International Journal of Pure and Applied Mathematics
Volume 117 No. 15 2017, 51-68
ISSN: 1311-8080 (printed version); ISSN: 1314-3395 (on-line version)
url: http://www.ijpam.eu
Special Issue

ijpam.eu

Fuzzy Logic with Bee Colony based Trusted Data Forwarding Routing Protocol (FLBC-TDFRP) for Mobile Ad Hoc Networks

[1]A.K. Ashfauk Ahamed, [2]M. Anand Kumar and [3]B.L. Shivakumar

[1]Department of Computer Applications,

Kongunadu Arts and Science College,

Coimbatore, India.

[2]Department of Information Technology,

Karpagam University,

Coimbatore, India.

[3]Sri Ramakrishna Polytechnic College,

Coimbatore, India.

Abstract

A mobile ad hoc network is a wireless network deployed in the region where there is no infrastructure or minimal infrastructure. Data forwarding in a secured manner is one among the thrust research are in such ad hoc scenario since there is more probability of interference in wireless channel. This planned research work aims in design and development of fuzzy logic with bee colony based trusted data forwarding routing protocol (FLBC-TDFRP) for mobile ad hoc networks. A belief form is developed using fuzzy logic. Then scout and forager authentication mechanism is incorporated in artificial bee colony. Finally proactive strategy is utilized in order to perform routing. Simulations are carried out through NS2 and the results portrays that the planned FLBC-TDFRP outperforms than that of the protocol chosen for comparison.

1. Introduction

A Mobile Ad Hoc Network (MANET) is a self-arranging system that consists of mobile hubs associated by remote connections that jointly structure a dynamic network construction. A secure MANET needs to convene more than a few security necessities like convenience, legitimacy, protection, uprightness, non-repudiation etc. The obligatory security prerequisites comprise secrecy, validation, uprightness, and non-repudiation. Some protocols are designed for MANET to be secure and strong. Because of absence of federal control, dynamic system topology, battery utilization, limited transmission capacity, elevated blunder rates and multi hop interchanges, the prerequisite of making the steering safe in MANETs is a huge contract contrast to the routing security in other networks that are based on infrastructure. The vast majority of the related work [1] – [4] in the range of secure steering conventions in MANET depends on key administration, grave encryption methods or on incessant loose watching of the neighbor nodes. During the fast moving of nodes in the MANET, these methods offer effectual but time devouring and costly outcomes. Trust definition as utilized by various scientists varies as indicated by the region of work [5]-[7]. The mobile node will attempt to forward a Request -To -Send (RTS) packet. Next, the mobile node will countercheck whether it gets back Clear-To-Send (CTS) packet [8]. In this paper a fuzzy logic with bee colony based trusted data forwarding routing protocol (FLBC-TDFRP) for mobile ad hoc networks is planned.

2. Related Works

In writing, secure steering conventions were thought to manage the limitations and necessities of impromptu systems. Marti et al. outlined Watchdog and Pathrater system [9] to upgrade the parcel sending strategy in the Dynamic Source Routing (DSR) convention [10]. It comprises of two parts: Watchdog and Pathrater. The Watchdog distinguishes narrow minded hubs that don't forward bundles and the Pathrater helps the directing conventions to maintain a strategic distance from these hubs. In view of the criticism got from the Watchdog, hubs were allocated appraisals. These evaluations are then used to choose courses having hubs with the most extreme sending rate. The principle errand of Watchdog is that it won't not identify a getting into mischief hub within the sight of: Ambiguous crashes, Receiver impacts, Limited transmission control, false trouble making and Partial dropping.

CONFIDANT (Cooperation of Nodes, Fairness in Dynamic Ad hoc Networks) [11] incorporates a trust supervisor and a notoriety framework to the Watchdog and Pathrater instrument [9]. The trust supervisor assesses the occasions detailed by the Watchdog and with a specific end goal to caution different hubs in the system concerning malignant hubs; for not sending, it sends alert. The notoriety framework at every hub keeps up a boycott of hubs and shares this rundown with the hubs in its companions list. The CONFIDANT convention

depends on a discipline thought, by not sending parcels of hubs whose trust level dips under a specific limit.

ARAN (Authenticated Routing for Ad-hoc Networks) planned by B. Dahill [12] that distinguishes and secures against mischievous activities of vindictive hubs in an ad-hoc organize. ARAN, in light of unbalanced cryptography, make employments of computerized endorsements and all hubs should keep up crisp testaments with a put stock in server and ought to know the server's open key. It requires the utilization of a trusted testament server in the system which is against the way of MANETs.

SEAD (Secure Efficient Ad hoc Distance vector) arranged by Y.Hu. [13], in light of Destination Sequenced Distance Vector (DSDV) [14] convention. It utilizes one way hash capacity and validation to recognize refreshes got from pernicious and non-vindictive hubs. It overpower the DoS and asset utilization assaults however falls flat when the aggressor utilizes a similar metric and succession number as utilized by the most recent refresh message. In the SEAD hubs, hash chain which has a limited size and should be recovered when every one of their components have been utilized. Y.Hu arranged ARIADNE [15], an on-request secure directing convention, in view of the Dynamic Source Routing (DSR) to safeguard against hub trade off. It depends on symmetric cryptography and the dispersal of shared mystery keys amongst source and the goal. For hub verification ARIADNE inclines toward utilizing the TESLA [16] broadcast confirmation plot with defered key exposure. TESLA requires clock synchronization between imparting hubs and this prerequisite is unrealistic in MANETs.

An exact and exact vindictive hub avoidance system for ad hoc networks is displayed in [17]. A hearty and appropriated get to control system in view of a trust form is arranged keeping in mind the end goal to secure the system and fortify participation by barring acting up hubs from the system. The system parts the get to control obligation into two settings: nearby and worldwide. The nearby setting responsibility is the area watch to advise the worldwide setting concerning the suspicious conduct.

In its turn, the worldwide setting investigates the data got and chooses in rebuffing the suspicious hub utilizing a voting plan. The prohibition instrument is displayed and plays out a parameter examination. Secure neighbor disclosure and wormhole confinement in the versatile ad hoc networks is arranged in [18]. Versatile Secure Neighbor Discovery (MSND), which offers a measure of assurance against wormholes by allowing the taking an interest portable hubs to securely decide whether they are neighbors, and a wormhole confinement convention, which allows the hubs that distinguished the nearness of a wormhole to decide wormhole's area. This additionally helps in recognizing the stale courses from the new ones, accordingly staying away from the arrangement of circles [19].

3. Planned Work

At earliest fuzzy logic is used and afterward the fuzzy logic slanted multi-criteria are depicted for appointing faith worth to every hub. faith is spoken as association connecting two fellow citizen hubs. Our planned structure assesses node faith and path faith. The node trust is the node's quality and they gave administrations to transmit packet, and the route trust is the nature of route. The fuzzy approach requires adequate master information for the definition of the rule base, the blend of the sets and the defuzzification. Applying fuzzy logic may be useful, for extremely complex process, when there is no basic numerical form, for exceptionally nonlinear procedures or if the procedure of master learning is to be performed.

Trust Calculation

In this stage the trust calculation is performed. It is mentioned as, during the time t, TRUST_VALUE (t) denotes the mobile node's trust. Usually this TRUST_VALUE will be a whole number which may be either 0 or 1. '0' means distrust and 1 means trust. v_i is denoted for evaluating nodes and v_j represents evaluated nodes. Certain conditions such as packet forwarding ratio, bandwidth and energy consumption are employed in order to ensure the appraise the forwarding pattern of the neighbor mobile nodes in the MANET environment.

For offering the packet transmission two criteria are considered with priority such as energy consumption and bandwidth. Since fuzzy logic is employed, the membership functions need to be configured for every paradigm in the phonetic set. The membership function evaluates the etymological terms as Very Low (VL), Low (L), Medium (M), High (H) and Very High (VH). Without doubt, fuzzification of the info factors is the primary stage of the fuzzy inference system. This stage recognizes how much information factors are belonging to each of the suitable fuzzy sets with the help of membership functions. In general, the energy consumption level attribute will fall under one or more fuzzy set. Also it is noteworthy that the degree of membership of a firm energy conservation ratio in this hiatus, in each set is distinctive.

Number of correctly forwarded packets to the whole amount of forwarded packets is defined as the forwarding ratio of the mobile node in MANETs. At the point when the bundles are sent to the next hub correctly, the corresponding node send parcel to its next bounce center point. Accordingly, when a malevolent hub tries to change the contents of the package then it is not said to be correctly forwarding. FORWARDING_RATIO (t) is measured by using the equation (1):

$$FORWARDING\_RATIO = \frac{N_c}{N_A} \quad (1)$$

Where N_c means the quantity of correctly forwarded packets and N_A means the total number of packets forwarded.

It is to be marked into the consideration that two types of packets such as control bundles and information parcels, FORWARDING_RATIO separated in the control parcel sending proportion, appeared as CPFR, and information parcel sending proportion, appeared as DPFR.

When a node attempts to send a package, it seats itself in a licentious state to verify the retransmission through the forwarding node. Likewise, the sender node keeps track of whether the package is correctly sent or not. During the transmit of a packet, a sender node elevates the number of control packets of all its neighbor nodes prior driving a bundle by 1 with the exception of the hub where the parcel originates from. As far as unicast type of communication is concerned, the sender mobile node only increases the control bundles of next jump by 1. When the package is correctly sent, the sender mobile hub increases its counter by 1.

It is quite natural that when the malicious behavior of a neighboring node is identified its forwarding ratio will drop down. It is also to be noted that when the trust_value _forwarding_ratio is low, the rating of trust esteem (communicated by TRUST_VALUE) also will be low.

The following fuzzy policy are represented for tracking down the malicious behavior of the neighboring node:

Fuzzy Rule 1: if trust_value_forwarding_ratio is very high, then TRUST_VALUE is very high.

Fuzzy Rule 2: if trust_value _forwarding_ratio is high, then TRUST_VALUE is high.

Fuzzy Rule 3: if faith_value _forwarding_ratio is average, then TRUST_VALUE is average.

Fuzzy Rule 4: if trust_value _forwarding_ratio is small, then TRUST_VALUE is small.

Fuzzy Rule 5: if faith_value forwarding_ratio is very small, then TRUST_VALUE is very low.

Accordingly, the TRUST_VALUE is a straightly proportional to trust_value _forwarding_ratio. Bandwidth is the next metric chosen keeping in mind the end goal to measure the trust estimation of the hub. In a condition where a node does not have sufficient data transfer capacity to forward the packages, then its capability is small which can be concluded as unreliable. The fuzzy rules are given below

Fuzzy Rule 6: if bandwidth is very high, then TRUST_VALUE is very high.

Fuzzy Rule 7: if bandwidth is high, then TRUST_VALUE is high.

Fuzzy Rule 8: if bandwidth is medium, then TRUST_VALUE is medium.

Fuzzy Rule 9: if bandwidth is low, then TRUST_VALUE is low.

Fuzzy Rule 10: if bandwidth is very low, then TRUST_VALUE is very low.

The next chosen metric is the residual energy. The residual vitality devoured by every hub in the MANET is ascertained as the total of transmitted, got and handled vitality for all control parcels. It is significant that when the residual vitality of a hub is low, the capacity level of offering administrations will likewise be low. The accompanying fuzzy standards introduce the connection between residual vitality and TRUST_VALUE:

Fuzzy Rule 11: if residual energy is very high, then TRUST_VALUE is very high.

Fuzzy Rule 12: if residual energy is high, then TRUST_VALUE is high.

Fuzzy Rule 13: if residual energy is medium, then TRUST_VALUE is medium.

Fuzzy Rule 14: if residual energy is low, then TRUST_VALUE is low.

Fuzzy Rule 15: if residual energy is very low, then TRUST_VALUE is very low.

Calculation of Course Trust

As far as faith computation for route is concerned. The faith value of the route need not be more prominent than the trust estimations of transitional hubs. Hence it can be represented as, at time t, the course trust is ascertained by the accompanying condition:

$$RouteTv_{sd}(t) = \prod(\{TV_{ij}(t) \mid v_i, v_j \in P \text{ and } v_i \to v_j\}) \quad (2)$$

where v_s and v_d are the source hub and the goal hub of route P, correspondingly, v_i and v_j are two neighboring nodes and $v_i \to v_j$ denotes that v_j is the next-hop hub of v_i.

Scout and Forager Authentication

In a situation where the source hub in the system tries to forward the information to the destination node in the network, initially, it ensures its hop base to state a forager for an information parcel. Once when it identifies then it makes use of the whole source route in forager for all the packet sending and receiving process. If not, it simply broadcast a forward scout to all its neighbor nodes in order to discover new courses to the goal hub. This forward scout consists of source ID, destination ID, source route and TRUST_VALUE attached by the halfway hubs along the course.

Once subsequent to performing the sending and receiving process by the forward scout, the dispatcher node lays itself in licentious state and computes the faith cost of evaluated hubs as described in the previous section.

In another scenario where a hub obtains a onward inspect, it is capable enough to substantiate that the forward scout has not performed any modification by a malevolent hub. This is possible by making use of the list of node TRUST_VALUE. Then it adds its corresponding address with the source route and TRUST_VALUE obtained from the upstream hub on the course to the forward scout and retransmits it.

Once onward inspect arrived at the target node, it has the catalog of hubs and TRUST_VALUEs of each jump by the side of the route. Then it computes the best route once when there is more than one discovered route that has an equivalent jump count. After this, the target mobile node performs the unicast operation back to the source hub and subsequent to transmitting figures the trust estimation of the assessed hub. After the backward inspect (which is obtained by the cause hub), it checks whether it hadn't altered by a malevolent hub by making use of the list of node TRUST_VALUEs. After that it employs the foragers for sending information to the target node.

In the same way, subsequent to the communication of forager, each hub, calculates the faith cost of evaluated nodes. In this mechanism in order to defend the directing data identified by forager along the route, a sending node exploits a digital autograph. The receiving node in the mobile ad hoc network performs the operation to substantiate the integrity of routing information with the help of hash message.

Routing Mechanism

The FLBC-TDFRP inherits the mechanism of conventional Bellman-Ford Routing Algorithm with specific improvements. Every one of the hubs in the MANET comprise of a directing table. The steering table keeps up the accessible goals, the quantity of bounces to achieve the goal and the grouping number relegated by the goal hub. The arrangement number is utilized in the steering table keeping in mind the end goal to recognize invalid courses from new ones. This will keep away from the formation of loops during the packet transmission. The nodes in the MANET sporadically articulate their steering tables to their moment neighbor hubs. A mobile hub likewise sends its own particular steering table when there is a noteworthy change has happened in its table from the last refresh sent. As a result, the refresh is both time-driven and occasion driven.

During the time MANET is moderately steady, incremental updates are sent to steer clear of additional movement and full dump are fairly uncommon. In a rapid topology the varying system scenario, incremental parcels possibly produce full dumps which is more often circumstance happening. Every course refresh bundle, too to the steering table data, additionally has an exceptional

arrangement number doled out by the transmitter versatile hub. The course marked with the most astounding arrangement number is utilized. At the point when two courses have a similar arrangement number then the course with the shortest route is taken for the data transmission. Also depending on the previous transactions, the nodes guesstimate the resolving time of courses. The hubs will likewise concede the transmission of a steering refresh by settling time keeping in mind the end goal to evacuate such updates when a better route is found [20] [21].

4. Simulation Settings, Results and Discussions

Random waypoint form is chosen in order to place the node trajectories. As far as the random waypoint form is concerned, every mobile node in the MANET moves toward a progression of target positions. The moving speed is obtained between 0 to v_{max}. When the target position is attained, it will not move for a specific amount of time. Random waypoint form commonly guide to an uneven hub dispersion in the MANET by which it coincides with the real time scenario. On the other hand, toward the start of reproductions, the hubs' positions are reliably dispensed; therefore, the reenactment information in the initial 30 s is scratched off, and just the information at an enduring state is gathered. The performance of the existing routing protocol PSR, and FLBC-TDFRP are evaluated in the scenario of TCP flows with the default 250-m transmission run in ns-2 which moves with v_{max} = 30 m/s.

Fig.1. projects the performance analysis of the routing overhead with density. It is evident that the planned FLBC-TDFRP performs superior to the PSR protocol. Fig.2. shows the performance analysis of TCP throughput with density. It is obvious that the planned FLBC-TDFRP performs superior to the PSR protocol. Fig.3. depicts the performance analysis of End-to-end defer in TCP with density. It is clear that the planned FLBC-TDFRP performs superior to the PSR protocol.

Fig.4. projects the performance analysis of routing overhead with the velocity. It is proved that the planned FLBC-TDFRP performs superior to PSR protocol. Fig.5. depicts the performance analysis of TCP throughput with velocity. It is clear that the planned FLBC-TDFRP performs superior to PSR protocol. Fig.6. depicts the performance analysis of end-to-end defer in TCP with velocity. It is obvious that the planned FLBC-TDFRP performs superior to the PSR protocol.

Fig.7. projects the performance analysis of PDR in UDP with density. It is evident that the planned FLBC-TDFRP performs superior to the PSR protocol. Fig.8. shows the performance analysis of end-to-end defer in UDP with density. It is clear that the planned FLBC-TDFRP performs superior to PSR protocol. Fig.9. projects the performance analysis of End-to-end defer jitter in UDP with density. It is obvious that the planned FLBC-TDFRP performs superior to the

PSR protocol. Fig.10. shows the performance analysis of PDR in UDP with velocity. It is clear that the planned FLBC-TDFRP performs superior to the PSR protocol. Fig.11. depicts the performance analysis of End-to-end defer in UDP with velocity. It is proved that the planned FLBC-TDFRP performs superior to the PSR protocol. Fig.12. shows the performance analysis of End-to-end defer jitter in UDP with velocity. It is obvious that the planned FLBC-TDFRP performs superior to the PSR protocol [22][23].

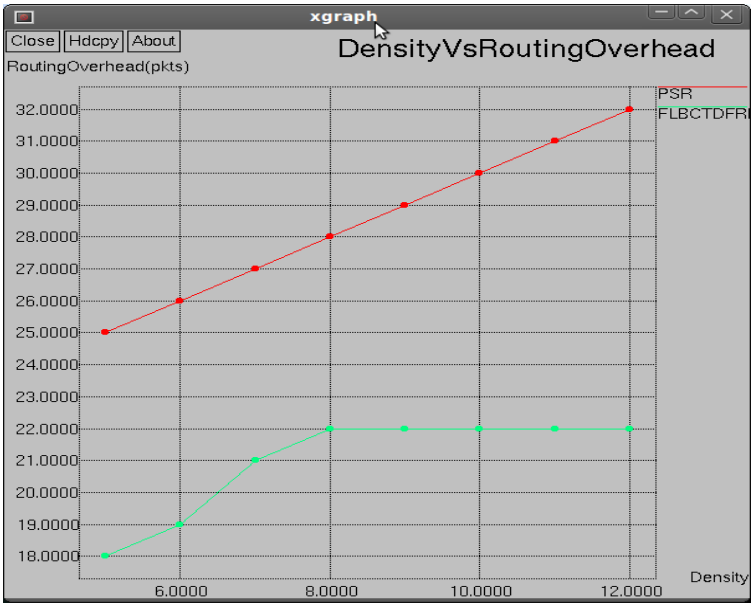

Figure 1: Routing Overhead with Density

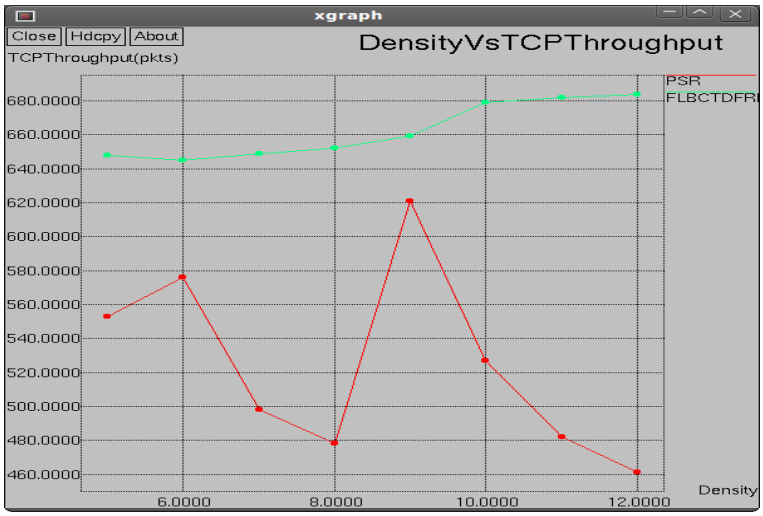

Figure 2: TCP Throughput with Density

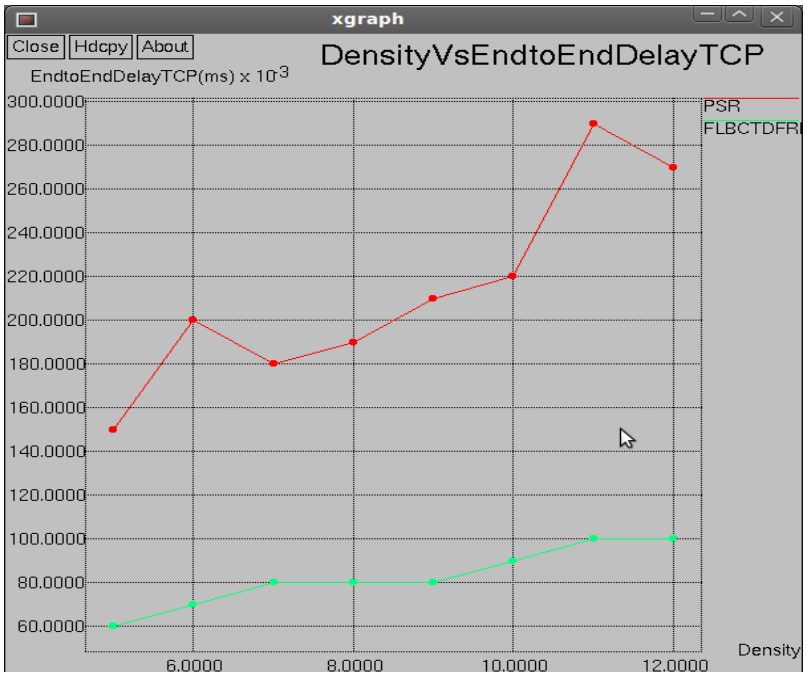

Figure 3: End-to-End Defer in TCP with Density

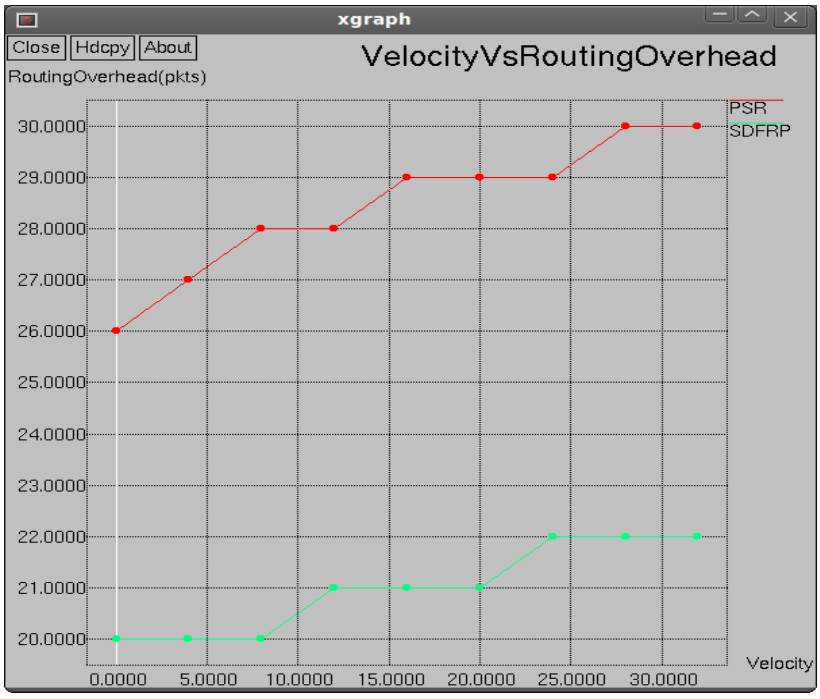

Figure 4: Routing Overhead with Velocity

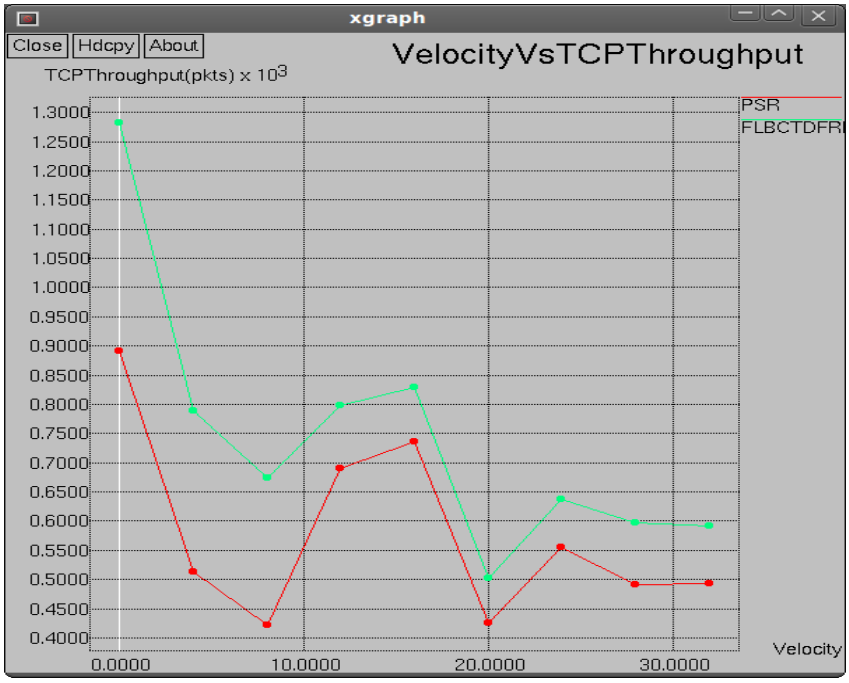

Figure 5: TCP Throughput with Velocity

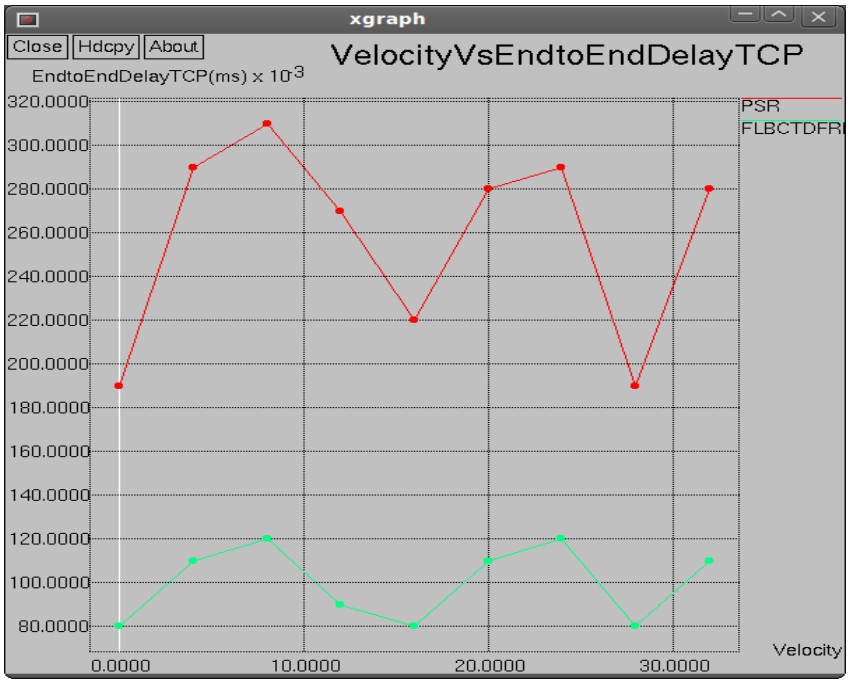

Figure 6: End-to-End Defer in TCP with Velocity

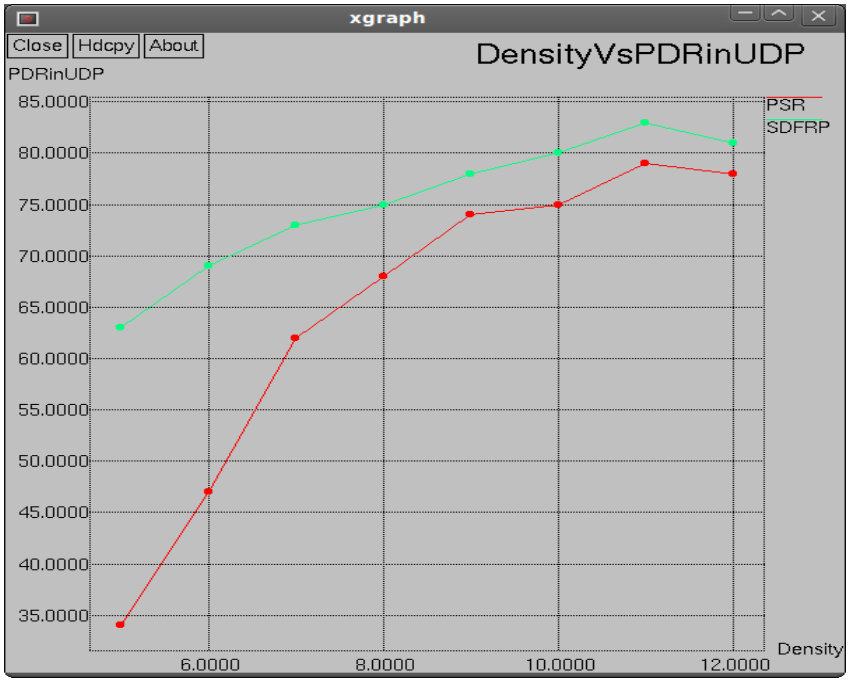

Figure 7: PDR in UDP with Density

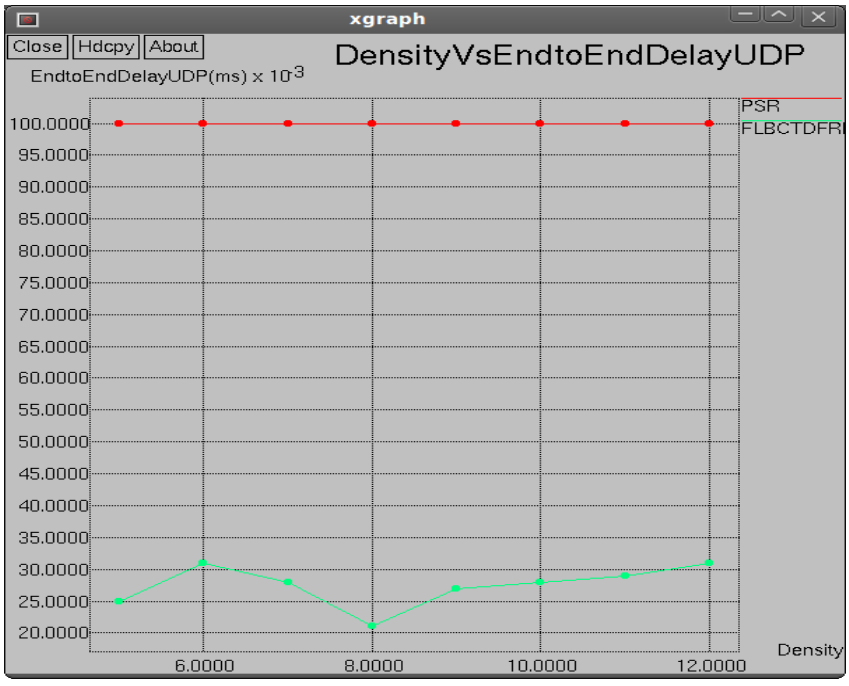

Figure 8: End-to-End Defer in UDP with Density

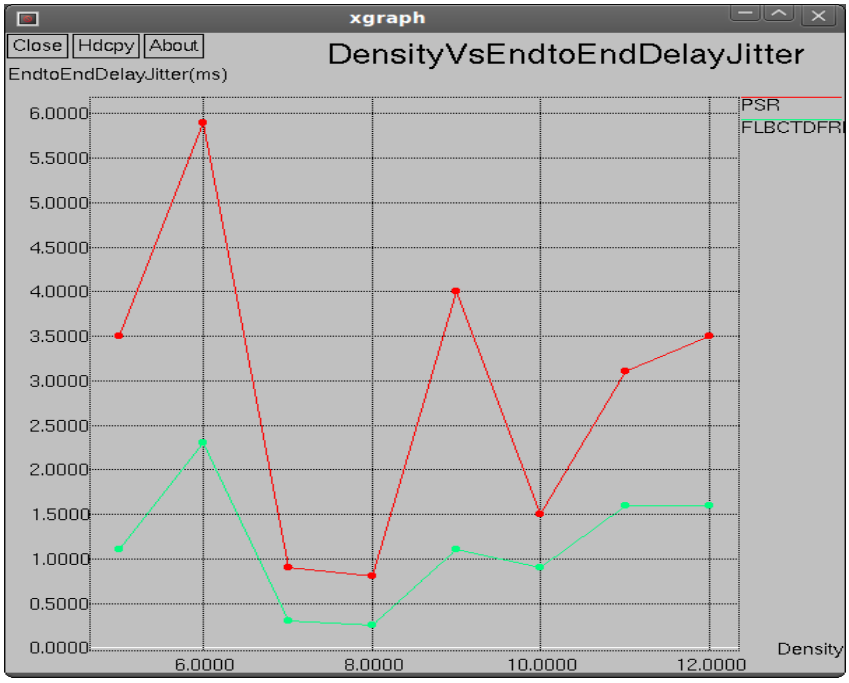

Figure 9: End-to-End Defer Jitter in UDP with Density

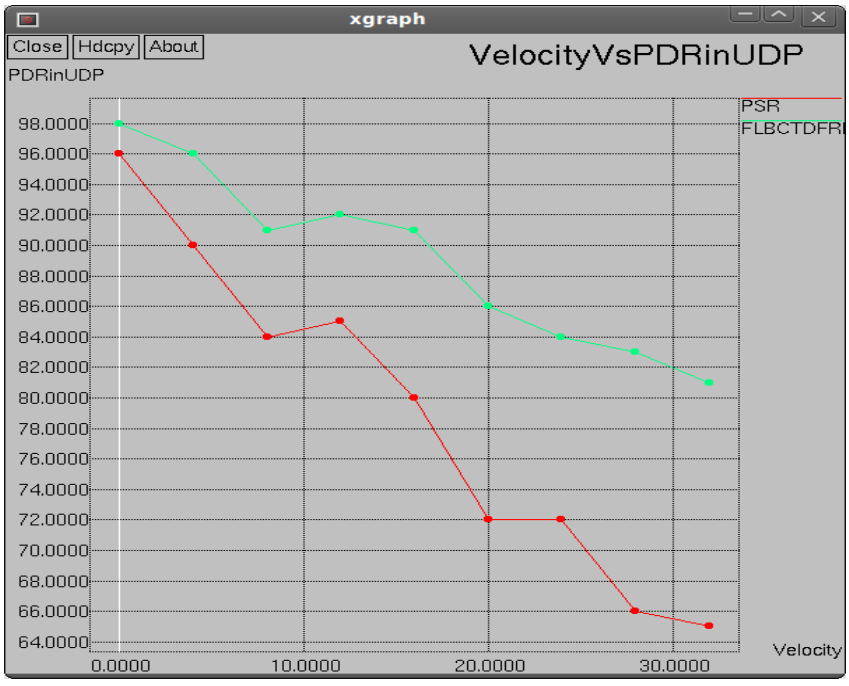

Figure 10: PDR in UDP with Velocity

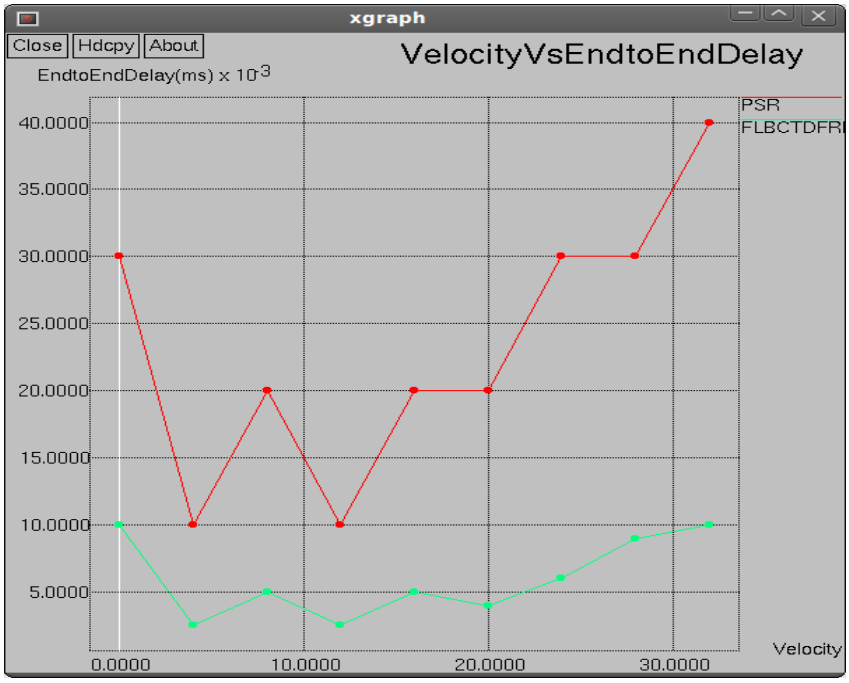

Figure 11: End-to-End Defer in UDP with Velocity

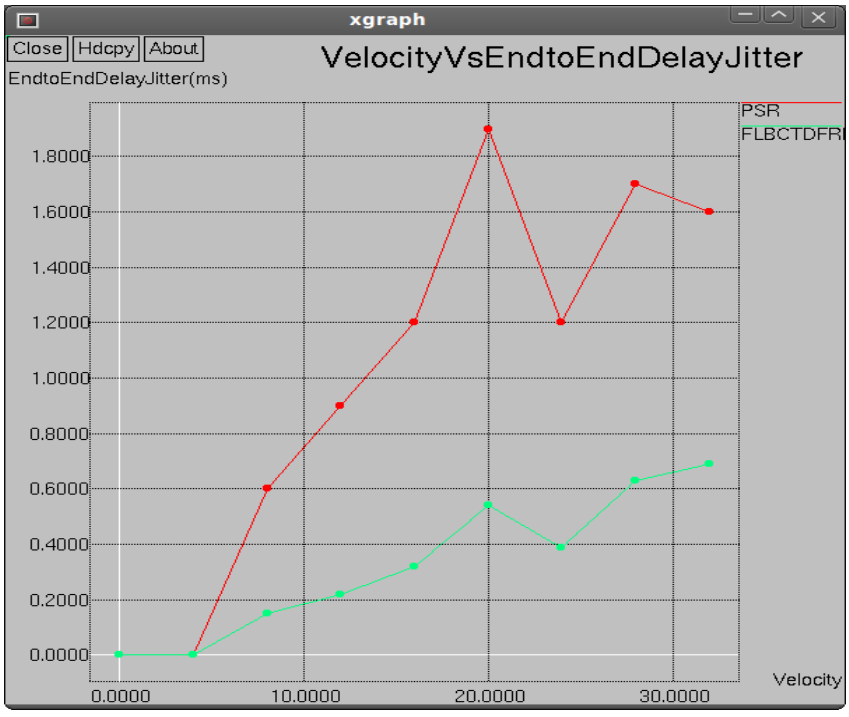

Figure 12: End-to-End Defer Jitter in UDP with Velocity

5. Conclusion

The planned research work aims in design and development of Fuzzy Logic with Bee Colony based Trusted Data Forwarding Routing Protocol (FLBC-TDFRP) for mobile ad hoc networks. A faith form is developed using fuzzy logic. Then the scout and forager authentication mechanism is incorporated in the artificial bee colony. Finally proactive strategy is utilized in order to perform routing. Simulations are carried out through NS2. Bundle conveyance proportion, end-to-end defer and jitter are chosen as performance metrics for testing the efficiency of the planned routing protocol and the results portrays that the planned FLBC-TDFRP outperforms than the PSR protocol.

References

[1] Zhou L., Haas Z.J., Securing ad hoc networks, IEEE network 13(6) (1999), 24-30.

[2] Zapata M.G., Asokan N., Securing ad hoc routing protocols, In Proceedings of the 1st ACM workshop on Wireless security (2002), 1-10.

[3] Papadimitratos P., Haas Z.J., Secure data transmission in mobile ad hoc network, In ACM Workshop on Wireless Security, San Diego, CA (2003), 41-50.

[4] Narasimhan B., Vadivel R., Secured reliable multipath routing protocol (SRMRP) using trust computation and carrier sense multiple access with collision intimation (CSMA/CI) for heterogeneous IP-based mobile ad-hoc networks, International Journal of Computer Applications 60 (10) (2012), 12-16.

[5] Mui L., Mohtashemi M., Halberstadt A., A computational model of trust and reputation, IEEE 35th Annual Hawaii International Conference on System Sciences (2002), 2431-2439.

[6] Grandison T., Sloman M., A survey of trust in internet applications, IEEE Communications Surveys & Tutorials 3(4) (2000), 2-16.

[7] Olmedilla D., Rana O.F., Matthews B., Nejdl W., Security and trust issues in semantic grids, In Dagstuhl Seminar Proceedings. Schloss Dagstuhl-Leibniz-Zentrum für Informatik, 2006.

[8] Ahamed A.A., Kumar M.A., Shivakumar B.L., Secured Data Forwarding Routing Protocol (SDFRP) For Heterogeneous Mobile Ad Hoc Networks, International Journal of Computer Trends and Technology (IJCTT) 39 (1) (2016).

[9] Marti S., Giuli T.J., Lai K., Baker M., Mitigating routing misbehavior in mobile ad hoc networks, In Proceedings of the 6th

annual international conference on Mobile computing and networking (2000), 255-265.

[10] Johnson D.B., Maltz, D.A., Dynamic source routing in ad hoc wireless networks, Mobile computing (1996), 153-181.

[11] Buchegger S., Le Boudec J.Y., Performance analysis of the CONFIDANT protocol, In Proceedings of the 3rd ACM international symposium on Mobile ad hoc networking & computing (2002), 226-236.

[12] Sanzgiri K., Dahill B., Levine B.N., Shields C., Belding-Royer E.M., A secure routing protocol for ad hoc networks, 10th IEEE International Conference on Network Protocols (2002), 78-87.

[13] Hu Y.C., Johnson D.B., Perrig A., SEAD: Secure efficient distance vector routing for mobile wireless ad hoc networks, Ad hoc networks 1(1) (2003), 175-192.

[14] Perkins C.E., Bhagwat P., Highly dynamic destination-sequenced distance-vector routing (DSDV) for mobile computers, In ACM SIGCOMM computer communication review 24 (4) (1994), 234-244.

[15] Hu Y., Perrig A., Johnson D.B., Adriane: a secure on-demand routing protocol for ad hoc network, Eighth Annual International Conference on Mobile Computing and Networking (2002), 12-23.

[16] Perrig A., Canetti R., Tygar J.D., Song D., The TESLA broadcast authentication protocol, Rsa Cryptobytes 5 (2) (2005).

[17] Ferraz L.H.G., Velloso, P.B., Duarte, O.C.M., An accurate and precise malicious node exclusion mechanism for ad hoc networks, Ad hoc networks (2014), 142-155.

[18] Stoleru R., Wu H., Chenji H., Secure neighbor discovery and wormhole localization in mobile ad hoc networks, Ad Hoc Networks 10 (7) (2012), 1179-1190.

[19] Ahamed A., Shivakumar B.L., A Survey on DSDV Node Design in Wireless Ad Hoc Networks, International Journal of Advanced Research in Computer Science 6(8) (2015).

[20] Anand Kumar M., Karthikeyan S., Security Form for TCP/IP Protocol Suite, Journal of Advances in Information Technology 2 (2) (2011), 87-91.

[21] Anand Kumar M., Karthikeyan S., Investigating the Efficiency of Blowfish and Rejindael (AES) Algorithms, International Journal of Computer Network and Information Security 4 (2) (2012), 22-28.

[22] Anand Kumar M., Karthikeyan S., A New 512 Bit Cipher - SF Block Cipher, International Journal of Computer Network and Information Security 4 (11) (2012), 55-61.

[23] Anand Kumar M., Karthikeyan S., An Enhanced Security for TCP/IP Protocol Suite, International Journal of Computer Science and Mobile Computing 2 (11) (2013), 331-338.

[24] RAJESH, M. "A SYSTEMATIC REVIEW OF CLOUD SECURITY CHALLENGES IN HIGHER EDUCATION." The Online Journal of Distance Education and e- Learning 5.4 (2017): 1.

[25] Rajesh, M., and J. M. Gnanasekar. "Protected Routing in Wireless Sensor Networks: A study on Aimed at Circulation." Computer Engineering and Intelligent Systems 6.8: 24-26.

[26] Rajesh, M., and J. M. Gnanasekar. "Congestion control in heterogeneous WANET using FRCC." Journal of Chemical and Pharmaceutical Sciences ISSN 974 (2015): 2115.

[27] Rajesh, M., and J. M. Gnanasekar. "Hop-by-hop Channel-Alert Routing to Congestion Control in Wireless Sensor Networks." Control Theory and Informatics 5.4 (2015): 1-11.

[28] Rajesh, M., and J. M. Gnanasekar. "Multiple-Client Information Administration via Forceful Database Prototype Design (FDPD)." IJRESTS 1.1 (2015): 1-6.

[29] Rajesh, M. "Control Plan transmit to Congestion Control for AdHoc Networks." Universal Journal of Management & Information Technology (UJMIT) 1 (2016): 8-11.

[30] Rajesh, M., and J. M. Gnanasekar. "Consistently neighbor detection for MANET." Communication and Electronics Systems (ICCES), International Conference on. IEEE, 2016.