print.

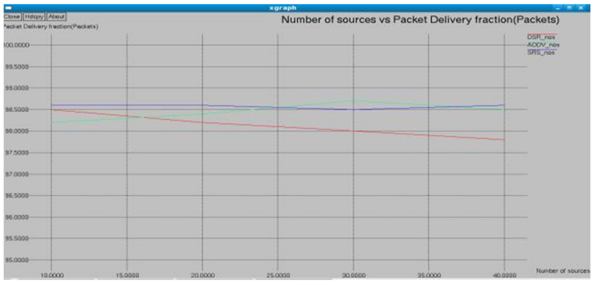

Figure 8 Number of Sources vs. Packet Delivery Fraction

The packet delivery fraction is measured for each of the routing protocols using several pause times with a maximum speed of 10 m/s, and then averaging the results. It is also concluded that DSR performance degrades with the increase of the number of sources. Also, performance of AODV and SRS are much closed to each other. However, the proposed SRS outperforms AODV in most cases as shown in figure 8.

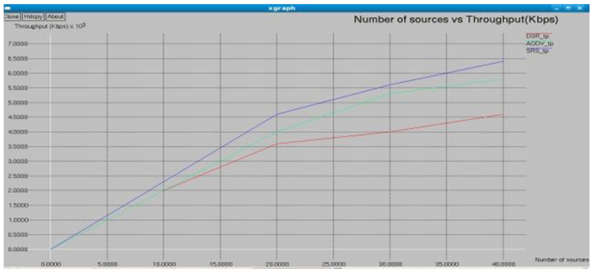

Figure 9 Number of Sources vs. Throughput

Throughput of the routing protocol means that in certain time the total size of useful packets that received at all the destination nodes. The unit of throughput is MB/s, however, in simulation; consider Kilobits per second (kb/s) the throughput for each routing protocol (DSR, AODV, and SRS) is measured using different numbers of source nodes, and then averaging results. The maximum speed was fixed to 10 m/s, the proposed SRS strategy outperforms both AODV and DSR as it has a good ability to transmit almost all data packets during the test period as shown in figure 9.

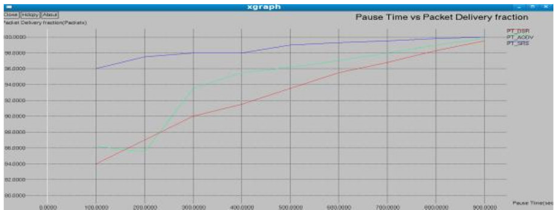

Figure 10 Pause Time vs. Packet Delivery Ratio

Using ten parallel connections, PDF is measured for the three competing routing protocols. In the case of low mobility (large pause time), the performance of the tree protocols is very similar. They are able to transfer most of the packets as a result of the lazy change of the network topology. However, this changes with increasing mobility. In the case of high mobility (small pause time), SRS outperforms both DSR and AODV in all cases. Further, AODV outperforms DSR in most cases as shown in figure 10.

6. Conclusion

A new scalable routing, which is called SRS. SRS tries to continuously inform the network mobile nodes with the changes in the network topology without overloading the network by a huge number of control messages. SRS is hybrid as the routing information at each node is continuously updated using artificial snacks; however, the path between the source node and the destination is constructed on demand. It also relies on a learning by accumulation concept, hence, new routes can be discovered by learning the accumulative data stored at the nodes routing tables using several foraging artificial snacks.

SRS offers a number of potential advantages over conventional routing protocols such as; (i) it uses no periodic routing advertisement messages but used artificial snacks instead, thereby reducing network bandwidth overhead, (ii) SRS minimizes the mobility impacts on the routing efficiency, (iii) battery power is also conserved on the mobile hosts, both by not sending the advertisements and by not needing to receive them, and (iv) SRS minimizes the end-to-end delay of data transmission as it accurately guarantees the shortest path from the source to destination. In spite of its effectiveness, SRS suffers from a relative bigger amount of routing cache requirements than AODV and DSR as each mobile node should maintain four different tables, which are CT, RT, IT, and ST. However, such hurdle can be avoided by limiting the size of the tables to store only the most recent routing information. SRS has been compared against AODV and DSR. Enhancement of network security is achieved by using trust agent with policy enforcing mechanism.Malicious nodes are identified by using tier keys for authenticate the communication which are generated by tier manager.

References

1. S. Nenad, B. Marija, S. Irini and D. Branimir, New algorithm for packet routing in mobile ad-hoc networks, Journal of Automatic Control, University of Belgrade, Vol. 20, pp. 9–16, 2010.
2. M. Lakshmi and P. Sankaranarayanan, Performance analysis of three routing protocols in wireless mobile ad hoc networks, Information Technology Journal, Vol. 5, No. 1, 114–120.
3. Boukerche, A. Bamis, I. Chatzigiannakis and S. Nikoletseas, A mobility aware protocol synthesis for efficient routing in ad hoc mobile networks, The International Journal of Computer and Telecommunications Networking,Vol. 52,No. 1, pp. 130–154, 2008.
4. M. Abolhasan, T. Wysocki and E. Dutkiewicz, A review of routing protocols for mobile ad hoc networks, Ad Hoc Networks,Vol. 2, pp. 1–22, 2004.
5. B. Liang and J. Zygmunt, Hybrid routing in ad hoc networks with a dynamic backbone, IEEE Transactions on Wireless communications, Vol. 5, No. 6, pp. 1–14, 2006
6. K. Tripathi, M. Pandey, and S. Verma, Comparison of reactive and proactive routing protocols for different mobility conditions in WSN, Proceedings of the 2011 International Conference on Communication, Computing & Security, 2011.
7. U. Lee, S. Midkiff, and J. Park, A Proactive Routing Protocol for Multi-Channel Wireless
8. Ad-hoc Networks (DSDV-MC), Proceedings of the International Conference on Information Technology Coding and Computing, Vol. 2, pp. 710–715, April 2005.
9. R. Singh, D. Singh and L. Kumar, Performance Evaluation of DSR and DSDV Routing Protocols for Wireless Ad Hoc Networks, Int. J. Advanced Networking and Applications, Vol. 2, No. 4, pp. 732–737, 2011.
10. P. Sarala, D. Kalaiselvi, Multipath Dynamic Source Routing with Cost and Ant Colony Optimization for MANETS, International Journal of Applied Engineering Research, Vol. 1, No. 1, 2010.
11. Ben Liang, and Zygmunt J. Haas, Hybrid Routing in Ad Hoc Networks with a Dynamic Virtual Backbone, IEEE Transactions On Wireless Communications, Vol. 5, No. 6, JUNE 2006, 1–14
12. Nikaein Navid, Wu Shiyi, and Christian Bonnet. HARP: Hybrid Ad hoc Routing Protocol, International Symposium on Telecommunications, IST 2001, 2001.
13. Z. Haas, A new routing protocol for reconfigurable wireless networks, Proceedings of IEEE International Conference on Universal Personal Communication Atlanta, GA, 1997. pp. 1–11
14. M. Peralman and Z. Haas, Determining the optimal configuration for the zone routing protocol, IEEE Journal on Selected Areas in Communications, Special Issue on Wireless Ad hoc Networks, Vol. 17, No. 8, pp. 1395–1414, 1999.
15. S. Das, Performance Comparison of Two On-demand routing Protocols for Ad hoc Networks, IEEE Personal Communications Magazine special issue on Ad hoc Networking, pp. 16–28, 2001.
16. S. Lee, E. Royer, and C. Perkins, Scalability study of the ad hoc on-demand distance vector routing, ACM/Wiley International Journal of Network Management, pp. 97–114, 2003.
17. Gang Xu, Liviu Iftoden,'A policy Enforcing Mechanism for Trusted Ad Hoc Networks' transaction on dependable and secure computing, IEEE 2011
18. M. Blaze, J. Feigenbaum and J. Lacy, ―Decentralized Trust Management,‖ Proc. IEEE Conf. Privacy and Security, pp. 164-173, 1996.
19. M. Blaze, J. Feigenbaum, J. Ioannidis, and A.D. Keromytis, ―The Keynote Trust-Management System, Version 2,‖ RFC 2704, Sept. 1999.

Cite this article as: M S Gowtham, R Sarath Kumar. "Enhancement of Network Security in Snack Routing Strategy Using Trust Agent". *International Conference on Systems, Science, Control, Communication, Engineering and Technology 2016*: 466-474. Print.